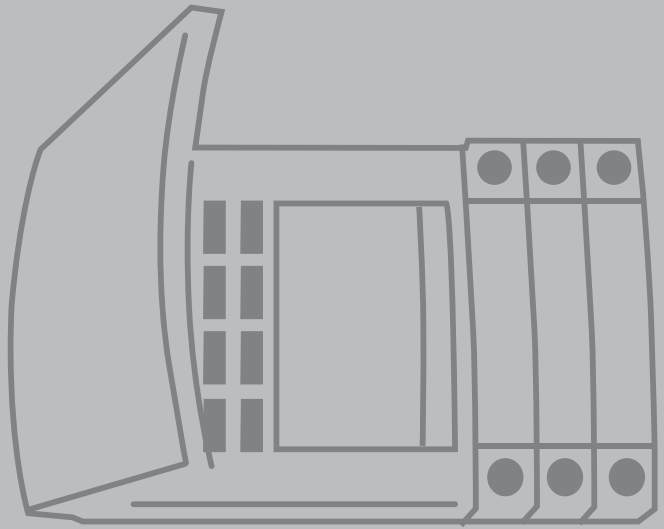


JABLOTRON 100+

OBSAH

PRAVIDELNÁ ÚDRŽBA SYSTÉMU

:: Pro spolehlivou funkci celého systému je potřeba dodržovat intervaly pravidelné údržby. Většinu požadavků na údržbu provádí servisní fi rma v rámci pravidelných servisních prohlídek min. 1x ročně.

:: Uživatelská údržba spočívá zejména v udržování jednotlivých periferií v čistotě. Pro možnost otevření detektorů (výměna baterií) nebo v případě potřeby jejich odejmutí z montáže může SPRÁVCE přepnout systém do režimu ÚDRŽBA. Požadavek na režim ÚDRŽBA konzultujte s montážní fi rmou. Při nastavení systému splňujícího normu EN-50131-1, stupeň zabezpečení 2, není režim ÚDRŽBA dostupný.

:: Přepnutí lze provést pomocí SW J-Link nebo z menu klávesnice s LCD displejem. Po autorizaci lze v menu vybrat položku „Režim údržba“ a poté vybrat sekce, ve kterých je požadována. V tomto režimu nebudou vyhlašovány žádné poplachy z vybraných sekcí, a to i v případě otevření nebo sejmutí detektorů z montáže.

:: Režim údržba je signalizován zeleným poblikáváním aktivačního tlačítka (2 bliknutí každé 2 sekundy) a zhasnutím obou tlačítek na segmentu dané sekce.

:: Při manipulaci s periferiemi je nutné dbát zvýšené opatrnosti, aby nedošlo k poškození plastů a mechanismů zajišťujících funkci detektorů.

:: Kryt je zpravidla zajištěn pružnou západkou, kterou je nutno lehce vtlačit malým nástrojem (šroubovákem) do těla detektoru a poté odklopit kryt. V některých případech je tato západka zajištěna malým vrutem, který je nutno napřed vyšroubovat.

:: Baterie v detektoru vyměňte vždy všechny najednou (použijte baterie stejného typu a od stejného výrobce).

:: Některé periferie mohou vyžadovat testování (např. požární detektory). Více informací si vyžádejte u servisního technika).

1. ÚVOD

Kvalitní zabezpečovací systém vyžaduje v první řadě odbornou montáž, ale pro zajištění skutečného bezpečí se neobejde bez nepřetržitého dohledu a profesionálního zásahu při poplachu. Využijte proto spolu s montáží systému JABLOTRON 100+ nabízenou unikátní celkovou ochranu připojením hlídaného objektu k Bezpečnostnímu centru.

Tato služba je první 3 měsíce poskytována zcela zdarma!

Systém JABLOTRON 100+ je navržen až pro 600 uživatelů a rozdělit jej lze až na 15 samostatných sekcí. Umožňuje použít až 230 periferií a nabízí až 128 programovatelných výstupů pro multifunkční využití, např. pro domácí automatizaci.

2. OVLÁDÁNÍ SYSTÉMU JABLOTRON 100+

Ovládání zabezpečovacího systému lze provádět různými způsoby. Pro odjištění je vždy nutné provést autorizaci, což je identifikace uživatele. Systém rozpozná, který uživatel ho právě používá, a dovolí mu tak dle jeho přednastaveného oprávnění ovládat právě takové části, k nimž má povolený přístup. Pro zajištění lze vybrat mezi způsoby zajišťování s autorizací nebo bez autorizace. V případě nastavení zajišťování bez autorizace se není nutné autorizovat a zajistit lze pouze stiskem daného pravého tlačítka segmentu přístupového modulu. Každý krok s identifikací data, času a jména uživatele se zapisuje do paměti systému. Tyto informace jsou dostupné po neomezenou dobu. Pouhou autorizací uživatele lze také zrušit vzniklý poplach (vypnout sirény) v těch částech systému, na které má uživatel práva k ovládání, nedojde tím však automaticky k odjištění (není-li změněno výchozí nastavení).

Poznámka: dle nainstalované konfigurace a nastavení systému nemusí být všechny dále popisované způsoby a volby dostupné. Nastavení systému konzultujte se svým servisním technikem.

Uživatelé a jejich oprávnění

OPRÁVNĚNÍ KÓDU	POPIS
Kód PCO	Má absolutně nejvyšší oprávnění pro změny nastavení chování systému a jako výhradní kód může odblokovat systém po poplachu. Může otevírat servisní režim. Má přístup do všech záložek nastavení včetně záložky komunikace na PCO, do které může přístup Servisnímu technikovi (kódu Servis) omezit. Pokud nemá parametrem „Správce omezuje Servis a PCO“ omezeno ovládání, smí ovládat všechny použité sekce v systému i programovatelné výstupy. Může vytvářet další Správce i ostatní uživatele s nižším oprávněním a přidělovat jim kódy, RFID čipy a karty. Má oprávnění mazat paměť poplachu i sabotáží. **Počet kódů PCO není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Servisní kód (Servis)	Může otevírat servisní režim a provádět změny nastavení chování systému. Má přístup do všech záložek nastavení včetně záložky komunikace na PCO, pokud ho nemá omezen nadřazeným technikem PCO. Pokud nemá parametrem „Správce omezuje Servis a PCO“ omezeno ovládání, smí ovládat všechny použité sekce v systému i programovatelné výstupy. Může vytvářet uživatele s oprávněním PCO, Servis, Správce i ostatní uživatele s nižším oprávněním a přidělovat jim kódy, RFID čipy a karty. Má oprávnění mazat paměť poplachu i sabotáží. Počet kódů Servis není v rámci volných pozic v systému omezen. **Z výroby je nastaven kód 1010. Uživatel Servis je vždy na pozici 0 a nelze jej smazat.**
Kód Správce (hlavní)	Má vždy plný přístup do všech sekcí a oprávnění ovládat všechny programovatelné výstupy. Může vytvářet další Správce a ostatní kódy s nižším oprávněním a udělovat jim oprávnění pro sekce a programovatelné výstupy, přidělovat jim kódy, RFID čipy a karty. Má oprávnění mazat paměť poplachu. Kód hlavního Správce může být v systému jen jeden a nelze smazat. Při zapnuté funkci „Omezení přístupu kódu servis a PCO“ musí být použita autorizace kódu Správce jako potvrzující souhlas k přístupu oprávnění Servis nebo PCO. Z výroby je nastaven kód 1234. **Uživatel Správce je vždy na pozici 1 a nelze jej smazat.**
Kód Správce (další)	Má hlavním Správcem přidělený přístup do vybraných sekcí, pro které může vytvářet další uživatele se stejným nebo nižším oprávněním pro ovládání sekcí a programovatelných výstupů, přidělovat jim kódy, RFID čipy a karty. Má oprávnění mazat paměť poplachu do přidělených sekcí. Při zapnuté funkci „Omezení přístupu kódu servis a PCO“ musí být použita autorizace kódu Správce jako potvrzující souhlas k přístupu oprávnění Servis nebo PCO. **Počet kódů dalšího Správce není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Kód Uživatel	Má Správcem přidělené oprávnění k ovládání vybraných sekcí a programovatelných výstupů. Může si sám přidělovat a mazat RFID čipy a karty a měnit vlastní telefonní číslo. Při nastavení systému s prefixem si může svůj kód uživatele měnit. Má oprávnění mazat paměť poplachu do přidělených sekcí. Vybraní uživatelé mohou mít časově omezený přístup do sekcí. **Počet kódů Uživatel není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**

