

# JABLOTRON 100<sup>+</sup>

## Benutzerhandbuch



<b>1.</b>	<b>EINFÜHRUNG</b>	<b>3</b>
<b>2.</b>	<b>BETRIEB DES SYSTEMS JABLOTRON 100+</b>	<b>3</b>
2.1	Der Betrieb vor Ort	5
2.1.1	Die Verwendung der Systemtastatur	5
2.1.2	Codeberechtigung über die Tastatur	7
2.1.2.1	Scharfschaltung der Alarmanlage	9
2.1.2.2	Unscharfschaltung der Alarmanlage	9
2.1.2.3	Erzwungene Zugriffssteuerung	10
2.1.2.4	Teilscharfschaltung einer Alarmanlage	10
2.1.2.5	Beenden eines ausgelösten Alarms	10
2.1.2.6	Bereichssteuerung vom Menü der Tastatur mit einem LCD-Display	11
2.2.1	Die Verwendung der Systemtastaturen JA-110E und JA-150E	12
2.2.1.1	Scharfschaltung der Alarmanlage	14
2.2.1.2	Unscharfschaltung der Alarmanlage	15
2.2.1.3	Teilweise Scharfschaltung des Alarmsystems	15
2.2.1.4	Erzwungene Zugriffssteuerung	16
2.2.1.5	Einen Voll-Alarm beenden	16
2.2.1.6	Bereichssteuerung über die Berechtigung	17
2.2.1.7	Bereichssteuerung vom Menü der Tastatur	17
2.2.2	Steuerung des Systems mit einer Fernbedienung	17
2.2.3	Das System mit einem Computer (J-Link) steuern	18
2.3	Steuerung per Fernsteuerung – MyJABLOTRON	18
2.3.1	Steuerung des Systems über die MyJABLOTRON-App für Smartphones	19
2.3.2	Steuerung des Systems über die webbasierte Schnittstelle MyJABLOTRON	19
2.3.3	Steuerung des Systems über das Sprachmenü	19
2.3.4	Steuerung des Systems über SMS-Befehle	20
2.3.5	Steuerung des Systems per Fernzugriff mit einem Computer (J-Link)	20
2.3.6	Steuerung der programmierbaren Ausgänge (PG)	20
2.3.6.1	Tastaturbereich	20
2.3.6.2	Berechtigung über die Tastatur eines Benutzers	20
2.3.6.3	Vom Menü einer Tastatur mit einem LCD-Display	20
2.3.6.4	Fernsteuerung	21
2.3.6.5	MyJABLOTRON-App für Smartphones	21
2.3.6.6	webbasierte MyJABLOTRON-Schnittstelle	21
2.3.6.7	Einwählen	21
2.2.6.8	SMS-Nachricht	21
<b>3.</b>	<b>SPERRUNG/ DEAKTIVIERUNG IM SYSTEM</b>	<b>21</b>
3.1	Sperren von Benutzern	21
3.2	Sperren von Meldern	21
3.3	Zeitschaltuhr	22
<b>4.</b>	<b>ANPASSUNG DES SYSTEMS</b>	<b>22</b>
4.1	Änderung des Zugriffscodes eines Benutzers	22
4.2	Ändern, Löschen oder Hinzufügen von RFID-Karten / Tags / Chip	22
4.3	Ändern von Benutzernamen oder Telefonnummern	22
4.4	Hinzufügen/ Löschen eines Benutzers	22
4.5	Einrichten von Kalenderereignissen	23

5.	EREIGNISVERLAUF	23
5.1	Mit der LCD-Tastatur	23
5.2	Mit J-Link und einem Computer	23
5.3	Login bei MyJABLOTRON (webbasiert/Smartphone)	23
6.	REGELMÄSSIGE WARTUNG	24
7.	TECHNISCHE PARAMETER	25
8.	BEGRIFFSVERZEICHNIS	26

Vielen Dank, dass Sie sich für das Sicherheitssystem JABLOTRON 100+ entschieden haben. Dieses System ist eine einzigartige und flexible Lösung für die Sicherheit von gewerblichen und privaten Objekten, mit der sowohl drahtgebundene als auch drahtlose Geräte verwendet werden können. JABLOTRON 100+ ist sehr einfach zu steuern. Die Einfachheit der Steuerung besteht aus zwei Schritten, der Berechtigung mit einem Code oder einem RFID-Tag, gefolgt von dem Drücken eines einzelnen Tastaturbereichs mit zugewiesener Funktion auf einer Tastatur. Betätigen Sie zuerst eine Bereichstaste und berechtigen Sie sich dann. Die Steuerungsbereiche verwenden eine einfache und leicht verständliche Ampellogik. Die Anzahl der Bereiche kann sofort an die Anforderungen der Räumlichkeiten angepasst werden. Die Systemserie JABLOTRON 100+ bietet eine breite Palette an Meldern mit zeitlosem Design. Sie kann dank der kompletten Steuerung per Fernzugriff von überall aus bedient werden. Mit der webbasierten Schnittstelle MyJABLOTRON, der MyJABLOTRON-Applikation für Smartphones und der Software J-Link können Sie das System per Fernzugriff steuern, programmieren und überwachen.



Das System JABLOTRON 100+ ist für bis zu 600 Benutzer ausgelegt und kann in 15 einzelne Bereiche unterteilt werden. Es können bis zu 230 Geräte angeschlossen werden, wobei das System bis zu 128 programmierbare Mehrzweckausgänge (z. B. Hausautomatisierung) bietet.

## 2. BETRIEB DES SYSTEMS JABLOTRON 100+

Das Sicherheitssystem kann auf verschiedene Arten gesteuert werden. Um eine Alarmanlage unscharf zu schalten, ist immer eine Berechtigung in Form einer Benutzeridentifikation erforderlich. Das System erkennt die Identität der Benutzer und ermöglicht ihnen, die Systembereiche zu bedienen, denen sie zur Steuerung zugewiesen wurden. Sie können zwischen verschiedenen Einstellungsmöglichkeiten mit oder ohne Berechtigung wählen. Bei einer Standardberechtigung müssen Sie sich nicht selbst berechtigen, da das System nur durch Drücken der rechten Bereichstaste auf einer Tastatur bedient werden kann. Der Benutzername, das Datum und die Uhrzeit werden bei jedem Zugriff auf das System aufgezeichnet und im Systemspeicher gespeichert. Diese Information ist unbegrenzt verfügbar. Jeder Benutzer kann einen ausgelösten Alarm (Stoppen der akustischen Sirenen) auch nur durch Berechtigung in irgendeinem Teil des Systems (abhängig von seinen Zugriffsrechten) abbrechen. Dadurch wird das System jedoch nicht automatisch unscharf geschaltet (es sei denn, die Standardeinstellung des Systems wird geändert).

*Hinweis: Abhängig von der Konfiguration der Installation und Systemeinstellungen sind einige der unten beschriebenen Optionen möglicherweise nicht verfügbar. Fragen Sie Ihren Errichter hinsichtlich der Konfiguration der Installation.*

### Benutzer und ihre Zugriffsrechte

CODE-BERECHTIGUNG	TYPBESCHREIBUNG
AES-Code	Dieser Code entspricht der höchsten Berechtigungsstufe zur Konfigurierung des Systems. Ein Benutzer dieses Codes kann das System nach einem ausgelösten Alarm entsperren. Er kann den Errichtermodus eingeben, hat Zugriff auf alle Programmbereiche mit allen Optionen, einschließlich der AES-Kommunikation, auf die der Zugriff eines Errichters (Errichtercode) verweigert werden kann. Solange der Parameter „Administrator-beschränkter Service / AES-Recht“ unbeschränkt bleibt, kann der AES-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 AES-Codes ist nur durch die Maximalkapazität der Zentrale beschränkt. Der AES-Code wird nicht standardmäßig voreingestellt.
Errichtercode (Service)	Mit diesem Code kann der Errichter das System verwalten und konfigurieren. Er hat Zugriff auf alle Programmebenen und Optionen, einschließlich der AES-Kommunikation, wenn nicht der Zugriff durch einen übergeordneten AES verweigert wurde. Solange der Parameter „Administrator-beschränkter Errichter/ AES-Recht“ 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. Mit diesem Code ist man auch befugt, einen Alarm und den Sabotagealarmspeicher zu löschen. Der Code ist standardmäßig 1010. Der Service-Benutzer ist immer in der Zentrale auf Position 0 und kann nicht gelöscht werden.

CODE-BERECHTIGUNG	TYPBESCHREIBUNG
Administratorcode (Admin)	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, Zugriffs-codes, 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 „Administrator-beschränkt Errichter/AES-Recht“ aktiviert ist, muss der Administratorcode berechtigt werden, um den Zugriff für den AES und Errichter zu bestätigen. Der Code ist standardmäßig 1234. Der Hauptadministrator ist immer auf Position 1 und kann nicht gelöscht werden.
Administratorcode (Andere)	Mit diesem Administrator-Code hat man das Zugriffsrecht auf alle 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 „Administrator-beschränkt Errichter/AES-Recht“ aktiviert ist, muss das Zugangsrecht des Administratorcodes bestätigt werden. Die Anzahl der Administratorcodes (andere) ist nur durch die Maximalkapazität der Zentrale beschränkt. Es gibt keinen in den Werkseinstellungen festgelegten Code.
Benutzercode	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 Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Scharfschalten	Mit diesem Code darf man nur einen bestimmten Bereich scharf schalten und kann PG-Ausgänge (EIN/AUS) steuern. Benutzer dieser Berechtigungsstufe dürfen ihren Code nicht ändern und dürfen den Alarmspeicher nicht löschen. Die Anzahl der eingestellten Codes ist nur durch die Maximalkapazität 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 Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Überfallalarm	Mit diesem Code kann nur ein Panikalarm/ Überfallalarm ausgelöst werden. Der Benutzer dieses Codes kann weder diesen Code ändern noch den Alarmspeicher löschen. Die Anzahl der Panikcodes ist durch die Maximalkapazität 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 Überwachungscode das System nur während oder nach einem Alarm deaktivieren, solange der Alarmspeicher noch aktiv ist. Ein Benutzer dieses Codes darf weder diesen ändern noch den Alarmspeicher löschen. Die Anzahl der Überwachungs-codes ist nur durch die Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Entsperrern	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 Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.

### Die Sicherheit von Zugriffs-codes, kontaktlosen RFID-Geräten und Fernsteuerungen:

Jedem Benutzer kann ein 4-, 6-, oder 8-stelliger Code und bis zu zwei RFID-Tags zugewiesen zu werden, die eine Zugriffsberechtigung beim System ermöglichen. Die Benutzerberechtigung ist für jede Bedienung über die Tastatur, das Sprachmenü, den Computer oder der webbasierten und mobilen Apps erforderlich. Die Codelänge beeinflusst die Anzahl der möglichen Kombinationen und damit die Sicherheit des Codes.



### Die Anzahl der Codekombinationen hängt von der Konfiguration ab:

Parameter der Zentrale	4 ZIFFERN	6 ZIFFERN	8 ZIFFERN
„Code mit einem Präfix“ aktiviert	$= 10^4 = (10.000)$	$= 10^6 = (1.000.000)$	$= 10^8 = (100.000.000)$
„Code mit einem Präfix“ und „Erzwungene Zugriffssteuerung“ deaktiviert	$= 10^4 - (\text{Anzahl der Benutzer} - 1)$	$= 10^6 - (\text{Anzahl der Benutzer} - 1)$	$= 10^8 - (\text{Anzahl der Benutzer} - 1)$
„Code mit einem Präfix“ deaktiviert; „Erzwungene Zugriffssteuerung“ aktiviert	$\leq 10^4 - ((\text{Anzahl der Benutzer} - 1) * 3)$	$\leq 10^6 - ((\text{Anzahl der Benutzer} - 1) * 3)$	$\leq 10^8 - ((\text{Anzahl der Benutzer} - 1) * 3)$
Verwendung von nur einer RFID-Karte mit einer Auswahl von 14 Zeichen (6 Konstante + 8 Variable)	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$
„Code mit einem Präfix“ und „Kartenbestätigung mit einem Code“ aktiviert	$= (10^8 * 10^4) = 10^{12} = (1.000.000.000.000)$	$= (10^8 * 10^6) = 10^{14} = (100.000.000.000.000)$	$= (10^8 * 10^8) = 10^{16} = (1.000.000.000.000.000)$
„Code mit einem Präfix“ deaktiviert; „Kartenbestätigung mit einem Code“ aktiviert	$= 10^8 * (10^4 - (\text{Anzahl der Benutzer} - 1))$	$= 10^8 * (10^6 - (\text{Anzahl der Benutzer} - 1))$	$= 10^8 * (10^8 - (\text{Anzahl der Benutzer} - 1))$

Wege zur Verbesserung des Schutzes gegen das Erraten eines gültigen Codes:

- ▶ Verwendung eines Codes mit mehreren Ziffern (6 oder 8-stelliger Code),
- ▶ Erweiterte Berechtigungsarten (z. B. „Kartenbestätigung mit einem Code“ oder „Doppelte Berechtigung“).