OPRÁVNĚNÍ KÓDU	POPIS
Kód Zajisti	Kód opravňující přidělenou sekci v systému pouze zajistit. Oprávnění na ovládání programovatelných výstupů s autorizací se vztahuje na zapínání i vypínání. Uživatel tohoto kódu nemá oprávnění si kód sám měnit, ani nemůže mazat paměť poplachu. **Počet kódů Zajisti není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Kód Pouze PG	Kód opravňující pouze ovládat programovatelné výstupy s autorizací. Oprávnění se vztahuje jak na zapínání, tak i na vypínání. Uživatel tohoto kódu nemá oprávnění si kód sám měnit. **Počet kódů Pouze PG není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Kód Tíseň	Kód opravňující pouze vyhlásit událost „Tíseň“. Uživatel tohoto kódu nemá oprávnění si kód sám měnit, ani nemůže mazat paměť poplachu. **Počet kódů Tíseň není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Kód Guard	Kód určený pro bezpečnostní službu. Toto oprávnění umožňuje celý systém zajistit. Odjistit ho však celý může pouze během poplachu, nebo po jeho skončení, dokud je signalizována paměť poplachu. Uživatel tohoto kódu nemá oprávnění si kód sám měnit, ani nemůže mazat paměť poplachu. **Počet kódů Guard není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**
Kód Odblokování	Kód určený výhradně pro odblokování systému po Zablokování poplachem. Uživatel tohoto kódu nemá oprávnění ovládat systém, sám si kód měnit, ani nemůže mazat paměť poplachu. **Počet kódů Odblokování není v rámci volných pozic v systému omezen a z výroby není žádný nastaven.**

Bezpečnost přístupových kódů, bezdotykových RFID prvků a dálkových ovladačů:

Ústředna zabezpečovacího systému umožňuje každému uživateli přidělit jeden 4, 6 nebo 8 místný kód a až dva RFID čipy pro jeho autorizaci v systému. Autorizace uživatele je požadována při každé manipulaci s přístupovým modulem, hlasovým menu, počítačem nebo webovou či mobilní aplikací. Délka kódu ovlivňuje počet možných kombinací, a tím i bezpečnost kódu.

Parametry ústředny	4-MÍSTNÝ	6-MÍSTNÝ	8-MÍSTNÝ
Při zapnutém parametru **„Kódy s prefixem“**	= 10^4 = (10.000)	= 10^6 = (1.000.000)	= 10^8 = (100.000.000)
Při vypnutých parametrech **„Kódy s prefixem“** a **„Ovládání pod nátlakem“**	= 10^4 – (Počet použitých uživatelů v systému – 1)	= 10^6 – (Počet použitých uživatelů v systému – 1)	= 10^8 – (Počet použitých uživatelů v systému – 1)
Při vypnutém parametru **„Kódy s prefixem“** a zapnutém parametru **„Ovládání pod nátlakem“**	≤ 10^4 – ((Počet použitých uživatelů v systému – 1) * 3)	≤ 10^6 – ((Počet použitých uživatelů v systému – 1) * 3)	≤ 10^8 – ((Počet použitých uživatelů v systému – 1) * 3)
Při použitím jen **RFID karty** s rozsahem 14 znaků (6 pevných + 8 variabilních)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)

Parametry ústředny	4-MÍSTNÝ	6-MÍSTNÝ	8-MÍSTNÝ
Při zapnutých parametrech **„Kódy s prefixem“** a **„Potvrzení RFID karty kódem“**	= (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)
Při vypnutém parametru **„Kódy s prefixem“** a zapnutém **„Potvrzení RFID karty kódem“**	= 10^8 * (10^4 – (Počet použitých uživatelů v systému – 1))	= 10^8 * (10^6 – (Počet použitých uživatelů v systému – 1))	= 10^8 * (10^8 – (Počet použitých uživatelů v systému – 1))

Řešením jak bezpečnost proti dohledání platného kódu zvýšit je např.:

:: volbou vícemístného číselného kódu (6 nebo 8 místné kódy)
:: vyšší volbou způsobu autorizace, např. „Potvrzení karty kódem“ nebo „Dvojitou“ autorizací

Způsoby ovládání systému JABLOTRON 100+

Lokálně:

:: Systémovým přístupovým modulem (klávesnicí)
:: Dálkovým ovladačem
:: Počítačem přes USB kabel s použitím programu J-Link

Vzdáleně:

:: Aplikací MyJABLOTRON v chytrém mobilním telefonu
:: Počítačem přes webové rozhraní MyJABLOTRON
:: Telefonem přes hlasové menu
:: Telefonem SMS zprávou
:: Počítačem přes internet s použitím programu J-Link
:: Prozvoněním z autorizovaného telefonního čísla (pouze pro ovládání programovatelných výstupů)

Pro ovládání systému JABLOTRON 100+ mohou být použity různé varianty klávesnic, které umožňují nejen ovládat, ale zároveň přehledně signalizovat stav jednotlivých částí. Vlastní ovládání (odjištění nebo zajištění systému a další funkce automatizace) se provádí pomocí dvoutlačítkových segmentů. Tlačítka segmentu jsou výstižně popsána a barevně prosvětlena (logikou semaforu) tak, aby byl na první pohled zřetelně indikován jejich stav. Segment lze použít též pro signalizaci stavu (např. otevřená garážová vrata) nebo ovládání různých zařízení automatizace (např. topení či žaluzie). Maximální počet segmentů je 20 na jednu klávesnici. Segment může být použit také pro přivolání pomoci v nouzi (zdravotní nebo tísňový poplach).

2.1. LOKÁLNÍ OVLÁDÁNÍ

SVÍTÍ ZELENĚ
ODJIŠTĚNO | VYPNUTO
BLIKÁ ZELENĚ
PŘÍCHOD

BLIKÁ ČERVENĚ
POPLACH | PAMĚŤ POPLACHU
SVÍTÍ ZELENĚ
VŠE V POŘÁDKU
BLIKÁ ZELENĚ
OVLÁDEJTE
BLIKÁ ZELENĚ 2x ZA 2s
ÚDRŽBA
SVÍTÍ ŽLUTĚ
PORUCHA
BLIKÁ ŽLUTĚ
NEÚSPĚŠNÉ ZAJIŠTĚNÍ

SVÍTÍ ČERVENĚ
ZAJIŠTĚNO | ZAPNUTO
BLIKÁ ČERVENĚ
POPLACH |
PROBĚHL POPLACH

SVÍTÍ ŽLUTĚ
ZAJIŠTĚNO ČÁSTEČNĚ

ČTEČKA KARET |
KLÁVESNICE

Typy modulů a jejich kombinace 100+

Čtečka bezdotykových RFID karet

umožňuje ovládat systém pomocí segmentů s autorizací uživatele výhradně bezdotykovým způsobem (RFID čipem nebo RFID kartou)

Klávesnice se čtečkou

systém je ovládán pomocí segmentů s autorizací uživatele buď zadáním číselného kódu či bezdotykovým způsobem (RFID čipem nebo RFID kartou), případně kombinací obou způsobů pro vyšší bezpečnost

Klávesnice s displejem a čtečkou

systém lze ovládat pomocí segmentů s autorizací uživatele buď zadáním číselného kódu či bezdotykovým způsobem (RFID čipem nebo RFID kartou), případně kombinací obou způsobu pro vyšší bezpečnost, nebo také autorizací a výběrem možností nabízených z menu LCD displeje přístupového modulu.

Při odjišťování systému pomocí tlačítek

na segmentech je vždy vyžadována autorizace uživatele. Pro zajišťování sekcí a ovládání automatizace pomocí tlačítek na segmentech je autorizace uživatele pro každý segment volitelná.

Autorizace

se provádí zadáním kódu nebo přiložením čipové karty (či přívěsku s RFID čipem) přidělených v systému konkrétnímu uživateli. Každý uživatel může mít maximálně jeden číselný kód a dva RFID čipy (ať už v podobě karet či přívěsků).

Doporučené bezdotykové čipy: JABLOTRON 100+, Oasis, případně jiné čipy pracující na 125 kHz EM. Je-li od alarmu vyžadována zvýšená bezpečnost ovládání, je možné nastavit potvrzovanou autorizaci s použitím čipů i kódů (volitelná funkce). Chce-li uživatel ovládat více segmentů najednou, po autorizaci stiskne postupně segmenty požadovaných sekcí. Lze tak např. současně zajistit dům i odjistit garáž. Při zapnuté funkci „kódy s prefixem" může být kód pro autorizaci na klávesnici maximálně jedenáctimístný. Skládá se z tzv. prefixu (jednomístné až třímístného číslo), oddělovací hvězdičky a kódu (4, 6, 8 místného – dle nastavení) (např. 123*1234 nebo 1*1234). Každý uživatel může sám libovolně měnit svůj kód za prefixem, přičemž změna kódu se provádí pomocí klávesnice s LCD displejem, softwarem J-Link či z aplikace MyJABLOTRON.

Při zapnuté funkci „kódy s prefixem" lze jednotlivým uživatelům povolit změnu jejich kódu. Pokud prefix není vyžadován, změnu kódů může provádět pouze Správce.

2.1.2. AUTORIZACE ZADÁNÍM KÓDU NA KLAVESNICE

Autorizace kódem uživatele se provádí zadáním platného kódu na číselníku klávesnice nebo RFID čipem.

V systému je možné používat 4, 6 nebo 8 místné kódy.

Systém lze nastavit pro používání kódu s prefixem nebo bez prefixu (výchozí nastavení). Pro systémy s větším počtem uživatelů lze prefix zapnout. O změnu typu kódu požádejte servisního technika.

Kód bez prefixu se zadává ve formátu: kkkk

kde:

kkkk je dle nastavení 4, 6 nebo 8 místný kód, povolené kódy jsou 0000 až 99999999

Z výroby má ústředna nastaven kód Správce: **1234; 123456; 12345678;**

Kód s prefixem se zadává ve formátu: ppp*kkkk

kde:

ppp je pořadové číslo (pozice 0 až 600) uživatele (tzv. prefix)

* je oddělovač (klávesa *)

kkkk je kód (dle počtu nastavených pozic 4, 6 nebo 8 místný, povolené kódy jsou 0000 až 99999999

Z výroby má ústředna nastaven kód Správce: **1*1234; 1*123456; 1*12345678;**

UPOZORNĚNÍ: kód hlavního správce má prefix **1**

hlavní servisní kód má prefix **0**

O změnu typu kódu požádejte servisního technika.

Struktura a popis vnitřního menu klávesnice s LCD displejem

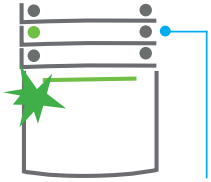
Autorizace kódem nebo čipem správce nebo uživatele

ZRUŠ VAROVNOU INDIKACI	Umožňuje zrušit indikaci poplachu/ neúspěšné zajištění na všech sekcích, pro které má uživatel oprávnění.
OVLÁDÁNÍ SEKCE	Umožňuje ovládat sekce systému, pro které má uživatel oprávnění, a které jsou povolené ve vnitřním nastavení.
OVLÁDÁNÍ PG	Umožňuje ovládat PG výstupy, pro které má uživatel oprávnění a které jsou povoleny ve vnitřním nastavení.
PAMĚŤ UDÁLOSTÍ	Umožňuje procházet události v paměti s detaily.
BRÁNÍ V ZAJIŠTĚNÍ	Nabízí přehled detektorů bránících v zajištění, pokud je tato volba dle nastavení ústředny.
PORUCHY V SYSTÉMU	Zobrazuje přehled detektorů hlásících poruchu ze sekcí, pro které má uživatel oprávnění.
BLOKOVANÉ DETEKTORY	Zobrazuje přehled blokovaných detektorů ze sekcí, pro které má uživatel oprávnění.
STAV SYSTÉMU	Nabízí přehled o stavu systému (akt. detektory, poruchy, sabotáže, vybité baterie, blokování apod.).
NASTAVENÍ	Umožňuje editaci uživatelů a periferií (pouze při odpojeném USB).
NASTAVENÍ DISPLEJE	Umožňuje měnit intenzitu podsvícení a kontrast displeje.
REŽIM ÚDRŽBA	Umožňuje Správci přepnout jemu přiřazené sekce do režimu Údržba.

2.1.2.1. ZAJIŠTĚNÍ

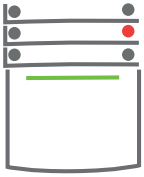
1. Autorizovat se na klávesnici

Svítí tlačítka sekcí, které lze ovládat a zeleně bliká prosvětlené indikační tlačítko na klávesnici.



2. Stisknout pravé tlačítko

(které nesvítí) pro zajištění požadované sekce. Je možné postupně zajistit více sekcí. Prodleva mezi volbami sekcí však nesmí být delší než 2 sekundy.



3. Povel se provede

klávesnice akusticky indikuje čas pro odchod. Daná sekce je tímto zajištěna, pouze detektory s reakcí „Zpožděná“ po dobu odchodového zpoždění umožňují opuštění střeženého prostoru. Segment zajištěné sekce svítí červeně.

Pokud jsou při zajištění některé stavové detektory aktivní (např. otevřené okno), systém se zachová (na základě nastavené konfigurace) jedním z následujících způsobů:

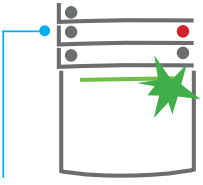
:: Detektory budou střežit automaticky až po jejich zklidnění
:: Systém upozorní po dobu 8 sekund blikáním červeného tlačítka segmentu, že jsou v systému aktivní detektory, pak se zajistí (výchozí nastavení).
:: Zajistit sekci s aktivními detektory lze opakovaným stiskem pravého tlačítka segmentu. Uživatel tak potvrdí záměr zajistit s aktivní periferií (např. otevřené okno). V opačném případě nedojde k zajištění sekce s aktivním detektorem.
:: Aktivní detektor zabrání zajištění sekce. Tento stav je signalizován blikáním červeného tlačítka segmentu. Na klávesnici s LCD displejem lze v menu vyčíst periferie bránící v zajištění.

Neúspěšné zajištění je indikováno žlutým blikáním indikačního tlačítka (nutno zapnout funkci „Neúspěšné zajištění). Požadované nastavení chování systému konzultujte se servisním technikem.

2.1.2.2. ODJIŠTĚNÍ

1. Po vstupu do objektu

(aktivace detektoru s reakcí „Zpožděná“) systém začne signalizovat příchodové zpoždění trvalým pískáním a blikáním zeleného tlačítka segmentu sekce, ve které probíhá příchodové zpoždění.

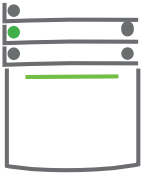


Autorizovat se na klávesnici

– rozbliká se zelené indikační tlačítko na klávesnici.

2. Stisknout levá tlačítka

na segmentech pro sekce, které chceme odjistit.



3. Povel se provede,

segmenty trvale zeleně indikují odjištění daných sekcí.

Poznámka: Je-li zapnuta volba „Autorizace odjistí sekci s probíhajícím příchodovým zpožděním“, tak pouhá autorizace odjistí sekci, ve které probíhá příchodové zpoždění. *Požadované nastavení chování systému konzultujte se servisním technikem.*

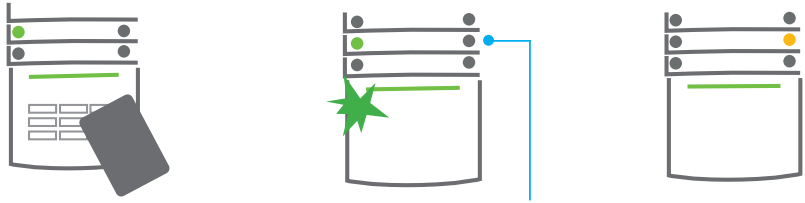
2.1.2.3. ODJIŠTĚNÍ POD NÁTLAKEM

Odjištění pod nátlakem je odjištění ve speciálním režimu, kdy se systém zdánlivě pouze odjistí, avšak zároveň je vyvolán tichý tísňový poplach, který je reportován nastaveným uživatelům (včetně PCO). Odjištění pod nátlakem se provede tak, že se k poslednímu číslu platného kódu přičte číslo 1.