### Bedienungswege der JABLOTRON 100+:

#### Vor Ort:

- ▶ Systemtastatur
- ▶ Systemfernbedienung
- ▶ Computer mit einem USB-Kabel und der Software J-Link

#### Per Fernzugriff:

- ▶ Smartphone-Applikation MyJABLOTRON
- ▶ Computer über die MyJABLOTRON-Schnittstelle
- ▶ Telefon über das Sprachmenü
- ▶ Telefon via SMS
- ▶ Computer über das Internet mit der Software J-Link
- ▶ Einwahl von einer berechtigten Telefonnummer (nur für programmierbare Ausgänge)



## 2.1 DER BETRIEB VOR ORT

### 2.1.1 DIE VERWENDUNG DER SYSTEMTASTATUR

Das System JABLOTRON 100+ kann über eine Vielzahl von Zugriffsmethoden gesteuert werden, mit denen Sie den Status einzelner Bereiche nicht nur steuern, sondern auch anzeigen können. Mit den Zwei-Tasten auf der Tastatur kann das System direkt gesteuert werden (Scharf- oder Unscharf schalten des Systems und andere Automatisierungsfunktionen). Die Bereichstasten sind deutlich und farbig (Ampellogik) gekennzeichnet, so dass jeder Bereichsstatus eindeutig angezeigt wird. Ein Bereich kann auch als Statusanzeige (z. B. Garagentor öffnen) oder zur Steuerung verschiedener automatisierter Geräte (zum Beispiel Heizung oder Jalousien) verwendet werden. Die maximale Anzahl der Bereiche beträgt 20 für ein Bedienteil. Ein Bereich kann auch so programmiert werden, um direkt einen Notruf auszulösen z.B. medizinischer Notruf oder ein Überfall / Panikalarm.

**Dauerhaft grün**  
UNSCHARF / AUS

**Blinkt grün**  
EINGANGS-  
VERZÖGERUNG

**Blinkt rot**  
ALARM / ALARMSPEICHER

**Dauerhaft grün**  
ALLES OK

**Blinkt grün**  
STEUERUNG

**Blinkt grün 2x alle 2 Sek.**  
WARTUNG

**Dauerhaft gelb**  
FEHLER

**Blinkt gelb**  
SCHARFSCHALTUNG  
NICHT ERFOLGREICH



**Dauerhaft rot**  
SCHARF / EIN

**Blinkt rot**  
ALARM /  
ALARMSPEICHER

**Dauerhaft gelb**  
TEILSCHARF

KARTENLESER /  
TASTATUR

### Die Bedienteile und ihre Kombinationen:



**RFID-Kartenleser** – ermöglicht die Steuerung des Systems und der verschiedenen Bereiche bei Verwendung der Benutzercodes und mit den berührungslosen Lesern (RFID-Karte / Tag).

**Kartenleser mit einer Tastatur** – Der Benutzer kann das System bedienen und die Bereiche steuern unter Verwendung eines Codes oder bei der Verwendung des berührungslosen Lesers. Es kann entweder einen Code eingegeben werden, oder der berührungslose Leser mit RFID Karte / Tag verwendet werden. Für eine höhere Sicherheit ist auch die Kombination beider Methoden möglich.

**Kartenleser mit Tastatur und LCD-Display** – Der Benutzer kann das System bedienen und steuern unter Verwendung eines Codes oder bei der Verwendung des berührungslosen Lesers mit RFID Karte / Tag. Für eine höhere Sicherheit ist auch eine Kombination beider Methoden möglich. Alternativ kann das System auch über das Menü des LCD Display bedient und gesteuert werden.

Bei der Unscharfschaltung des Alarmsystems über die Bereichstasten muss sich der Benutzer immer identifizieren und berechtigen. Bei der Scharfschaltung des Alarmsystems und der Steuerung von Automatisierungsfunktionen ist die Identifikation und Berechtigungsabfrage optional.





Die Benutzer können sich selbst identifizieren und berechtigen, indem sie die zugewiesenen Codes eingeben oder die RFID-Karten / Tags verwenden. Jeder Benutzer kann einen Code und bis zu zwei RFID-Chips (Karten oder Tags) haben.

Empfohlene kontaktlose Codeträger: JABLOTRON 100+, Oasis oder Codeträger andere Anbieter können verwendet werden, wenn diese mit der Leserfrequenz von 125 kHz EM kompatibel sind. Wenn eine höhere Sicherheit erforderlich ist, kann das Alarmsystem so programmiert werden, dass eine Berechtigung und Freigabe erst dann erfolgt, wenn der RFID Codeträger und ein zusätzlicher Code verwendet wird.

Wenn ein Benutzer mehrere Bereiche gleichzeitig steuern möchten, müssen sie sich zunächst identifizieren und berechtigen und dann die Bereiche und Funktionstasten drücken. So kann zum Beispiel mit einer Berechtigung das Haus scharf geschaltet und die Garage unscharf geschaltet werden.

Wenn der Parameter „Code mit einem Präfix“ aktiviert ist, kann der Berechtigungscode auf der Tastatur aus bis zu elf Ziffern bestehen: einem Präfix (ein bis drei Ziffern), einem Stern \* (das das Präfix vom Hauptcode trennt), und einem 4-, 6-, und 8-stelligem Code, was von der Konfiguration abhängt (zum Beispiel: 123\*12345678, oder 1\*12345678). Alle Benutzer können ihren eigenen Code ändern, der dem Präfix folgt. Der Code wird auf der Tastatur mit dem LCD-Display, in J-Link oder der MyJABLOTRON-App geändert.

*Wenn der Parameter „Code mit einem Präfix“ aktiviert ist, können die Benutzer ihren Code ändern. Wenn der Parameter „Code mit einem Präfix“ deaktiviert ist, können die Codes nur vom Administrator geändert werden.*

### 2.1.2 CODEBERECHTIGUNG ÜBER DIE TASTATUR

Die Berechtigung mit einem Benutzercode erfolgt über das Eingeben eines gültigen Codes auf der Tastatur oder über einen RFID-Tag.

Es kann ein 4-, 6- oder 8-stelliger Code im System verwendet werden.

Das System kann so konfiguriert werden, dass Präfix-Codes verwendet oder weggelassen werden (Standardeinstellung) können. Für Alarmsysteme mit einer erhöhten Benutzeranzahl kann das Präfix aktiviert werden. Zur Änderung dieser Option kontaktieren Sie bitte Ihren Errichter.

#### **Code ohne Präfix: CCCC**

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

**Standardcodes der Zentrale**

**Administrator: 1234; 123456; 12345678;**

#### **Code ohne Präfix: nnn\*CCCC**

**nnn** ist das Präfix, das die Nummer der Position des Benutzers darstellt (Position 0 bis 600)

**\*** ist eine Trennung (key \*)

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

**Standardcodes der Zentrale**

**Administrator: 1\*1234; 1\*123456; 1\*12345678;**

#### **WARNHINWEIS:**

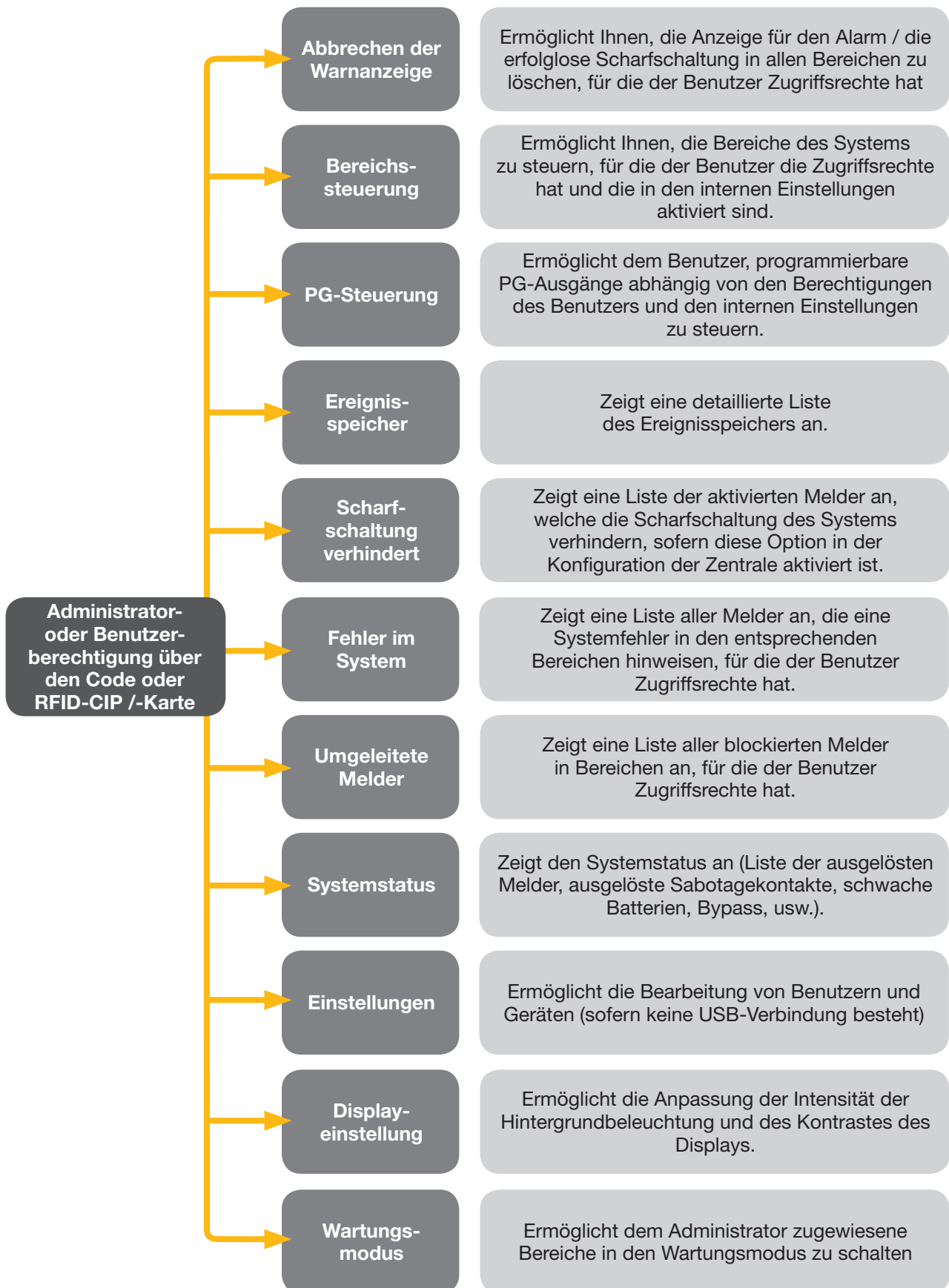
Der Haupt-Administratorcode beginnt mit dem Präfix 1

Der Haupt-Servicecode beginnt mit dem Präfix 0

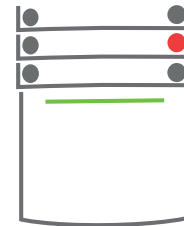
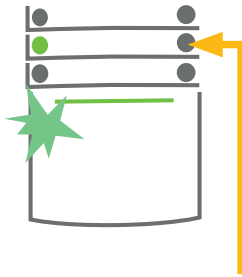
Zur Änderung des Codetyps kontaktieren Sie bitte den Errichter Ihres Alarmsystems.