Příklad pro kódy s perifexem: Platný kód: 2*9999 Kód pro odjištění pod nátlakem: 2*9990

Příklad pro kódy bez perifexu: Platný kód: *9999 Kód pro odjištění pod nátlakem: 9990

2.1.2.4. ČÁSTEČNÉ ZAJIŠTĚNÍ



1. Autorizovat se na klávesnici

(zadáním kódu nebo přiložením čipu, případně karty). Rozbliká se zelené prosvětlené indikační tlačítko.

2. Stisknout pravé tlačítko

segmentu příslušné sekce.

3. Povel se provede,

segment trvale žlutě indikuje částečné zajištění dané sekce.

V systému lze nastavit i částečné zajištění, které umožní hlídat jen pomocí vybraných detektorů v sekci.

Příklad: Přes noc je možné nechat zajištěná pouze okna a dveře, zatímco pohybové detektory uvnitř prostoru nereagují.

Pokud chcete celkově zajistit objekt, v němž je umožněno částečné zajištění, je nutné tlačítko pro celkové zajištění stisknout dvakrát. Po prvním stisku tlačítko svítí žlutě, po druhém červeně.

Je-li systém částečně zajištěn (svítí žlutě), pro přepnutí do celkového zajištění je nutné po autorizaci stisknout žluté tlačítko. Po stisku bude systém zajištěn celkově a tlačítko změní barvu na červenou.

2.1.2.5. PŘERUŠENÍ PROBÍHAJÍCÍHO POPLACHU

1. Autorizovat

se na klávesnici (zadáním kódu nebo přiložením čipu).

2. Stisknout

levé tlačítko segmentu sekce, ve které probíhá poplach.

3. Provedeno

odjištění a ztišení sirén. Zeleně svítící tlačítko signalizuje odjištění příslušné sekce. Červené tlačítko blikáním indikuje paměť poplachu.

4. Autorizovat

se a znovu stisknout zelené tlačítko pro zrušení indikace paměti poplachu.

5. Provedeno,

segment trvalým svitem zeleného tlačítka indikuje odjištěnou sekci.

Probíhající poplach je na klávesnici signalizován rychlým blikáním červeného tlačítka segmentu a prosvětleného indikačního tlačítka. Pro zrušení poplachu je nutné se autorizovat na klávesnici. Sekce zůstává nadále zajištěná, rychlé červené blikání na segmentu signalizuje informaci o proběhlém poplachu. Signalizace přetrvává i po odjištění.

V případě signalizace proběhlého poplachu ve Vaší nepřítomnosti vyhledejte v historii událostí zdroj poplachu a buďte při kontrole objektu ostražití nebo vyčkejte příjezdu bezpečnostní agentury (je-li váš systém připojen k PCO).

Indikace proběhlého poplachu na segmentu zůstává do dalšího zajištění, případně ji lze ukončit zopakováním odjištění. U klávesnic s LCD s displejem je možno světelnou signalizaci o proběhlém poplachu zrušit v menu Hlavní nabídka – „Zrušit varovnou indikaci".

Indikaci proběhlého sabotážního poplachu může ukončit pouze Servisní technik nebo Správce.

Poznámka: V nastavení splňující normu EN-50131-1, stupeň zabezpečení 2. je vždy nutné se nejdříve autorizovat a poté provést požadovanou akci.

Při zrušení poplachu dálkovým ovladačem dojde zároveň k odjištění příslušné sekce.

2.1.2.6. OVLÁDÁNÍ SEKCÍ Z MENU KLÁVESNICE S LCD DISPLEJEM

Na klávesnici s LCD displejem jsou v levém horním rohu displeje zobrazeny stavy sekcí. Plně zajištěná sekce je vyobrazena číslem sekce v plném obdélníku 2, částečně zajištěná číslem v rámečku 4.

Postup ovládání z menu klávesnice:

:: Autorizace platným kódem nebo čipem.
:: Vstup do menu stiskem klávesy ENTER.
:: Ovládání sekcí → ENTER.
:: Pomocí šipek vybrat požadovanou sekci.
:: Opakovaným stiskem klávesy ENTER se mění stav sekce částečné zajištění / zajištění / odjištění.
:: Po ukončení ovládání opuštění menu klávesou ESC.

2.1.3. OVLÁDÁNÍ KLÁVESNICÍ JA-110E, JA-150E

Stav jednotlivých sekcí je indikován stavovými indikátory A, B, C, D nad LCD displejem a funkčními tlačítky. Vlastní ovládání (odjištění nebo zajištění systému a další funkce automatizace) se provádí pomocí funkčních tlačítek. Funkční tlačítka sekcí a stavové indikátory (A, B, C, D) jsou barevně prosvětleny tak, aby byl na první pohled zřetelně indikován stav sekcí.

:: ZELENÁ – odjištěno :: ŽLUTÁ – částečně zajištěno :: ČERVENÁ – zajištěno

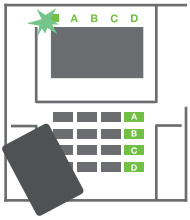
Autorizace se provádí zadáním kódu na klávesnici nebo přiložením RFID karty (nebo RFID přívěsku) přidělené v systému konkrétnímu uživateli. Chce-li uživatel ovládat více sekcí najednou, po autorizaci stiskne postupně funkční tlačítka požadovaných sekcí. Lze tak s platností jedné autorizace ovládat všechny sekce (např. zajistit dům a odjistit garáž).

Struktura a popis vnitřního menu klávesnice s LCD displejem

Autorizace kódem nebo čipem správce nebo uživatele

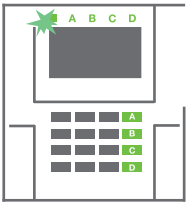
ZRUŠ VAROVNOU INDIKACI	Umožňuje zrušit indikaci poplachu/ neúspěšné zajištění na všech sekcích, pro které má uživatel oprávnění.
OVLÁDÁNÍ SEKCE	Umožňuje ovládat sekce systému, pro které má uživatel oprávnění, a které jsou povolené ve vnitřním nastavení.
OVLÁDÁNÍ PG	Umožňuje ovládat PG výstupy, pro které má uživatel oprávnění a které jsou povoleny ve vnitřním nastavení.
PAMĚŤ UDÁLOSTÍ	Umožňuje procházet události v paměti s detaily.
BRÁNÍ V ZAJIŠTĚNÍ	Nabízí přehled detektorů bránících v zajištění, pokud je tato volba dle nastavení ústředny.
PORUCHY V SYSTÉMU	Zobrazuje přehled detektorů hlásících poruchu ze sekcí, pro které má uživatel oprávnění.
BLOKOVANÉ DETEKTORY	Zobrazuje přehled blokovaných detektorů ze sekcí, pro které má uživatel oprávnění.
STAV SYSTÉMU	Nabízí přehled o stavu systému (akt. detektory, poruchy, sabotáže, vybité baterie, blokování apod.).
NASTAVENÍ	Umožňuje editaci uživatelů a periferií (pouze při odpojeném USB).
NASTAVENÍ DISPLEJE	Umožňuje měnit intenzitu podsvícení a kontrast displeje.
REŽIM ÚDRŽBA	Umožňuje Správci přepnout jemu přiřazené sekce do režimu Údržba.

2.1.3.1. ZAJIŠTĚNÍ



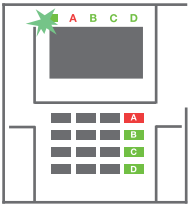
1. Autorizovat se na klávesnici

Svítí tlačítka sekcí A, B, C, D, ke kterým máte oprávnění, a zeleně bliká systémový indikátor na klávesnici.



2. Stisknout funkční tlačítko pro zajištění požadované sekce

Je možné postupně zajistit více sekcí. Prodleva mezi volbami sekcí však nesmí být delší než 2 sekundy.nesmí být delší než 2 sekundy.



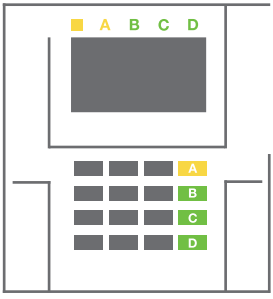
3. Povel se provede

klávesnice akusticky indikuje čas pro odchod. Daná sekce je tímto zajištěna, pouze detektory s reakcí „Zpožděná" po dobu odchodového zpoždění umožňují opuštění střeženého prostoru. Stavový indikátor a funkční tlačítko zajištěné sekce svítí červeně.

:: Systém se zajistí, aktivní detektory budou automaticky blokovány *).
:: Systém upozorní 8 sekund červeným blikáním funkčního tlačítka, že jsou v systému aktivní detektory, pak se zajistí (aktivní detektory budou blokovány) *).
:: Zajistit sekci s aktivními detektory lze opakovaným stiskem funkčního tlačítka sekce. Uživatel tak musí potvrdit záměr zajistit s aktivní periferií (např. otevřené okno). V opačném případě nedojde k zajištění sekce s aktivním detektorem.
:: Aktivní detektor zabrání zajištění sekce. Tento stav je signalizován červeným blikáním funkčního tlačítka. Na LCD displeji lze v menu vyčíst periferie bránící v zajištění.

*) **UPOZORNĚNÍ**: Volby a) a b) nejsou podporovány pro konfiguraci EN 50131 st. zabezpečení 2 (nastavený profil ústředny).

Pokud v době odchodového zpoždění dojde k aktivaci detektoru s reakcí „OKAMŽITÁ" nebo po dočasování odchodového zpoždění zůstane aktivní detektor s reakcí „ZPOŽDĚNÁ", systém se znovu odjistí. Neúspěšné zajištění je indikováno žlutým blikáním systémového indikátoru, reportováno na ARC a signalizováno externí sirénou (platí pro stupeň zabezpečení 2).

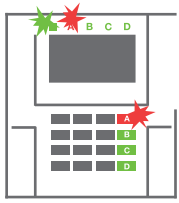


Pokud je systém nastaven na zajišťování bez autorizace, není nutné provést autorizaci, stačí stisknout funkční tlačítko dané sekce. Je také možné nastavit zajištění pouhou autorizací.

UPOZORNĚNÍ: Zajišťování bez autorizace snižuje maximální možnou klasifikaci systému na stupeň zabezpečení 1. Aplikace této volby je nutné zvážit s ohledem na všechna rizika spojená s použitím.

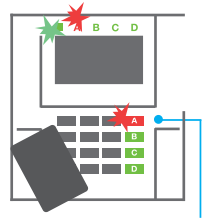
Požadované nastavení chování systému konzultujte s projektantem nebo servisním technikem.

2.1.3.2. ODJIŠTĚNÍ



1. Po vstupu do objektu

Svítí tlačítka sekcí A, B, C, D, ke kterým máte oprávnění, a zeleně bliká systémový indikátor na klávesnici.

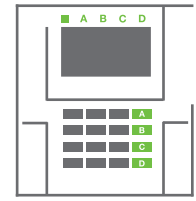


2. Autorizujte se na klávesnici

zeleně se rozbliká systémový indikátor.

3. Stiskněte funkční tlačítka

pro sekce, které chcete odjistit.



4. Povel se provede

klávesnice akusticky indikuje čas pro odchod. Daná sekce je tímto zajištěna, pouze detektory s reakcí „Zpožděná" po dobu odchodového zpoždění umožňují opuštění střeženého prostoru. Stavový indikátor a funkční tlačítko zajištěné sekce svítí červeně.

Poznámka: Je-li zapnuta volba „Autorizace odjistí sekci s probíhajícím příchodovým zpožděním" tak pouhá autorizace odjistí sekci, ve které probíhá příchodové zpoždění. Tuto volbu je nutné aplikovat obezřetně ve více sekčních systémech.

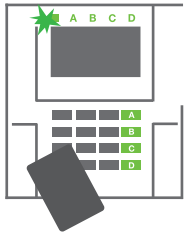
Požadované nastavení chování autorizačního panelu konzultujte se servisním technikem.

2.1.3.3. ČÁSTEČNÉ ZAJIŠTĚNÍ

UPOZORNĚNÍ: Tato volba je doplňkovou funkcí poplachového systému.

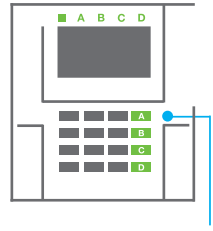
V systému lze nastavit i částečné zajištění, které umožní hlídat jen pomocí vybraných detektorů v sekci.

Příklad: přes noc je možné nechat zajištěná pouze okna a dveře, zatímco pohybové detektory uvnitř prostoru nereagují.



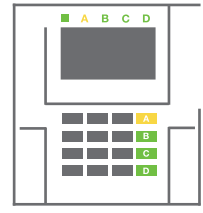
1. Autorizujte se na klávesnici

(zadáním kódu nebo přiložením RFID karty nebo přívěšku). Systémový indikátor se rozbliká zeleně.



2. Stiskněte funkční tlačítko

příslušné sekce.



3. Povel se provede

funkční tlačítko a stavový indikátor trvalým rozsvícením žlutě indikují částečné zajištění dané sekce.

Pokud chcete celkově zajistit objekt, v němž je umožněno částečné zajištění, stiskněte funkční tlačítko dlouze (2s) nebo stiskněte dvakrát. Po prvním stisku tlačítko svítí žlutě, po druhém červeně.

Pro plné zajištění ze stavu částečně zajištěno (funkční tlačítko svítí žlutě) po autorizaci dlouze stiskněte žluté tlačítko. Po stisku bude systém zajištěn celkově a tlačítko změní barvu na červenou.

Částečné zajištění lze nastavit tak, aby je bylo možné provést i bez autorizace.

Pro odjištění ze stavu částečně zajištěno po autorizaci stiskněte žluté tlačítko. Po stisku bude systém odjištěn a tlačítko změní barvu na zelenou.

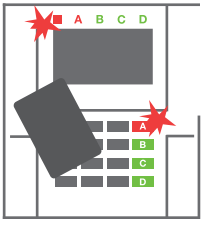
2.1.3.4. ODJIŠTĚNÍ POD NÁTLAKEM

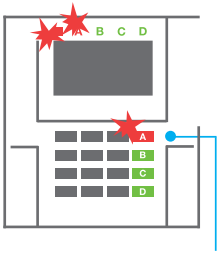
Odjištění pod nátlakem je odjištění ve speciálním režimu, kdy se systém zdánlivě pouze odjistí, avšak zároveň je vyvolán tichý tísňový poplach, který je reportován nastaveným uživatelům (včetně PCO).

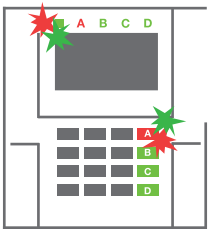
Odjištění pod nátlakem se provede tak, že se k poslednímu číslu platného kódu přičte číslo 1. Pro povolení této funkce kontaktujte servisního technika.

Příklad: Platný kód: 9999 Kód pro odjištění pod nátlakem: 9990

2.1.3.5. PŘERUŠENÍ PROBÍHAJÍCÍHO POPLACHU







1. **Autorizujte se na klávesnici**

(zadáním kódu nebo přiložením čipu).

2. **Stiskněte funkční tlačítko**

sekce, ve které probíhá poplach.

3. **Provede se odjištění a ztišení**

sirén. Rychlým střídavým blikáním zelená/ červená indikační tlačítkoa stavový indikátor signalizují paměť poplachu.

Probíhající poplach je na klávesnici signalizován rychlým červeným blikáním stavového indikátoru a prosvětleného funkčního tlačítka. Pro zrušení poplachu je nutné se autorizovat na klávesnici. Sekce zůstává nadále zajištěná, rychlé červené blikání funkčního tlačítka signalizuje informaci o proběhlém poplachu. Signalizace přetrvává i po odjištění.

UPOZORNĚNÍ: V případě signalizace proběhlého poplachu ve Vaší nepřítomnosti vždy vstupujte do objektu s maximální ostražitostí a vyhledejte v historii událostí zdroj poplachu. Buďte při kontrole objektu ostražití nebo vyčkejte příjezdu bezpečnostní agentury (je-li váš systém připojen k pultu centrální ochrany).

Indikace proběhlého poplachu na funkčním tlačítku zůstává do dalšího zajištění, případně ji lze zrušit v menu klávesnice: **Hlavní nabídka – Zrušit varovnou indikaci**. Indikaci proběhlého sabotážního poplachu může ukončit pouze Servisní technik a Správce.

Poznámka: Ve výchozím profilu nastavení je možné použít postup, kdy lze nejdříve stiskem funkčního tlačítka zvolit požadovanou akci a poté ji potvrdit autorizací na klávesnici.

Při zrušení poplachu dálkovým ovladačem dojde zároveň k odjištění příslušné sekce.