## Struktur und Beschreibung des internen LDC-Tastaturmenüs



### 2.1.2.1 SCHARFSCHALTUNG DER ALARMANLAGE



1. Berechtigen Sie sich über die Tastatur. Die Bereiche, die gesteuert werden können, leuchten auf und die hintergrundbeleuchtete Anzeige beginnt grün zu blinken.
2. Drücken Sie die rechte Taste (die, die nicht aufleuchtet) und schalten Sie den jeweiligen

3. Der Befehl wird ausgeführt und die Tastatur zeigt die Ausgangsverzögerung akustisch

an. Der Bereich ist jetzt scharf geschaltet, nur die Melder mit der programmierten Funktion „Verzögerten Zone“ bieten Zeit, um den überwachten Bereich während der Ausgangsverzögerung zu verlassen. Die Bereichstaste der scharf geschalteten Bereiche wird rot angezeigt.

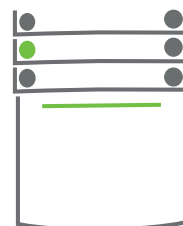
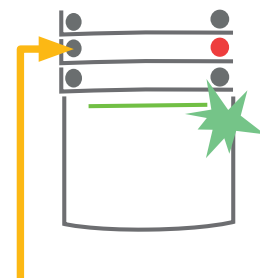
Wenn ein Melder während der Scharfschaltung des Alarmsystems aktiviert oder ausgelöst wird (z.B. ein offenes Fenster), reagiert das System (entsprechend der Systemkonfiguration) wie folgt:

- ▶ Aktivierte Melder werden nach dem Statuswechsel automatisch überwacht (Standardeinstellung).
- ▶ Das System zeigt die ausgelösten und aktiven Melder für 8 Sekunden rot blinkend an in dem Sicherungsbereich und schaltet sich nach Ablauf dieser Zeit automatisch scharf.
- ▶ Die Scharfschaltung mit ausgelösten und aktivierten Meldern ist auch möglich, indem Sie wiederholt auf die Bereichstaste auf der rechten Seite drücken. Auf diese Weise bestätigt der Benutzer die Absicht, den Bereich mit einem ausgelösten Melder (z. B. einem geöffneten Fenster) scharf zu schalten. Ansonsten wird der Bereich mit dem ausgelösten aktivierten Melder nicht scharf geschaltet.
- ▶ Ein ausgelöster aktivierter Melder verhindert, dass der Bereich scharf geschaltet wird. Dieser Status wird optisch durch eine blinkende rote Bereichstaste angezeigt. Der Melder, der die Scharfschaltung verhindert, wird im Menü auf dem LCD-Display angezeigt.

Eine erfolglose Scharfschaltung wird durch eine gelb blinkende Anzeigentaste angezeigt („Fehlgeschlagene Scharfschaltung“ muss aktiviert sein).

Wenden Sie sich zur Programmierung der gewünschten Funktionen an den Errichter des Alarmsystems.

### 2.1.2.2 UNSCHARFSCHALTUNG DER ALARMANLAGE



1. Wenn Sie das Gebäude betreten (Auslösung des Melders mit der Reaktion „Verzögerte Zone“), signalisiert das System die Eingangsverzögerung mit einem Dauerton und die Bereichstaste des Sicherungsbereiches, in dem der verzögerte Eingang ausgelöst wurde, blinkt grün.

2. Drücken Sie die linke Bereichstaste des Bereichs, den Sie unscharf schalten möchten.

3. Der Befehl wird ausgeführt und die Bereichstasten werden grün und zeigen die unscharf geschalteten Bereiche an.

**Hinweis:** Wenn die Parameter „den Bereich über die Berechtigung nur während der Eingangsverzögerung unscharf schalten“ aktiviert ist, wird die einfache Berechtigung den Bereich unscharf schalten, in dem die Eingangsverzögerung ausgelöst wurde.

Wenden Sie sich zur Programmierung der gewünschten Funktionen an den Errichter des Alarmsystems.

### 2.1.2.3 ERZWUNGENE ZUGRIFFSSTEUERUNG

Diese besondere Funktion ermöglicht die Unscharfschaltung des Systems in einem speziellen Modus. Das System wird scheinbar normal unscharf, löst jedoch im Hintergrund einen stillen Panikalarm aus, welcher ausgewählten Benutzern gemeldet wird (einschließlich der AES).

Die Unscharfschaltung unter Bedrohung oder Zwang erfolgt durch Hinzufügen von 1 zur letzten Zahl eines gültigen Codes.

Beispiel eines Codes mit einem Präfix:

**Gültiger Code: 2\*9999**

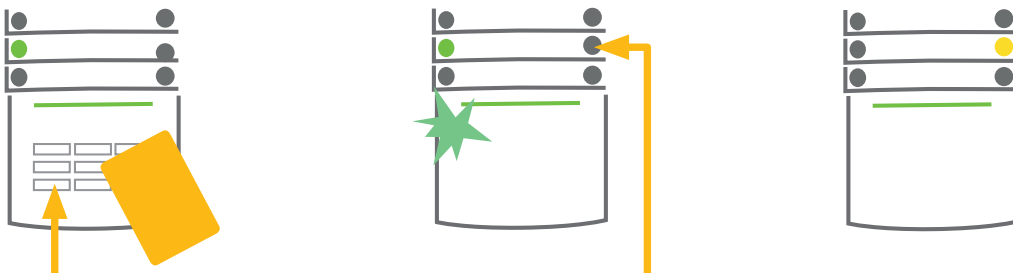
**Code für die Unscharfschaltung unter Zwang: 2\*9990**

Beispiel eines Codes ohne Präfix:

**Gültiger Code: 9999**

**Code für die Unscharfschaltung unter Zwang: 9990**

### 2.1.2.4 TEILSCHARFSCHALTUNG EINER ALARMANLAGE



1. Berechtigen Sie sich über die Tastatur (geben Sie einen Code ein oder halten Sie eine Karte oder Tag vor den Leser). Die grüne hintergrundbeleuchtete Anzeigetaste beginnt zu blinken.

2. Drücken Sie die rechte Bereichstaste des ausgewählten Bereichs.

3. Der Befehl wird ausgeführt und die Bereichstaste wird gelb und zeigt einen teilweise scharf geschalteten Bereich an.

Das System kann auch teilweise scharf geschaltet werden, wobei nur bestimmte Melder in einem Bereich überwacht werden. Beispiel: Nachts können nur die Tür- und Fenstermelder scharf geschaltet werden, während Bewegungsmelder in einem Haus auf nicht reagieren sollen.

Um ein Gebäude, das teilweise scharf geschaltet ist, vollständig scharf zu schalten, muss die Taste zur Scharfschaltung des Systems zweimal gedrückt werden. Nachdem die Taste einmal gedrückt wurde, blinkt sie gelb, wenn sie noch einmal gedrückt wird, blinkt sie rot.

Wenn das System teilweise scharf geschaltet ist - was durch eine dauerhaft gelbes Licht angezeigt wird - kann das gesamte System vollständig über die Berechtigung und das Drücken der gelben Taste scharf geschaltet werden. Wenn die Taste gedrückt wird, wird das System vollständig scharf geschaltet und die Taste wird rot.

### 2.1.2.5 BEENDEN EINES AUSGELÖSTEN ALARMS



1. Berechtigen Sie sich über die Tastatur (geben Sie einen Code ein, halten Sie einen Tag vor den Leser).

2. Drücken Sie die linke Bereichstaste des Bereichs, in dem der Alarm ausgelöst wurde.

3. Die Unscharfschaltung wird beendet und die Sirenen werden stumm geschaltet. Die grüne blinkende Taste zeigt die Unscharfschaltung des entsprechenden Bereichs an. Das rote blinkende Licht zeigt den Alarmspeicher an.

4. Berechtigen Sie sich und drücken Sie wieder die grüne Taste, um die Anzeige des Alarmspeichers abzubrechen.  
5. Der Bereich zeigt den unscharf geschalteten Bereich mit einer dauerhaft leuchtenden grünen Taste an.

Ein ausgelöster Alarm wird durch eine schnell blinkende rote Bereichstaste und eine leuchtende Anzeigentaste angezeigt. Zur Beendigung des Alarms müssen Sie sich über die Tastatur berechtigen. Der Bereich bleibt scharf geschaltet und die schnell blinkende rote Bereichstaste zeigt den Alarmspeicher an. Die Anzeige blinkt weiter, nachdem das System unscharf geschaltet wurde.

Wenn die Anzeige des Alarmspeichers während Ihrer Abwesenheit aktiviert wurde, suchen Sie nach der Ursache des Alarms im Ereignisverlauf und seien Sie sehr vorsichtig beim Betreten und Überprüfen der Räumlichkeiten oder warten Sie, bis der Sicherheitsdienst eintrifft (vorausgesetzt, Ihr System ist mit einem AES verbunden).

Die Anzeige des Alarmspeichers des Bereichs bleibt eingeschaltet, bis das System erneut scharf geschaltet wird. Alternativ kann sie durch erneute Unscharfschaltung des Systems abgebrochen werden. Die Alarmanzeige kann auch im Hauptmenü über die Tastatur mit einem LCD-Display abgebrochen werden - Warnanzeige abbrechen.

*Die Anzeige eines ausgelösten Sabotagealarms kann nur von einem Errichter oder dem Administrator beendet werden.*

*Hinweis: Bei Verwendung des Systemprofils „EN 50131-1, Stufe 2“ ist es immer erforderlich, sich zuerst zu berechtigen und dann die gewünschte Aktion durchzuführen.*

Die Beendigung eines Alarms per Fernsteuerung schaltet auch den entsprechenden Bereich unscharf.

### 2.1.2.6 BEREICHSSTEUERUNG VOM MENÜ DER TASTATUR MIT EINEM LCD-DISPLAY

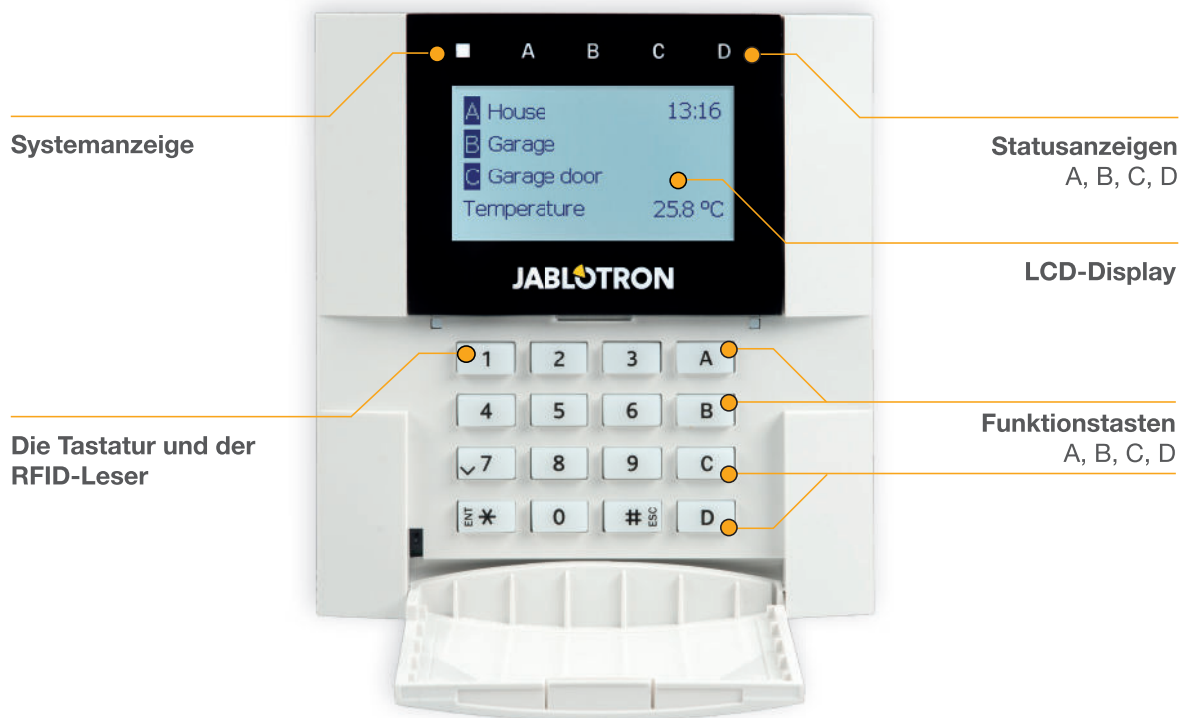
Der Status der Bereiche ist im oberen linken Teil des LCD-Displays der Tastatur angezeigt. Ein vollständig scharf geschalteter Bereich wird durch eine Zahl in einem schwarzen Rechteck dargestellt. **2**; ein teilweise scharf geschalteter Bereich wird durch eine umrahmte Zahl dargestellt **4**.

Steuerung des Tastaturmenüs:

- ▶ Berechtigung über einen gültigen Code oder einen RFID-Chip.
- ▶ Rufen Sie das Menü mit ENTER auf.
- ▶ Bereichssteuerung → ENTER.
- ▶ Wählen Sie den gewünschten Bereich mit den Pfeilen aus.
- ▶ Das wiederholte Drücken von ENTER wechselt zwischen den Bereichsstatusoptionen teilweise scharf / scharf / unscharf.
- ▶ Drücken Sie ESC, um das Menü zu verlassen.



## 2.2.1 DIE VERWENDUNG DER SYSTEMTASTATUREN JA-110E UND JA-150E



Der Status der einzelnen Bereiche wird durch die Statusanzeigen A, B, C, D über dem LCD-Display und durch die Funktionstasten angezeigt. Die Zentrale kann direkt gesteuert werden (Scharf- oder Unscharfschaltung des Alarms und andere Automatisierungsfunktionen), indem man die Funktionstasten auf der Tastatur verwendet. Die Funktionstasten und die Statusanzeigen A, B, C, D sind farbig hinterleuchtet, um den Bereichsstatus deutlich anzuzeigen.

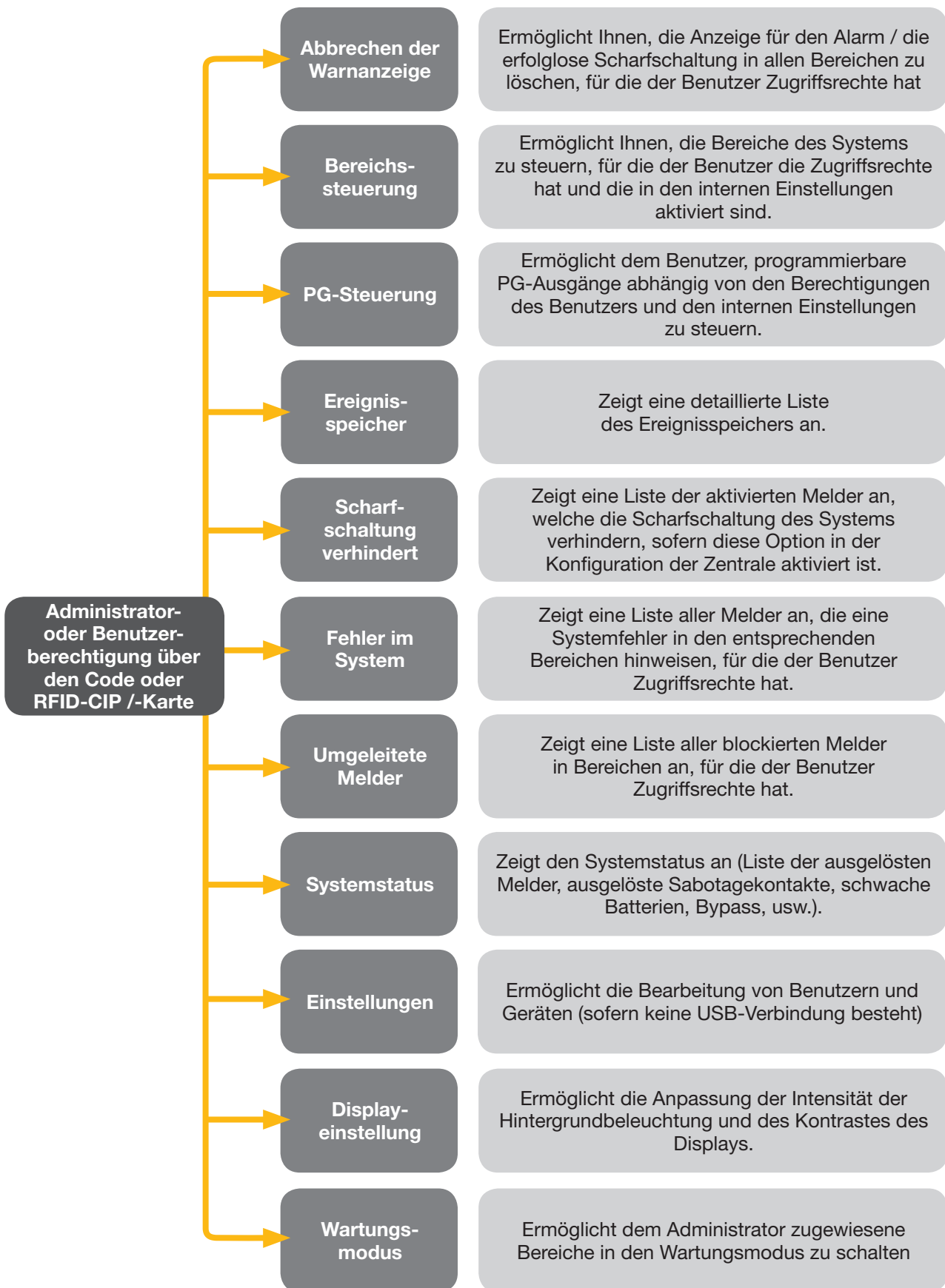
- ▶ **GRÜN** – Unscharf
- ▶ **GELB** – Teilweise unscharf
- ▶ **ROT** – Scharf

Die Berechtigung kann durch Eingabe eines Zugriffscode auf der Tastatur oder durch Verwendung einer RFID-Karte / Tag erfolgen, die einem Benutzer zugewiesen wurde. Jeder Benutzer kann einen Code und einen RFID-Chip (eine Karte oder ein Tag) haben.

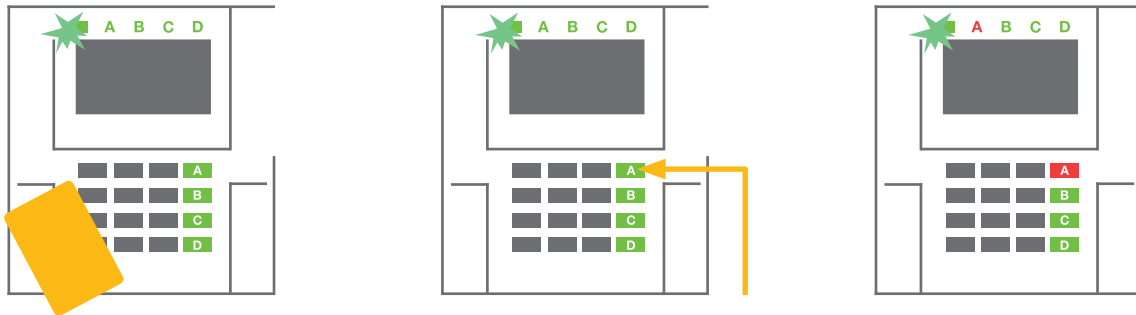
Wenn Benutzer mehrere Bereiche gleichzeitig steuern möchten, müssen sie sich berechtigen und dann die Funktionstasten der jeweiligen Bereiche drücken. Auf diese Weise können Benutzer alle Bereiche (z. B. das Haus und die Garage) innerhalb einer einzigen Berechtigung unscharf schalten.



Struktur und Beschreibung des internen LCD-Tastaturmenüs



## 2.2.1.1 SCHARFSCHALTUNG DER ALARMANLAGE



1. Berechtigen Sie sich über die Tastatur. Die Funktionstasten A, B, C, D der Bereiche, die Sie steuern können, leuchten auf und die Systemanzeige leuchtet grün auf.

2. Drücken Sie die Funktionstasten zur Scharfschaltung des jeweiligen Bereichs. Sie können mehrere Bereiche hintereinander scharf schalten. Die Verzögerung zwischen der Auswahl der Bereiche darf dabei nicht 2 Sekunden überschreiten.

3. Der Befehl wird ausgeführt und die Tastatur zeigt akustisch die Ausgangsverzögerung an. Der Bereich ist jetzt scharf geschaltet. Nur Melder mit der Reaktion einer „Verzögerten Zone“ bieten Zeit zum Verlassen des überwachten Bereichs während der Ausgangsverzögerung. Die Statusanzeige und eine Funktionstaste des scharf geschalteten Bereichs werden rot.

Wenn ein Melder bei der Scharfschaltung des Alarms ausgelöst wird (z.B. eine offenes Fenster), reagiert das System (entsprechend der Systemkonfiguration) auf die folgenden Weisen:

- Die Zentrale schaltet sich selbst scharf. Ausgelöste Melder werden automatisch gesperrt. \*) (Standardeinstellung).
- Das System zeigt optisch ausgelöste Melder über eine Funktionstaste an, die 8 Sekunden lang rot blinkt. Die Zentrale schaltet sich automatisch scharf, sobald dieser Zeitraum abgelaufen ist (ausgelöste Melder werden gesperrt). \*
- Die Scharfschaltung mit ausgelösten Meldern ist auch möglich, indem Sie wiederholt auf die Funktionstaste drücken. Auf diese Weise bestätigt der Benutzer die Absicht, den Bereich mit einem ausgelösten Melder (z. B. einem geöffneten Fenster) scharf zu schalten. Ansonsten wird der Bereich mit dem ausgelösten Melder nicht scharf geschaltet.
- Ein ausgelöster Melder verhindert, dass der Bereich scharf geschaltet wird. Dieser Status wird optisch durch eine blinkende rote Funktionstaste angezeigt. Der Melder, der die Scharfschaltung verhindert, wird im Menü auf dem LCD-Display angezeigt.

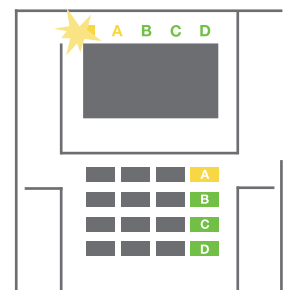
**\*) WARNHINWEIS:** Die Optionen a) und b) werden nicht von der EN 50131, Stufe 2 (ausgewähltes Systemprofil in der Zentrale) unterstützt.

Wird ein Melder mit der Reaktion „Alarm der Sofortigen Zone“ während einer Ausgangsverzögerung ausgelöst oder bleibt ein Melder mit der Reaktion „Alarm der Verzögerten Zone“ nach Ablauf der Ausgangsverzögerung aktiv, wird die Zentrale wieder unscharf geschaltet. Eine erfolglose Scharfschaltung wird durch eine gelb blinkende Systemanzeige angezeigt, die an das AES gemeldet und von einer externen Sirene angezeigt wird (gilt für Sicherheitsstufe 2).