2.1.3. OVLÁDÁNÍ SYSTÉMU DÁLKOVÝM OVLADAČEM

Dálkové ovladače musí být do systému přiřazeny montážním technikem. Mohou být spojeny s konkrétními uživateli, což zamezí zasílání notifikačních SMS zpráv uživateli, který systém právě ovládá (je-li notifikace nastavena). Dálkové ovladače kontrolují a indikují stav své baterie a jsou vybaveny optickou i akustickou signalizací.

OBOUSMĚRNÝ OVLADAČ

Funkce tlačítek ovladačů je rozlišena vlisovanými symboly zámků. Zavřený zámek zajistí nastavené sekce, otevřený je odjistí. Správné provedení požadavku je potvrzeno kontrolkou, odjištění - zelená, zajištění – červená. Chyba komunikace (mimo dosah ústředny) je signalizována bliknutím žluté. Tlačítky se symboly plného a prázdného kolečka lze ovládat další sekce. Tlačítka dálkového ovladače lze nastavit i pro ovládání programovatelných výstupů, a to buď v režimu jedním tlačítkem zapni, druhým vypni nebo může mít každé tlačítko nastavenou samostatnou funkci v režimu pulsu nebo přepínání. Pro další funkce je možné nastavit i současný stisk páru tlačítek. Čtyř tlačítkový ovladač tak může mít až 6 nezávislých funkcí. nebo jeden programovatelný stavový výstup (např. zapínat a vypínat osvětlení), případně dva programovatelné výstupy (např. garážová vrata a dveřní zámek).

V případě nastavení systému na potvrzování při zajišťování s aktivní periferií (kap. 2.2.1), ovladač při požadavku na zajištění v případě aktivní periferie signalizuje nezajištění zelenou kontrolkou. Zajištění je nutné potvrdit dalším stiskem tlačítka zajištění. Zajištění sekce je poté potvrzeno červenou kontrolkou.

Tlačítka ovladače lze zablokovat proti neúmyslnému stisknutí (dětská pojistka). K vyslání povelu pak dojde až po opakovaném stisku tlačítka. Vybitá baterie v ovladači je signalizována akusticky (3x pípnutí) a opticky probliknutím žluté signálky po stisku tlačítka.

Informace o dalších možnostech nastavení dálkových ovladačů si vyžádejte u servisního technika.

JEDNOSMĚRNÝ OVLADAČ

Jednosměrné ovladače při stisku tlačítka vyšlou ovládací signál bez zpětné kontroly. Vyslání signálu je potvrzeno krátkým svitem červené kontrolky a případně pípnutím.

2.2. VZDÁLENÉ OVLÁDÁNÍ

Nevyšší komfort pro vzdálené ovládání a správu systému poskytuje služba MyJABLOTRON. MyJABLOTRON je unikátní služba, která umožňuje on-line přístup k zařízením z produkce společnosti JABLOTRON. Je určena pro koncové uživatele k dohledu nad zařízeními a k jejich ovládání. Je možné ji využívat buď jako Aplikaci v chytrých mobilních telefonech nebo jako webovou aplikaci.

Uživateli zabezpečovacího systému JABLOTRON služba umožňuje:

:: zjistit aktuální stav systému
:: zajistit/odjistit systém či jeho část
:: ovládat programovatelné výstupy
:: prohlížet historii událostí
:: zasílat oznámení na vybrané kontakty SMS, e-mailem, PUSH notifikace
:: pořizovat snímky z foto verifikačních zařízení a sledovat jejich historii v záložce fotogalerie či přímo v historii událostí
:: zjišťovat aktuální hodnoty detektorů teploty nebo spotřeby energií včetně zobrazení historie měření v grafech
:: a další užitečné funkce

Založení účtu ve službě MyJABLOTRON provádí Bezpečnostní centrum JABLOTRON SECURITY (systém musí obsahovat tzv. bezpečnostní SIM kartu) na základě požadavku instalačního technika či uživatele. Uživatelským jménem bude uživatelem zvolená e-mailová adresa, na kterou je také odesláno heslo pro první přihlášení. Heslo lze následně kdykoli změnit v nastavení účtu.

Podrobné informace jsou dostupné na Zákaznické lince JABLOTRON na čísle 800 800 522.

2.2.1. OVLÁDÁNÍ SYSTÉMU APLIKACÍ MyJABLOTRON V CHYTRÉM TELEFONU (SMATPHONE)

Po založení uživatelského účtu je možné zabezpečovací systém vzdáleně monitorovat a ovládat pomocí aplikace MyJABLOTRON pro chytré telefony se systémem Android nebo iOS.

2.2.2. OVLÁDÁNÍ SYSTÉMU WEBOVÝM ROZHRANÍM MyJABLOTRON

Systém JABLOTRON 100+ lze snadno a pohodlně ovládat pomocí počítače a internetu z webového rozhraní MyJABLOTRON, které je přístupné ze stránek **www.myjablotron.com**.

2.2.3. OVLÁDÁNÍ SYSTÉMU POMOCÍ HLASOVÉHO MENU

Systém lze ovládat z telefonu pomocí hlasového menu, které uživatele provede nabídkou funkcí v přednastaveném jazyce. Pro vstup do hlasového menu je nutné zavolat na telefonní číslo zabezpečovacího systému.

Přístup do hlasového menu může být povolen buď všem telefonním číslům bez omezení, nebo pouze kontaktům uloženým v systému. Dle nastavení může být vyžadována autorizace zadáním platného kódu uživatele na klávesnici telefonu. Po vstupu do menu systém sdělí aktuální stav všech sekcí přiřazených danému uživateli. Tyto sekce je následně možné ovládat klávesami telefonu dle nabídky, a to jak hromadně, tak jednotlivě.

Z výroby je systém nastaven na zvednutí hovoru po třetím zazvonění (cca 15 sekund vyzvánění).

2.2.4. OVLÁDÁNÍ SYSTÉMU SMS ZPRÁVOU

SMS povelem lze ovládat jednotlivé sekce i programovatelné výstupy, podobně jako z tlačítkových segmentů klávesnic. Tvar ovládací SMS zprávy je KÓD_POVEL. Text povelu pro ovládání sekcí je pevně přednastavený (ZAJISTI/ODJISTI), s případným doplněním číselného parametreu sekce. V rámci jedné SMS lze ovládat více sekcí najednou. V tomto případě se za povel přiřazují čísla sekcí.

Příklad: SMS povelu pro zajištění sekcí 2 a 4.

KÓD_ ZAJISTI_2_4

Texty povelů pro ovládání výstupů PG může nastavit montážní technik, např. ZALUZIE DOLU. Lze nastavit, že kód před povelem není vyžadován. V tom případě je uživatel identifikován podle telefonního čísla odesílatele SMS zprávy. Nastavení provede servisní technik.

2.2.5. OVLÁDÁNÍ SYSTÉMU POČÍTAČEM VZDÁLENĚ (J-LINK)

Systém JABLOTRON 100+ lze vzdáleně ovládat pomocí počítače s nainstalovaným programem J-Link. Stáhnout jej můžete z webových stránek **www.myjablotron.com**.

2.2.6. OVLÁDÁNÍ PROGRAMOVATELNÝCH VÝSTUPŮ PG

2.2.6.1. SEGMENTEM KLÁVESNICE

Stiskem pravého tlačítka se PG výstup zapne, stiskem levého se vypne. Pokud je výstup nastaven jako pulzní, je vypnutí automatické dle nastaveného času.

Ovládání PG může nebo nemusí být ukládáno do paměti událostí ústředny. Nastavení provede servisní technik.

Dle nastavení systému je/není pro ovládání výstupu PG vyžadována autorizace.

2.2.6.2. AUTORIZACE UŽIVATELE NA KLÁVESNICI

Pouhou autorizací uživatele na klávesnici (zadáním kódu nebo přiložením RFID čipů) lze zapnout PG výstup, který má nastavenu aktivaci právě z této klávesnice.

2.2.6.3. Z MENU KLÁVESNICE S LCD DISPLEJEM

Na klávesnici s LCD displejem lze po autorizaci v menu ovládat PG výstupy, pro které má autorizovaný uživatel oprávnění.

Postup ovládání z menu:

:: Autorizace platným kódem nebo čipem.
:: Vstup do menu stiskem klávesy ENTER.
:: Ovládání PG → ENTER.
:: Pomocí šipek vybrat požadovanou skupinu PG (1-32) (33-64) (65-96) (97-128) → ENTER.
:: Pomocí šipek vybrat požadované PG → ENTER.
:: Opakovaným stiskem klávesy ENTER se mění stav PG (aktivní PG výstup je na displeji signalizován číslem PG v plném obdélníku.
:: Po ukončení ovládání opuštění menu klávesou ESC.

2.2.6.4. DÁLKOVÝM OVLADAČEM

Stiskem přiřazeného tlačítka dálkového ovladače. U obousměrných dálkových ovladačů je sepnutí PG potvrzeno kontrolkou.

2.2.6.5. APLIKACI MyJABLOTRON V CHYTRÉM TELEFONU

Stisknutím segmentu daného PG v záložce PG výstupů.

2.2.6.6. WEBOVÝM ROZHRANÍM MyJABLOTRON

Kliknutím na Vypnuto/Zapnuto v záložce Automatizace (PG).

2.2.6.7. PROZVONĚNÍM

Pro každé telefonní číslo použité v systému (jeden uživatel může mít nastavené jedno tel. číslo) může být nastaveno ovládání jednoho PG výstupu pouhým prozvoněním bez navázání spojení. Prozvoněním se rozumí vytočení telefonního čísla SIM karty použité v zabezpečovacím systému a následné ukončení vyzvánění ještě před vyzvednutím hovoru systémem. Z výroby je systém nastaven na vyzvednutí hovoru po třetím zazvonění (cca 15 sekund vyzvánění).

2.2.6.8. SMS ZPRÁVOU

Zasláním SMS zprávy s nastaveným textem pro zapnutí/vypnutí daného PG výstupu. Dle nastavení je/není vyžadována autorizace.

Příklad: KÓD_NASTAVENÝ TEXT

3. BLOKOVÁNÍ V SYSTÉMU

3.1. BLOKOVÁNÍ UŽIVATELŮ

Pro krátkodobé znemožnění přístupu uživatele (např. z důvodu vyzrazení kódu či ztráty čipu) lze kteréhokoli uživatele tzv. zablokovat. Toto zablokování způsobí, že uživatel nebude mít přístup do systému, jeho kód ani čipy nebudou systémem akceptovány. Na telefonní číslo zablokovaného uživatele nebudou zasílány žádné SMS zprávy s reporty ani hlášení voláním.

Blokování uživatele smí provádět správce systému nebo servisní technik. Nastavit ho lze v menu klávesnice s LCD displejem následujícím postupem: Nastavení / Uživatelů / Uživatel / Blokování volbou "Ano". Dále je možné uživatele zablokovat lokálním nebo vzdáleným přístupem z programu J-Link kliknutím na uživatele ve sloupci Nastavení / Uživatelé / Vypnutí.

U blokovaného (vypnutého) uživatele se v programu až do zrušení blokování zobrazí symbol červeného puntíku.

3.2. BLOKOVÁNÍ DETEKTORŮ

Pro krátkodobé vypnutí funkce kteréhokoli detektoru lze použít stejný postup jako pro blokování uživatele. Blokování detektoru se provádí v případě, že není žádoucí jeho aktivace (např. detekování pohybu v místnosti, kde zůstává zvíře). Blokována je pouze poplachová funkce, sabotážní a servisní události jsou dále vyhodnocovány.

Zablokování smí provádět správce systému nebo servisní technik. Blokování detektoru lze nastavit v menu klávesnice s LCD displejem následujícím postupem: Nastavení / Periferií / Blokování volbou "Ano". Dále je možné detektory zablokovat z programu J-Link kliknutím na detektor ve sloupci Nastavení / Diagnostika / Vypnutí. U blokovaného detektoru se v programu zobrazí symbol žlutého puntíku, a to až do zrušení blokování, které se provádí stejným postupem. Blokovat periferii je možné i pomocí aplikace MyJABLOTRON pro chytré telefony.

3.3. VYPNUTÍ AKCE KALENDÁŘE

Slouží pro krátkodobé vypnutí automatické kalendářní akce v systému. Vypnutí automatické kalendářní akce (např. odjištění systému z nočního střežení v nastavený čas) způsobí, že se akce nebude vykonávat (např. při odjezdu na dovolenou).

Vypnutí lze provést lokálně nebo vzdáleně z programu J-Link kliknutím na sekci ve sloupci Nastavení / Kalendář / Vypnutí. U blokovaného řádku se zobrazí symbol červeného puntíku, a to až do zrušení vypnutí, které se provádí stejným postupem.

4. UŽIVATELSKÉ NASTAVENÍ SYSTÉMU

4.1. ZMĚNA PŘÍSTUPOVÉHO KÓDU UŽIVATELE

Pokud je systém nastaven na ovládání pomocí kódů bez prefixu, má oprávnění ke změně kódů výhradně správce systému a servisní technik. Správce systému může změny provádět nejen z menu klávesnice s LCD displejem, ale i prostřednictvím programu J-Link nebo z aplikace MyJABLOTRON pro chytré mobilní telefony. Změna kódu pomocí klávesnice s LCD displejem se provádí po autorizaci volbou Nastavení / Uživatelé / Uživatel / Kód. Pro vložení nového kódu je nutno položku editovat („rozblikat") stisknutím klávesy Enter, zadat nový kód a potvrdit klávesou Enter. Po ukončení provádění změn je nutné u dotazu "Zapsat Konfiguraci?" zvolit možnost "Uložit".

V případě, že je systém nastaven na ovládání pomocí kódů s prefixem, je možné povolit jednotlivým uživatelům měnit si svůj kód z menu klávesnice s LCD displejem. Změna, vymazání nebo přidání RFID čipu či karty uživatele.

Pokud je systém nastaven na ovládání pomocí kódů s prefixem, má každý uživatel možnost přidávat, měnit nebo mazat své RFID čipy nebo karty z menu klávesnice s LCD displejem. Tyto změny se provádí po autorizaci volbou Nastavení / Uživatelé / Uživatel / Přist.karta1 (nebo 2). Pro vložení nového RFID čipu nebo karty je nutno položku editovat („rozblikat“) stisknutím klávesy Enter a přiložit RFID čip nebo kartu ke čtecí části klávesnice (tj. před klávesy) nebo zadat výrobní číslo uvedené pod čárovým kódem a opět potvrdit klávesou Enter. Pro vymazání přístupové karty je potřeba zadat při editaci pole namísto výrobního čísla jednu nulu: “0”. Po ukončení provádění změn je nutné u dotazu “Zapsat Konfiguraci?” zvolit možnost “Uložit”.

Oprávnění přidávat, měnit a mazat RFID čipy a karty má i správce a servisní technik systému. Správce systému může změny provádět nejen z menu klávesnice s LCD displejem, ale i prostřednictvím programu J-Link.

4.2. ZMĚNA TELEFONNÍHO ČÍSLA ČI JMÉNA UŽIVATELE

Pokud je systém nastaven na ovládání pomocí kódů s prefixem, má každý uživatel možnost přidávat, měnit nebo mazat své telefonní číslo z menu na LCD klávesnici. Změny se provádějí po autorizaci volbou Nastavení / Uživatelé / Uživatel / Tel. číslo. Pro provedení změn je nutné položky editovat (rozblikat) stisknutím klávesy Enter, zadat nové údaje a opět potvrdit klávesou Enter. Pro vymazání telefonního čísla zadejte při editaci pole namísto telefonního čísla jednu nulu: “0”. Po ukončení provádění změn je nutné u dotazu “Zapsat Konfiguraci?” zvolit možnost “Uložit”.

Oprávnění přidávat, měnit a mazat telefonní čísla či měnit jména uživatelů má i správce a servisní technik systému. Správce systému může změny provádět nejen z menu klávesnice s LCD displejem, ale i prostřednictvím programu J-Link.

4.3. PŘIDÁNÍ NOVÉHO UŽIVATELE / SMAZÁNÍ UŽIVATELE

Pro vložení nového uživatele (smazání stávajícího uživatele) má oprávnění pouze správce systému, případně servisní technik. Nový uživatel může být do systému zaveden (stávající uživatel smazán) výhradně programem J-Link, v případě servisního technika programem F-Link.

Při zakládání musí mít nastavená oprávnění přístupu do jednotlivých sekcí a ovládání programovatelných výstupů s vyžadovanou autorizací.

4.4. NASTAVENÍ KALENDÁŘE

V systému lze nastavit kalendářní akce (odjištění / zajištění / částečné zajištění nebo ovládání, příp. blokování PG). Nastavení kalendářní akce se provádí v programu J-Link v záložce Kalendář.