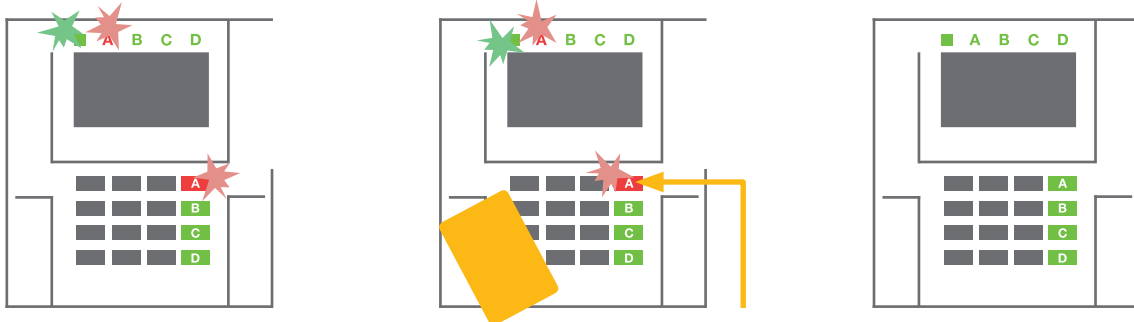
Wenn die Zentrale so konfiguriert ist, dass sie sich ohne Berechtigung scharf schaltet, müssen Sie sich nicht berechtigen. Alles, was Sie tun müssen, ist eine Funktionstaste eines bestimmten Bereichs zu drücken. Es ist auch möglich, die Zentrale so zu konfigurieren, dass sie sich einfach über die Berechtigung scharf schaltet.

**WARNHINWEIS:** Eine Scharfschaltung ohne Berechtigung senkt automatisch die Sicherheitsstufe auf Stufe 1. Berücksichtigen Sie daher alle Risiken bei Verwendung dieser Funktion.

Wenden Sie sich zur Programmierung des gewünschten Verhaltens des Alarmsystems an einen Projektberater oder Errichter.



### 2.2.1.2 UNSCHARFSCHALTUNG DER ALARMANLAGE



1. Wenn Sie das Gebäude betreten (und ein Melder mit einer Reaktion „Verzögerte Zone“ ausgelöst wird), beginnt das System die Eingangsverzögerung zu aktivieren und zeigt dies mit einem Dauerton an, wo eine Eingangsverzögerung ausgelöst wurde. Die Systemanzeige und eine Funktionstaste blinken rot.

2. Berechtigen Sie sich über die Tastatur – die Systemanzeige beginnt grün zu blinken.

3. Drücken Sie die Funktionstasten der Bereiche, die Sie unscharf schalten möchten.

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

*Hinweis: Wenn der Parameter „Unscharfschaltung des Bereichs über die Berechtigung nur während der Eingangsverzögerung“ aktiviert ist, schaltet die einfache Berechtigung einen Bereich unscharf, in dem die Eingangsverzögerung ausgelöst wurde. Diese Option sollte bei der Verwendung mehrerer Bereiche mit Vorsicht verwendet werden.*

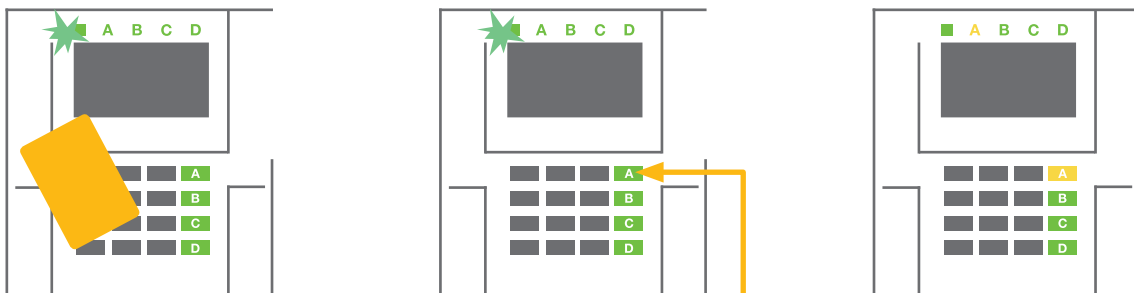
Wenden Sie sich zur Programmierung des gewünschten Systemverhaltens an einen Errichter.

### 2.2.1.3 TEILWEISE SCHARFSCHALTUNG DES ALARMSYSTEMS

**WARNHINWEIS:** Dies ist eine zusätzliche Funktion des Alarmsystems.

Das System kann auch so konfiguriert werden, dass es teilweise scharf geschaltet wird, wobei nur bestimmte Melder in einem Bereich überwacht werden.

**Beispiel:** In der Nacht ist es möglich, nur die Tür- und Fenstermelder scharf zu schalten, während die ausgewählten Bewegungsmelder keinen Alarm auslösen, wenn sich jemand innerhalb des Bereichs bewegt.



1. Berechtigen Sie sich über die Tastatur (geben Sie einen Code ein oder halten Sie eine RFID-Karte oder Tag vor den Leser). Die Anzeigentaste des Systems beginnt grün zu blinken.

2. Drücken Sie die Funktionstaste des ausgewählten Bereichs.

3. Der Befehl wird ausgeführt und die Funktionstasten werden dauerhaft gelb, um einen teilweise scharf geschalteten Bereich anzuzeigen.

Zur Scharfschaltung eines gesamten und teilweise scharf geschalteten Gebäudes halten Sie die Taste zur Scharfschaltung der Zentrale für 2 Sekunden gedrückt oder drücken Sie diese zwei Mal. Nach einmaligem Drücken der Taste wird ein gelbes Licht und nach dem zweiten Drücken ein rotes Licht dauerhaft angezeigt.

Wenn das System bereits teilweise scharf geschaltet ist - die Funktionstaste zeigt ein dauerhaftes gelbes Licht an - kann das gesamte System vollständig über die Berechtigung und das längere Drücken der gelben Taste scharf geschaltet werden. Wenn die Taste gedrückt wird, ist das System vollständig scharf geschaltet und die Taste wird rot.

Es kann auch so teilweise scharf geschaltet werden, dass keine Berechtigung erforderlich ist.

Um die Zentrale unscharf zu schalten, wenn sie teilweise scharf geschaltet ist, drücken Sie die gelbe Taste. Die Zentrale schaltet sich unscharf und die Taste wird grün.

### 2.2.1.4 ERZWUNGENE ZUGRIFFSSTEUERUNG

Hier erfolgt eine Unscharfschaltung in einem speziellen Modus. Das System scheint unscharf geschaltet zu sein, jedoch löst es einen stillen Panikalarm aus, der ausgewählten Benutzern gemeldet wird (einschließlich dem AES).

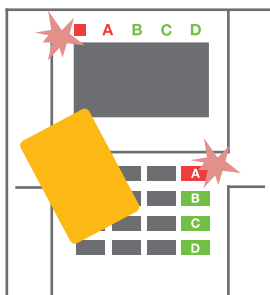
Die Unscharfschaltung unter Zwang wird ausgeführt, indem man 1 zur letzten Ziffer eines gültigen Codes hinzufügt. Kontaktieren Sie Ihren Errichter, wenn Sie diese Funktion verwenden möchten.

Beispiel:

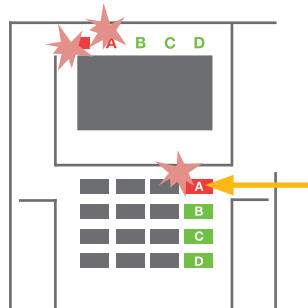
**Gültiger Code: 9999**

**Code zur Unscharfschaltung unter Zwang: 9990**

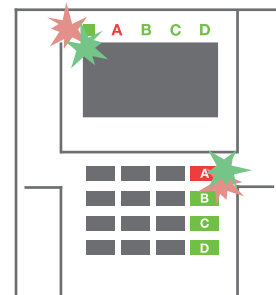
### 2.2.1.5 EINEN VOLL-ALARM BEENDEN



1. Berechtigen Sie sich über die Tastatur (geben Sie einen Code ein oder halten Sie einen Chip vor den Leser).



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



3. Die Unscharfschaltung ist beendet und die Sirenen verstummen. Die schnell nacheinander blinkenden Funktionstasten (grün/rot) und die Statusanzeigen zeigen den Alarmspeicher an.

Ein ausgelöster Alarm im Verlauf wird durch eine Statusanzeige und die schnell rot blinkende Funktionstaste angezeigt. Sie müssen sich über die Tastatur anmelden, um den Alarm zu beenden. Der Bereich bleibt weiterhin scharf geschaltet, wobei eine schnell blinkende rote Funktionstaste den Alarmspeicher anzeigt. Die Anzeige blinkt weiterhin, nachdem das System unscharf geschaltet wurde.

**WARNHINWEIS:** Wenn die Anzeige des Alarmspeichers während Ihrer Abwesenheit aktiviert wurde, betreten Sie das stets Gebäude mit Vorsicht, suchen Sie nach der Ursache des Alarms im Ereignisverlauf und seien Sie sehr vorsichtig beim Prüfen des Gebäudes oder warten Sie, bis der Sicherheitsdienst eingetroffen ist (vorausgesetzt, Ihr System ist mit einem Alarmempfangszentrum verbunden).

Die Anzeige des Alarmspeichers bleibt an, bis das System wieder scharf geschaltet wurde. Alternativ kann sie auch vom Menü der Tastatur aus beendet werden - Warnanzeige abrechen.

Die Anzeige eines ausgelösten Sabotagealarms kann nur von einem Errichter oder Administrator beendet werden.

*Hinweis: Bei Verwendung des „Standard“-Systemprofil kann eine individuelle Aktion ausgewählt werden, indem man zuerst eine Funktionstaste drückt und sie dann über die Berechtigung auf der Tastatur bestätigt.*

Das Beenden eines Alarms per Fernsteuerung schaltet auch den entsprechenden Bereich unscharf.

### 2.2.1.6 BEREICHSSTEUERUNG ÜBER DIE BERECHTIGUNG

Der Errichter kann die Zentrale so konfigurieren, dass sie nur über die Berechtigung gesteuert wird. So kann der Status aller Bereiche über die Berechtigung (indem man den Zugriffscode eingibt oder eine RFID-Chip verwendet) auf der Tastatur geändert werden.

### 2.2.1.7 BEREICHSSTEUERUNG VOM MENÜ DER TASTATUR

Steuerung vom Menü der Tastatur:

- Berechtigen Sie sich mit einem gültigen Code oder einem RFID-Chip
- Rufen Sie das Menü mit **ENTER** auf
- Bereichssteuerung → **ENTER**
- Wählen Sie den gewünschten Bereich mit den Pfeilen aus
- Wiederholtes Drücken der **ENTER**-Taste wechselt zwischen dem Status der Bereiche (teilweise scharf / scharf / unscharf)

Teilweise Scharfschaltung:

**1**

Vollständige Scharfschaltung:

**1**

- Drücken Sie **ESC** zum Verlassen des Menüs.



## 2.2.2 STEUERUNG DES SYSTEMS MIT EINER FERNBEDIENUNG

Fernbedienungen müssen vom Errichter im System angemeldet werden. Der Fernbedienung kann mit bestimmten Benutzern vernetzt werden, wodurch eine SMS-Benachrichtigung an den Benutzer verhindert wird, der gerade das System bedient (wenn die Benachrichtigungsparameter so eingestellt sind). Der Schlüsselanhänger bietet entweder eine bidirektionale Kommunikation, welche die Ausführung eines Befehls mit einer farbigen Leuchtanzeige bestätigt, oder eine Einweg-Kommunikation ohne Bestätigung. Schlüsselanhänger steuern und zeigen den Batteriestatus an und sind mit einer optischen und akustischen Anzeige ausgestattet.

### Bidirektionale Fernbedienungen

Die Tastenfunktionen werden durch die Sperrsymbole unterschieden. Das geschlossene Sperrsymbol schaltet den programmierten Bereich scharf; das geöffnete Sperrsymbol schaltet diesen unscharf. Die korrekte Ausführung des Befehls wird durch ein LED-Licht bestätigt; unscharf – grün, scharf – rot. Ein Kommunikationsfehler (der sich außerhalb des Funk-Bereiches der Zentrale befindet) wird durch eine einmal blinkende gelbe LED angezeigt. Die Tasten mit den vollen und leeren Kreissymbolen können andere Bereiche steuern. Die Tasten der Fernbedienung können auch so konfiguriert werden, dass sie PG-Ausgänge in unterschiedlichen Modi steuern: Die erste Taste schaltet ein / die zweite schaltet aus, wobei jede eine individuelle Funktion haben kann, wenn Impulse oder Schaltfunktionen verwendet werden. Für weitere Funktionen kann man auch zwei Tasten zur selben Zeit drücken. Auf diese Weise kann eine Fernbedienung mit 4 Tasten bis zu 6 individuelle Funktionen oder einen Status eines PG-Ausgangs (z.B. das Licht an- und ausschalten) und zwei PG-Ausgänge (z.B. das Schließen eines Garagentors und einer Tür) haben.



Wenn das System so konfiguriert ist, dass es sich nach einer Bestätigung scharf schaltet, zeigt der Melder eine fehlgeschlagene Scharfschaltung über eine grüne LED an, wenn das Gerät aktiviert wurde. Die Scharfschaltung muss durch wiederholtes Drücken der Sperrtaste bestätigt werden. Ein scharf geschalteter Bereich wird durch eine rote LED bestätigt.

Um unabsichtliches Drücken der Tasten zu verhindern, können diese gesperrt werden. Es wird ein Befehl gesendet, wenn eine Taste wiederholt gedrückt wurde.

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

*Für weitere Informationen hinsichtlich der Konfiguration der Fernsteuerung wenden Sie sich bitte an Ihren Errichter.*



### UNI- direktional Fernbedienung

Einweg- Fernbedienungen senden immer dann ein Signal, wenn eine Taste gedrückt wird, ohne dabei Feedback von der Zentrale zu bekommen. Das Senden des Signals wird durch kurzes Blinken einer roten LED und alternativ mit einem Piepton bestätigt.

Die Tastenfunktionen werden durch die Sperrsymbole unterschieden. Die Tastenfunktionen werden durch die Sperrsymbole unterschieden. Das geschlossene Sperrsymbol schaltet programmierte Bereiche scharf; das geöffnete Sperrsymbol schaltet sie unscharf. Die Tasten mit den Symbolen der vollen und leeren Kreise können weitere Bereiche oder einen PG-Ausgangsstatus (z.B. die Lichter an- und ausschalten) oder zwei PG-Ausgänge (z.B. ein Garagentor und eine Tür schließen) steuern.

Eine schwache Batterie wird durch eine rote LED und akustisch (mit 3 schnellen Pieptönen) angezeigt.



### 2.2.3 DAS SYSTEM MIT EINEM COMPUTER (J-LINK) STEuern

JABLOTRON 100+ kann lokal mit einem Computer über ein USB-Kabel und der installierten Software J-Link bedient werden. Diese kann für Administrationszwecke (Änderung der Benutzercodes, Karten/Tags, Telefonnummern usw.) und zur Einstellung von Kalenderereignissen verwendet werden.

J-Link ist für die lokale Verbindung mit einer Zentrale verfügbar und befindet sich auf dem Sicherheitslaufwerk des Systems (FLEXI\_CFG/j-link), das angezeigt wird, nachdem die Zentrale über ein USB-Kabel mit einem PC verbunden wurde.

Das System kann unter Verwendung der Symbole auf der unteren Leiste des Programms oder mit den Tasten „Status“ in dem Menü punkt „Bereich“ scharf / unscharf geschaltet werden. Wenn eine Tastatur mit mindestens einem steuerbaren Bereich mit dem System verwendet wird, kann das System in J-Link mit einer virtuellen Tastatur (klicken Sie auf „Tastatur“ im Hauptmenü) scharf / unscharf geschaltet werden.



**WARNHINWEIS:** Wenn das System über einen PC gesteuert wird, prüft dieser nicht, ob Geräte während der Scharfschaltung aktiviert werden. Dies kann zu einer Scharfschaltung mit einem aktivierten Gerät führen. Seien Sie deshalb vorsichtig, wenn Sie das System auf diese Weise steuern!

## 2.3 STEUERUNG PER FERNSTEUERUNG – MyJABLOTRON

Den höchsten Komfort hinsichtlich der Bedienung und Verwaltung des Systems bietet der MyJABLOTRON-Dienst.

Die webbasierte Schnittstelle von MyJABLOTRON ist ein einzigartiger Dienst, der Ihnen einen Online-Zugriff auf JABLOTRON-Geräte ermöglicht. Sie ermöglicht Endbenutzern, das System zu überwachen und zu steuern. Sie ist als Smartphone-App und als webbasierte Applikation verfügbar.

Der MyJABLOTRON-Dienst ermöglicht Benutzern:

- ▶ den aktuellen Systemstatus einzusehen,
- ▶ das System vollständig oder teilweise scharf / unscharf zu schalten,
- ▶ programmierbare Ausgänge zu steuern,
- ▶ den Ereignisverlauf einzusehen,
- ▶ ausgewählten Benutzern Berichte via SMS, Email oder als Push-Benachrichtigung zu senden,
- ▶ Bilder von Fotoverifikationsgeräten aufzunehmen und sie in der Fotogalerie oder direkt in den letzten Ereignissen zu suchen,
- ▶ den aktuellen Temperatur- und Energieverbrauch, einschließlich eines grafisch dargestellten Verlaufsüberblicks, zu überwachen,
- ▶ und andere nützliche Funktionen.

Abhängig von Ihrem Land oder der Region, kann ein webbasiertes MyJABLOTRON-Konto von einem autorisierten JABLOTRON-Partner eingerichtet werden. Der Login-Name ist die Email-Adresse des Benutzers. Das Passwort für den ersten Login wird an diese Adresse gesendet. Das Passwort kann jederzeit in den Benutzereinstellungen geändert werden.

### 2.3.1 STEUERUNG DES SYSTEMS ÜBER DIE MyJABLOTRON-APP FÜR SMARTPHONES

Nach der Erstellung des Benutzerkontos kann der Benutzer das System per Fernzugriff über die MyJABLOTRON-App für Android und iOS überwachen und steuern.

Die App kann kostenfrei in Google Play oder dem App Store heruntergeladen werden. Die Berechtigung des Benutzers kann sowohl über die Eingabe des Benutzercodes als auch je nach Technologie des Smartphones (Fingerabdruck, Face-ID usw.) erfolgen.

Nachdem Sie sich in das Konto eingeloggt haben, können Sie die aktiven Geräte sehen, die überwacht und gesteuert werden können.

Jedes Widget stellt einen Dienst dar. Das Tippen auf das Widget öffnet die Steuerungen mit einem Überblick über die Dienste. Das Menü ist entsprechend der Konfiguration in Lesezeichen aufgeteilt (Bereiche, Tastaturen, Automatisierung (PG), Thermostate und Thermometer, Zähler). In der unteren Leiste können Sie zwischen den Registerkarten Steuerung, Verlauf und Galerie schalten.

Die App ermöglicht dem Benutzer, ein Widget auf dem Homebildschirm mit einem direkten Link zu platzieren, um einen ausgewählten Bereich zu steuern oder um eine ausgewählte Funktion anzuzeigen, ohne die App öffnen zu müssen.



### 2.3.2 STEUERUNG DES SYSTEMS ÜBER DIE WEBBASIERTE SCHNITTSTELLE MyJABLOTRON

Das System JABLOTRON 100+ kann einfach und bequem mit Ihrem Computer via Internet und der webbasierten Schnittstelle von MyJABLOTRON, zu der Sie Zugang von [www.myjablotron.com](http://www.myjablotron.com) aus haben, bedient werden.

Wenn Sie sich in das Konto eingeloggt haben, können Sie alle aktiven Geräte sehen, die überwacht und gesteuert werden können.

Das Menü „Überblick“ enthält die Registerkarten „Bereich“ und „Verlauf“. Abhängig von den verwendeten Meldertypen, kann das Menü auch Registerkarten wie „Tastaturen“, „Automation (PG)“, „Thermostate und Thermometer“, „Zähler“ und „Galerie“ beinhalten.

Im unteren Teil der Homepage finden Sie einen Überblick über die letzten Systemereignisse.

MyJABLOTRON bietet kostenfreie Benachrichtigungen (SMS, Email, oder Push-Benachrichtigungen) für ausgewählte Ereignisse in den Bereichen des Systems, programmierbare Ausgänge, Thermometer oder Zähler. Diese Benachrichtigungen können in „Einstellungen“ eingerichtet werden.

Jedes System kann nur einen Hauptbenutzer mit Administratorrechten (Inhaber) haben. Dieser Benutzer hat das Recht, ein gesamtes Gebäude oder Teile davon (einzelne Bereiche, PG-Ausgänge, Fotoverifikation und Messgeräte) mit anderen Benutzern zu teilen, deren MyJABLOTRON-Konten automatisch erstellt werden, nachdem die Systemfreigabe konfiguriert wurde. Wenn ein Benutzer bereits ein MyJABLOTRON-Konto hat, erscheint die geteilte Installation auf dem Dashboard des Benutzers als weiteres aktives Gerät. Die Benachrichtigung über den freigegebenen Zugriff wird zusammen mit dem Passwort an die Email-Adresse (Login-Name) des neuen Benutzers gesendet.



### 2.3.3 STEUERUNG DES SYSTEMS ÜBER DAS SPRACHMENÜ

Das System kann von einem Telefon über das Sprachmenü gesteuert werden, das den Benutzer durch verschiedene Optionen in der vorkonfigurierten Sprache führt. Um in das Sprachmenü zu gelangen, wählen Sie die Telefonnummer des Alarmsystems.

Der Zugriff auf das Sprachmenü kann entweder allen Telefonnummern ohne Einschränkung oder alternativ nur berechtigten Telefonnummern, die in der Zentrale gespeichert sind, ermöglicht werden. Abhängig von der Konfiguration kann die Berechtigung über die Eingabe eines gültigen Codes in die Tastatur des Telefons erforderlich sein. Wenn der Benutzer das Menü aufruft, zeigt ihm das System eine Aktualisierung des aktuellen Status aller ihm zugewiesenen Bereiche. Der Anrufer kann dann diese Bereiche entweder einzeln oder gemeinsam steuern, indem er die Telefontastatur und verfügbare Menüoptionen verwendet.

Das System ist standardmäßig so eingestellt, dass eingehende Anrufe nach drei Ruftönen (ca. 15 Sekunden) angenommen werden.



### 2.3.4 STEUERUNG DES SYSTEMS ÜBER SMS-BEFEHLE

SMS-Befehle können individuelle Bereiche und programmierbare Ausgänge so wie die Bereichstasten der Tastatur steuern. Die Art der Textnachricht zur Steuerung des Systems ist: CODE\_COMMAND. Die eigentlichen Befehle (COMMAND) sind vordefiniert (SCHARF / UNSCHARF) mit einem zusätzlichen numerischen Parameter, der einen bestimmten Bereich identifiziert.

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

Ein Beispiel eines verwendeten SMS-Befehls zur Scharfschaltung der Bereiche 2 und 4.

#### CODE\_SET\_2\_4

Die Befehle zur Steuerung der programmierbaren Ausgänge können von einem Errichter programmiert werden. Zum Beispiel können Sie JALOUSIE RUNTER als Ihren Befehl zum Herunterlassen der Jalousien Ihrer Fenster verwenden. Das System kann auch so konfiguriert werden, dass kein Code vor einem Befehl benötigt wird. In solch einem Fall wird der Befehl einfach automatisch identifiziert, wenn das System die Telefonnummer des Benutzers erkennt, von der die SMS gesendet wurde. Die Konfiguration wird von einem Errichter vorgenommen.



### 2.3.5 STEUERUNG DES SYSTEMS PER FERNZUGRIFF MIT EINEM COMPUTER (J-LINK)

Das System JABLOTRON 100+ kann auch per Fernzugriff mit einem Computer mit der installierten Software J-Link gesteuert werden.

Sie kann im Abschnitt „Downloads“ von der Website [www.jablotron.com](http://www.jablotron.com) heruntergeladen werden und befindet sich auch auf der SD-Karte der Zentrale. Der Anmeldecode des Sicherheitssystems (ein 15-stelliger Code) und die Telefonnummer seiner SIM-Karte wird für den ersten Verbindungsaufbau per Fernzugriff benötigt. Der Fernzugriff wird durch einen Klick auf „Internet“ im Hauptmenü gestartet.

Nach dem Verbindungsaufbau mit der Zentrale erfolgt die Steuerung genauso wie über ein USB-Kabel.



### 2.3.6 STEUERUNG DER PROGRAMMIERBAREN AUSGÄNGE (PG)

#### 2.3.6.1 TASTATURBEREICH

Ein PG-Ausgang schaltet sich durch Drücken der rechten Bereichstaste ein und durch Drücken der linken Taste aus. Wenn der Ausgang als Impulsausgang konfiguriert ist, wird er entsprechend der voreingestellten Zeit ausgeschaltet.

Ein PG-Ausgang kann aber muss nicht im Ereignisspeicher der Zentrale gespeichert werden. Die Konfiguration nimmt ein Errichter vor.

Eine Berechtigung wird / wird nicht je nach Systemkonfiguration gefordert.

#### 2.3.6.2 BERECHTIGUNG ÜBER DIE TASTATUR EINES BENUTZERS

Ein PG-Ausgang kann nur über die Benutzerberechtigung (Eingabe eines Codes oder Verwendung eines RFID-Tags) aktiviert werden. Der PG-Ausgang muss so konfiguriert werden, dass er von einer bestimmten Tastatur aus aktiviert wird.

#### 2.3.6.3 VOM MENÜ EINER TASTATUR MIT EINEM LCD-DISPLAY

Nach der Benutzerberechtigung kann der programmierbare Ausgang vom Menü der Tastatur mit einem LCD-Display gesteuert werden. Der Benutzer hat, abhängig von den Berechtigungen des Benutzers, Zugriff auf die programmierbaren Ausgänge.

Steuerung vom Menü der Tastatur:

- ▶ Berechtigen Sie sich über einen gültigen Code oder einen RFID-Chip.
- ▶ Rufen Sie das Menü über ENTER auf.
- ▶ PG-Steuerung → ENTER.



- ▶ Wählen Sie die gewünschte PG-Gruppe mit den Pfeilen aus (1–32), (33–64), (65–96), (97–128) → ENTER.
- ▶ Wählen Sie den gewünschten PG mit den Pfeilen aus → ENTER.
- ▶ Wiederholtes Drücken von ENTER ändert den PG-Status (ein aktiver PG wird durch eine Zahl in einem schwarzen Rechteck **2** angezeigt).
- ▶ Drücken Sie ESC, um das Menü zu verlassen.

### 2.3.6.4 FERNSTEUERUNG

Durch Drücken einer zugewiesenen Taste einer Fernsteuerung. Bidirektionale Fernsteuerungen bestätigen die Aktivierung eines PG-Ausgangs mit einer LED-Anzeige.

### 2.3.6.5 MyJABLOTRON-APP FÜR SMARTPHONES

Durch das Tippen auf EIN/AUS in der Registerkarte Automatisierung (PG).

### 2.3.6.6 WEBBASIERTE MyJABLOTRON-SCHNITTSTELLE

Durch Fernbedienung Klicken auf EIN/AUS in der Registerkarte Automatisierung (PG).

### 2.3.6.7 EINWÄHLEN

Jede im System gespeicherte Telefonnummer (jeder Benutzer kann eine Telefonnummer haben) kann einen PG über die Einwahl steuern (d.h. ohne einen Anruf aufzubauen). Die Einwahl besteht darin, die Telefonnummer der im Sicherheitssystem verwendeten SIM-Karte zu wählen und aufzulegen, bevor das System den Anruf entgegennimmt. Das System nimmt den Anruf standardmäßig nach dem dritten Klingeln (ca. 15 Sekunden) entgegen.

### 2.2.6.8 SMS-NACHRICHT

Die Versendung einer SMS kann einen individuellen PG ein-/ausschalten. Je nach Systemkonfiguration ist die Berechtigung nicht erforderlich.

Beispiel: CODE\_CONFIGURED TEXT

## 3. SPERRUNG/ DEAKTIVIERUNG IM SYSTEM

### 3.1 SPERREN VON BENUTZERN

Jeder Benutzer kann vorübergehend gesperrt werden (z.B. wenn er seine Karte/Tag verliert oder sein Zugriffscode bekannt wurde). Wenn der Zugriff eines Benutzers gesperrt ist, wird sein ID-Code oder Karte/Tag nicht mehr vom System akzeptiert. Der Benutzer erhält zudem keine Warnungen per SMS oder Sprachmeldungen mehr.

Nur der Systemadministrator oder Errichter kann einen Benutzer sperren. Ein Weg zur Sperrung der Zugriffsrechte erfolgt über die Auswahl Einstellungen / Benutzer / Benutzer / Bypass und dann „JA“ auf der LCD-Tastatur. Eine weitere Option ist die lokale oder ferngesteuerte Sperrung über J-Link, bei der man auf den Benutzer in der Spalte zur Sperrung des Benutzers in Einstellungen / Benutzer / Benutzer klickt.

Ein gesperrter (deaktivierter) Benutzer wird mit einem roten Kreis gekennzeichnet, bis die Sperrung aufgehoben wird.

### 3.2 SPERREN VON MELDERN

Ein Melder kann in ähnlicher Form gesperrt werden wie ein Benutzer. Ein Melder wird dann gesperrt, wenn seine Aktivierung vorübergehend nicht benötigt wird (z.B. ein Bewegungsmelder in einem Raum, in dem sich Haustiere befinden oder der Ton einer Sirene). Das System führt Diagnosen der Sabotagekontakte durch und sendet Dienstereignisse, jedoch ist die Alarmfunktion deaktiviert.

Nur der Systemadministrator oder Errichter kann den Melder sperren. Dies wird durch die Auswahl von Einstellungen / Geräte / Bypass und der Auswahl „Ja“ auf der LCD-Tastatur erreicht. Eine weitere Option ist die Verwendung von J-Link, indem man auf die Spalte des Melders in Einstellungen / Diagnosen / Deaktiviert klickt. Ein gesperrter Melder wird mit einem gelben Kreis gekennzeichnet, bis die Sperrung über den selben Weg wieder aufgehoben wird. Ein Gerät kann auch über die Smartphone-App MyJABLOTRON gesperrt werden.



### 3.3 ZEITSCHALTUHR

Um automatisierte und zeitlich geplante Ereignisse vorübergehend im System zu deaktivieren, kann ein Timer deaktiviert werden. Die Deaktivierung eines zeitlich geplanten Ereignisses (z.B. Unscharfschaltung der Nachtüberwachung zu einer bestimmten Uhrzeit) verhindert die Ausführung des Ereignisses (z.B. während des Urlaubs).

Ein Timer kann lokal oder ferngesteuert über J-Link deaktiviert werden, indem man auf die Spalte des Bereichs in Einstellungen / Kalender / Gesperrt klickt. Ein deaktivierter Timer wird mit einem roten Kreis gekennzeichnet, bis die Sperrung über den selben Weg wieder aufgehoben wird.

## 4. ANPASSUNG DES SYSTEMS

### 4.1 ÄNDERUNG DES ZUGRIFFSCODES EINES BENUTZERS

Wenn das System ohne vorangestellte Codes eingerichtet wird, können nur der Systemadministrator und der Errichter die Sicherheitscodes ändern. Der Systemadministrator kann die Änderungen vom Menü der LCD-Tastatur, J-Link und der Smartphone-App MyJABLOTRON aus vornehmen. Der Code kann nach der Berechtigung durch die Auswahl Einstellungen / Benutzer / Code geändert werden. Um einen neuen Code einzugeben, muss der Bearbeitungsmodus eingegeben werden (der Code beginnt zu blinken), indem man Enter drückt, den neuen Code eingibt und dies durch Drücken von Enter bestätigt. Nachdem die Änderungen abgeschlossen wurden, müssen sie durch Speichern bestätigt werden, wenn Sie das System mit „Einstellungen speichern?“ dazu auffordert.

Wenn das System mit vorangestellten Codes eingerichtet wird, können einzelne Benutzer ihren Code über das LCD-Menü auf der Tastatur ändern.

### 4.2 ÄNDERN, LÖSCHEN ODER HINZUFÜGEN VON RFID-KARTEN / TAGS / CHIP

Wenn das System ohne vorangestellte Codes eingerichtet wird, können nur der Systemadministrator und der Errichter die Sicherheitscodes ändern. Der Systemadministrator kann die Änderungen vom Menü der LCD-Tastatur, J-Link und der Smartphone-App MyJABLOTRON aus vornehmen. Der Code kann nach der Berechtigung durch die Auswahl Einstellungen / Benutzer / Benutzer / Code geändert werden. Um einen neuen Code einzugeben, muss der Bearbeitungsmodus eingegeben werden (der Code beginnt zu blinken), indem man Enter drückt, den neuen Code eingibt und dies durch Drücken von Enter bestätigt. Nachdem die Änderungen abgeschlossen wurden, müssen sie durch Speichern bestätigt werden, wenn Sie das System mit „Einstellungen speichern?“ dazu auffordert.

Wenn das System mit vorangestellten Codes eingerichtet wird, können einzelne Benutzer ihren Code über das LCD-Menü auf der Tastatur ändern.

### 4.3 ÄNDERN VON BENUTZERNAMEN ODER TELEFONNUMMERN

Wenn das System mit voreingestelltem Code eingerichtet wird, können die Benutzer ihre Telefonnummern oder ihren Namen über das LCD-Menü auf der Tastatur ändern, hinzufügen oder löschen. Dies kann nach der Berechtigung durchgeführt werden, indem man auf Einstellungen / Benutzer / Benutzer / Telefon klickt. Um die Änderungen vorzunehmen, muss der Bearbeitungsmodus eingegeben werden, indem man Enter drückt. Nach Durchführung der Änderungen, müssen diese mit Enter bestätigt werden. Um eine Telefonnummer zu löschen, geben Sie „0“ in das Telefonfeld ein. Nachdem die Änderungen abgeschlossen wurden, müssen sie durch Speichern bestätigt werden, wenn Sie das System mit „Einstellungen speichern?“ dazu auffordert.

Der Systemadministrator und der Errichter können die Telefonnummer eines Benutzers oder einen Benutzernamen über das LCD-Menü auf der Tastatur hinzufügen, ändern oder löschen.

### 4.4 HINZUFÜGEN/ LÖSCHEN EINES BENUTZERS

Nur der Systemadministrator oder Errichter kann neue Benutzer zum System hinzufügen (oder diese löschen). Neue Benutzer können zum System über J-Link oder im Falle des Errichters über F-Link hinzugefügt (oder gelöscht) werden.



Bei der Erstellung eines neuen Benutzers müssen ihm Zugriffsrechte zugewiesen werden, sowie Bereiche, die der Benutzer verwenden und programmierbare Ausgänge, die er steuern kann. Es wird auch festgelegt, welche Art der Berechtigung benötigt wird.

## 4.5 EINRICHTEN VON KALENDEREREIGNISSEN

Es ist möglich, Kalenderereignisse (Unscharfschaltung / Scharfschaltung / teilweise Scharfschaltung / Steuern oder Sperren von PG-Ausgängen) zu konfigurieren. Die Kalenderereignisse können über J-Link in dem Reiter Kalender eingerichtet werden.

Es kann für jedes Kalenderereignis, jede Aktion, jeden Bereich oder PG-Ausgang und Ereignis eine Zeit festgelegt werden. Der Tag kann über den Wochentag, den Monat oder das Jahr festgelegt werden. Für einen ausgewählten Tag können Sie bis zu 4 Mal eine Aktion durchführen oder in regelmäßigen Intervallen wiederholen.

Somit können Kalenderereignisse nicht nur für die Bereichssteuerung, sondern auch für die Steuerung verschiedener Technologien im Objekt unter Verwendung von PG-Ausgängen angepasst werden.

Information	Service / PG	Area	PG Output	Start Date	End Date	Frequency	Action	Repeat	Priority	Status
>	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
1	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
2	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
3	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
4	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
5	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
6	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
7	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
8	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
9	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
10	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
11	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
12	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
13	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
14	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
15	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
16	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
17	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
18	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
19	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
20	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO
21	NO	NO	MON, Tues	1 to 31	1 to 31	NO	NO	NO	NO	NO

## 5. EREIGNISVERLAUF

Das Sicherheitssystem speichert alle durchgeführten Aktionen und Ereignisse (Scharfschaltung, Unscharfschaltung, Alarme, Fehler, Nachrichten, die an Benutzer und AESs versendet werden) auf der Micro-SD-Karte im System der Zentrale. Jeder Eintrag erfolgt mit Datum, Zeit (Start und Ende) und der Quelle (Grund / Ursache) des Ereignisses.

**Die verschiedenen Wege, um den Ereignisverlauf des Sicherheitssystems zu durchsuchen:**

### 5.1 MIT DER LCD-TASTATUR

Für den Zugriff auf den Ereignisverlauf mit der Tastatur ist die Benutzerberechtigung erforderlich. Nach der Berechtigung werden die verfügbaren Optionen (abhängig von den Rechten des Benutzers) angezeigt, indem man den Ereignisspeicher auswählt. Die Einträge können unter Verwendung der Pfeiltasten eingesehen werden.

### 5.2 MIT J-LINK UND EINEM COMPUTER

Der Systemspeicher kann mit J-Link durchsucht werden. Ereignisse können von der Zentrale in kleinen (ca. 1200 Ereignisse) oder größeren (ca. 4000 Ereignisse) Pakete heruntergeladen werden. Die Ereignisse können detailliert gefiltert oder zur besseren Orientierung farblich dargestellt oder in einen Ordner auf den Computer geladen werden.

### 5.3 LOGIN BEI MyJABLOTRON (WEBBASIERT/SMARTPHONE)

Alle Systemereignisse können nach dem Login bei MyJABLOTRON, der webbasierten oder Smartphone-Schnittstelle, eingesehen werden. Das Konto zeigt den Verlauf in der Reihe an, die den Rechten des Benutzers entspricht.

- ▶ Es ist wichtig, regelmäßige und rechtzeitige Wartungschecks durchführen zu lassen, um eine zuverlässige Funktionstüchtigkeit des Systems zu gewährleisten. Die normalen Wartungsarbeiten werden von einem Installationsunternehmen mindestens einmal pro Jahr bei der periodischen Wartungsinspektion durchgeführt.
- ▶ Die Wartung durch den Benutzer besteht hauptsächlich darin, die einzelnen Geräte sauber zu halten. Der ADMINISTRATOR des Systems kann das System in den WARTUNGS-Modus schalten, um die Melder öffnen zu können (Batteriewechsel) oder sie von der Installation zu löschen. Kontaktieren Sie das Installationsunternehmen, um den WARTUNGS-Modus einzustellen. Wenn das System als Systemprofil „EN 50131-1, Stufe 2“ konfiguriert ist, ist der WARTUNGS-Modus nicht verfügbar.
- ▶ Das System kann über J-Link oder vom Menü einer Tastatur mit einem LCD-Display in den Wartungsmodus geschaltet werden. Nach der Berechtigung kann ein „Wartungsmodus“ mit der Auswahl der Bereiche, in denen die Wartung erforderlich ist, ausgewählt werden. Im Wartungsmodus werden keine Alarmer in den ausgewählten Bereichen ausgelöst. Dies betrifft auch das Öffnen und Löschen von Meldern von der Installation.
- ▶ Der Wartungsmodus wird durch eine grün blinkende Aktivierungstaste (alle 2 Sekunden 2-mal aufblincken) und durch die zwei Bereichstasten des Bereichs angezeigt, die ausgehen.
- ▶ Mit den Geräten muss sorgfältig umgegangen werden, damit die Gehäuse und der Mechanismus des Melders nicht beschädigt werden.
- ▶ Die Abdeckung wird normalerweise mit einer Lasche befestigt, die mit einem kleinen Werkzeug (z.B. Schraubenzieher) leicht in das Gehäuse des Melders gedrückt wird, damit die Abdeckung abgenommen werden kann. In einigen Fällen ist die Lasche mit einer kleinen Sicherungsschraube gesichert, die zuerst abgeschraubt werden muss.
- ▶ Wenn Sie die Batterien im Melder wechseln, ersetzen Sie immer alle Batterien im Melder zur selben Zeit (verwenden Sie Batterien desselben Typs und desselben Herstellers).
- ▶ Für einige Geräte ist eine Prüfung erforderlich (z.B. Feuermelder/ Rauchwarnmelder). Für weitere Informationen kontaktieren Sie bitte Ihren Errichter.

PARAMETER	JA-103K	JA-107K		
<b>Stromzufuhr der Zentrale</b>	~ 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		
<b>Backup-Batterie</b>	12 V; 2.6 Ah (Blei-Gel)	12 V; 7 to 18 Ah (Blei-Gel)		
<b>Maximale Ladezeit der Batterie</b>	72 Std.			
<b>BUS-Spannung (rot - schwarz)</b>	12,0 bis 13,8V			
<b>Maximaler Dauerstromverbrauch von der Zentrale</b>	1000 mA	2000 mA permanent 3000 mA für 60 Minuten (max. 2000 mA für ein BUS)		
<b>Max. Dauerstromverbrauch für einen Backup von 12 Stunden</b>	Ohne GSM Wähl- & Übertragungs-gerät	LAN – AUS 115 mA LAN – EIN 88 mA	Gilt für 18 Ah Backup-Batterie	
			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
<b>Maximale Geräteanzahl</b>	50	230		
<b>LAN-Kommunikator</b>	ETHERNET SCHNITTSTELLE, 10/100BASE-T			
<b>Abmessungen (mm)</b>	268 x 225 x 83 mm	357 x 297 x 105 mm		
<b>Gewicht mit / ohne AKU</b>	1844 g/970 g	7027 g/1809 g		
<b>Reaktion auf eine ungültige Codeeingabe</b>	Alarm nach 10 falschen Codeeingaben			
<b>Ereignisspeicher</b>	Ca. 7 Millionen letzte Ereignisse, einschließlich Datum und Zeit			
<b>Netzteil</b>	Typ A (gemäß EN 50131-6)			
<b>GSM-Kommunikator</b>	850 / 900 / 1800 / 1900 MHz			
<b>GSM-Kommunikator 3G</b>	850 / 900 / 1800 / 1900 / 2100 MHz			
<b>Klassifizierung</b>	Sicherheitsstufe 2 / Umgebungsklasse II (gemäß EN 50131-1)			
<b>Betriebsumgebung</b>	Allgemeine Innenbereiche			
<b>Betriebstemperaturbereich</b>	-10 °C bis +40 °C			
<b>Durchschnittliche Betriebsfeuchtigkeit</b>	75 % RH, nicht kondensierend			
<b>Entspricht</b>	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			
<b>Funkfrequenz (with the JA 11xR module)</b>	868.1 MHz, JABLOTRON Protokoll			
<b>Funkemissionen</b>	ETSI EN 300 220-1,-2 (Modul R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)			
<b>EMC</b>	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7			
<b>Sicherheitskonformität</b>	EN 62368-1+A11			
<b>Betriebsbedingungen</b>	ERC REC 70-03			
<b>Zertifizierungsstelle</b>	Trezor Test s.r.o. (no. 3025)			
<b>Rufnummererkennung (CLIP)</b>	ETSI EN 300 089			



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](http://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.

### BUS-/Drahtlose Geräte

Der wichtigste Teil des Sicherheitssystems ist die Zentrale. Sie kann auf zwei Arten mit allen Geräten kommunizieren: unter Verwendung des BUS, d.h. Verwendung von Datenkabeln innerhalb der überwachten Räumlichkeiten oder Teilen davon; oder drahtlos über Funk. BUS-Geräte werden über die Zentrale mit Strom versorgt. Drahtlose Geräte benötigen Batterien, deren Lebensdauer von der Nutzungsintensität abhängt. Einige der drahtlosen Geräte werden mit 230 V vom Stromnetz versorgt.

### Segmente

Dies ist der Steuer- und Signalisierungsteil des Zugriffsmoduls (Tastatur). Der Bereich enthält eine Beschreibung seiner Funktion und hat zwei beleuchtete Tasten - eine grüne auf der linken und eine rote oder gelbe auf der rechten Seite. Ein Bereich dient dazu, einen Teil des Systems einfach und übersichtlich zu bedienen und gleichzeitig seinen Status über die farblichen Anzeigen anzuzeigen (grün bei unscharf, rot bei scharf und gelb bei teilweise scharf). Die Anzahl der Bereiche und deren Funktionen werden vom Errichter festgelegt.

### RFID-Karte/Tag/Chip

Die RFID-Karte / Tag ermöglicht dem Benutzer, das System zu bedienen, und wird für die kontaktlose Berechtigung verwendet, indem die Karte / das Tag einfach auf dem Tastaturleser platziert wird. Es ersetzt oder ergänzt numerische Code-Einträge. Die RFID-Karte kann in einer Brieftasche mitgeführt werden. Das RFID-Tag kann an einem Schlüsselring befestigt werden.

### Sicherungsbereich

Das Alarmsystem kann in mehrere kleinere, unabhängig voneinander funktionierende Teile, sogenannte Bereiche, unterteilt werden. Jeder Bereich kann seine zugeordneten Melder, Tastaturen sowie Sirenen, Benutzer und ihre Telefonnummern haben. Es kann bis zu 15 Bereiche pro System geben.

### Programmierbare PG-Ausgänge

Das Sicherheitssystem kann zum Ein- / Ausschalten oder Steuern anderer elektrischer Geräte oder Installationen verwendet werden. Dies geschieht über die Verwendung von programmierbaren Ausgängen, die vom Benutzer gesteuert werden können (per SMS, über die Tastatur usw.) oder die aufgrund des Systemstatus (Alarmstatus, Fehler usw.) automatisiert werden können.

### Gebäudeautomatisierung

Neben einem Einbruchalarmsystem bietet der JABLOTRON 100+ eine Reihe weiterer Funktionen. Zu den beliebtesten Funktionen gehören: elektrische Türschlösser, automatische Lichtschalter mit Bewegungsmeldern und die Fernsteuerung von Geräten (elektrische Heizung, Garagentore, Tore, Zugangsschranken usw.).

### Panik-, Überfall- & Geiselnahme Alarm

Wenn ein Benutzer in Gefahr ist und dringend Hilfe benötigt, kann der Panikalarm ausgelöst werden. Der Panikalarm kann als ein bestimmter Bereich auf der Tastatur, ein spezieller Code, als Notfalltaste oder eine bestimmte Tastenkombination auf einem Schlüsselanhänger eingestellt werden. Wenn eine Verbindung zu einem Sicherheitsdienst besteht, wird durch das Auslösen des Panikalarms sofort eine Reaktion (Fahrzeugversand) ausgelöst, die nicht telefonisch abgebrochen werden kann.

### Sicherheitsdienst, AlarmEmpfangsStelle AES, NotrufServiceLeitstelle NSL

Ein Alarmempfangszentrum und ein ständig besetzter Sicherheitsdienst (24/7/365) können sofort auf die von den bewachten Räumlichkeiten erhaltenen Informationen mit entsprechenden Maßnahmen reagieren oder die internen Regeln befolgen.









**M-DEJA100+-USER**  
**[www.jablotron.com](http://www.jablotron.com)**