Ke každé události lze nastavit akci, sekce nebo PG výstupy a čas události. Den lze definovat dnem v týdnu, měsíci nebo roce. V nastavený den je možné nastavit až 4 časy k provedení akce nebo lze nastavit opakování v pravidelných intervalech.

Kalendářní akce je tak možné variabilně přizpůsobit nejen pro ovládání sekcí, ale i pro řízení různých technologií v objektu pomocí PG výstupů.

5. HISTORIE UDÁLOSTÍ

Zabezpečovací systém ukládá veškeré chování a všechny události (zajištění, odjištění, poplachy, poruchy, reportování uživatelům i pultu centrální ochrany) do paměti ústředny na micro SD kartu. U všech události je vždy uvedeno datum a čas vzniku nebo ukončení a zdroj události (příčina nebo původ).

Prohlížet události je možné několika způsoby:

5.1. PROCHÁZENÍM UDÁLOSTÍ NA KLÁVESNICI S LCD DISPLEJEM

Pro přístup k událostem na klávesnici je nutná autorizace uživatele. Po autorizaci se v položce Paměť událostí zobrazí body dostupné dle příslušného oprávnění. Záznamy je možné procházet pomocí šipek.

5.2. VYČTENÍM UDÁLOSTÍ PROGRAMEM J-LINK V POČÍTAČI

Vyčtení paměti lze provést pomocí programu J-Link. Provádí se po částech, a to buď malých (cca 1.200 událostí), nebo větších (cca 4.000 událostí). Vyčtené události je možné detailně fi ltrovat, pro přehlednost barevně rozlišit a případně uložit do souboru na disk počítače.

5.3. PŘIHLÁŠENÍM DO MyJABLOTRON (NA WEBU NEBO V APLIKACI CHYTRÉHO TELEFONU)

Všechny události v systému jsou k dispozici ve webovém rozhraní MyJABLOTRON. Tyto údaje je možné číst po přihlášení do uživatelského účtu MyJABLOTRON. Účet respektuje zobrazení rozsahu historie podle nastavených oprávnění vlastníka účtu.

6. TECHNICKÉ PARAMETRY

PARAMETR	JA-103K		JA-107K	
Napájení ústředny	~ 110 – 230 V/50 – 60 Hz, max. 0,28 A s pojistkou F1,6 A/250 V, třída ochrany II		~ 110–230 V/50 – 60 Hz, max. 0,85 A s pojistkou F1,6 A/250 V, třída ochrany II	
Zálohovací akumulátor	12 V; 2,6 Ah (olověný gelový)		12 V; 7 až 18 Ah (olověný gelový)	
Maximální doba na dobití akumulátoru	48 h		48 h	
Napětí sběrnice (červený - černý)	12,0 až 13,8 V		12,0 az 13,8 V	
Max. trvalý odběr z ústředny	1000 mA		2000 mA trvale, 3000 mA po dobu 60 min (max. 2000 mA do jedné sběrnice)	
Max. trvalý odběr pro zálohování 12 hodin	JA-103K – akumulátor 2,6 Ah		JA-107K – akumulátor 18 Ah	
	Bez GSM komunikátoru	LAN – vypnuto: 115 mA LAN – zapnuto: 88 mA	Bez GSM komunikátoru	LAN – vypnuto: 1135 mA LAN – zapnuto: 1107 mA
	S GSM komunikátorem	LAN – vypnuto: 80 mA LAN – zapnuto: 53 mA	S GSM komunikátorem	LAN – vypnuto: 1100 mA LAN – zapnuto: 1072 mA
Max. trvalý odběr pro zálohování 24 hodin	Bez GSM komunikátoru	LAN – vypnuto: 21 mA	Bez GSM komunikátoru	LAN – vypnuto: 535 mA LAN – zapnuto: 499 mA
	S GSM komunikátorem	LAN – vypnuto: 17 mA	S GSM komunikátorem	LAN – vypnuto: 530 mA LAN – zapnuto: 494 mA
Max. počet periferií	50		230	
LAN komunikátor	Ethernet rozhraní 10/100 BASE		Ethernet rozhraní 10/100 BASE	

PARAMETR	JA-103K	JA-107K
Rozměry	268 x 225 x 83 mm	357 x 297 x 105 mm
Hmotnost s AKU/bez AKU	1844 g/970 g	7027 g/1809 g
Poplach chybným zadáním kódů	po 10 chybně zadaných kódech	
Paměť událostí	cca 7 milionů posledních událostí včetně data a času	
Typ napájecího zdroje	typ A dle ČSN EN 50131-6	
	T 031- V případě výpadku hlavního napájení je systém zálohován po dobu až 24 hodin. Zároveň je tato porucha reportována na PCO	
GSM komunikátor (2G)	850 / 900 / 1800 / 1900 MHz	
Třída prostředí	třída II (vnitřní všeobecné) dle ČSN EN 50131-1	
Stupeň zabezpečení	stupeň 2 dle ČSN EN 50131-1	
Průměrná provozní vlhkost	75 % RH, bez kondenzace	
Rozsah provozních teplot	-10 °C až +40 °C	
Splňuje	ČSN EN 50131-1 ed. 2+A1+A2, ČSN EN 50131-3, ČSN EN 50131-5-3+A1, ČSN EN 50131-6 ed. 2+A1, ČSN EN 50131-10, ČSN EN 50136-1, ČSN EN 50136-2, ČSN EN 50581	
Radiová pracovní frekvence (s modulem JA 11xR)	868,1 MHz	
Rádiové vyzařování	ČSN ETSI EN 300 220-1,-2 (modul R), ČSN ETSI EN 301 419-1, ČSN ETSI EN 301 511 (GSM)	
EMC	ČSN EN 50130-4 ed. 2+A1, ČSN EN 55032 ed. 2, ČSN ETSI EN 301 489-7	
Elektrická bezpečnost	ČSN EN 62368-1+A11	
Identifikace volajícího (CLIP)	ČSN ETSI EN 300 089	
Podmínky provozování	dle Všeobecného oprávnění ČTÚ č. VO-R/10, VO-R/1	
Certifikační orgán	Trezor Test s.r.o. (č. 3025)	

JABLOTRON ALARMS a.s. prohlašuje, že výrobky JA-103K a JA-107K jsou navrženy a vyrobeny ve shodě s harmonizačními právními předpisy Evropské unie: směrnice č. 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU (Nařízení vlády ČR č. 481/2012 Sb.), jsou-li použity dle jejich určení. Originál prohlášení o shodě je na www.jablotron.com v sekci Ke stažení.

Poznámka: Výrobky, ačkoliv neobsahují žádné škodlivé materiály, nevyhazujte do odpadků, ale předejte na sběrné místo elektronického odpadu. Podrobnější informace na www.jablotron.com v sekci Ke stažení.

TABLE OF CONTENTS

PERIODICAL MAINTENANCE

:: It is necessary to have regular and timely maintenance checks performed in order to secure reliable functioning of the system. Most of the maintenance is carried out by an installation company at least once a year during periodical maintenance inspections.

:: User maintenance consists mainly of keeping the individual devices clean. The ADMINISTRATOR of the system can switch se system to a MAINTENANCE mode in order to be able to open the detectors (change batteries) or to remove them from the installation. Consult the request to set the MAINTENANCE mode with the installation company. If the system is configured to the “EN 50131-1, grade 2” system profile, the MAINTENANCE mode is not available.

:: The system can be switched to the maintenance mode via the J-Link software or from the menu of the keypad with LCD display. After authorization a “Maintenance mode” can be selected with a selection of sections where the maintenance is needed. In the maintenance mode no alarms will be triggered in the selected sections, including opening or removing the detectors from the installation.

:: The maintenance mode is indicated by the activation button flashing green (2 flashes each 2 seconds) and by the two segment buttons of the particular section lighting off.

:: When handling with the devices a care must be taken to avoid damage to the plastic and mechanisms of the detectors.

:: The cover is usually secured with a tab that needs to me slightly pushed into the detector’s body with a small tool (e.g. screwdriver) and then the cover can be taken off. In some cases, the tab is secured with a small locking screw that must be unscrewed first.

:: When changing batteries in the detector, always replace all batteries in the particular detector at the same time (use batteries of the same type and from the same manufacturer).

:: Some devices may require testing (e.g. fi re detectors). For more information please contact your service technician.

1. INTRODUCTION

The JABLOTRON 100+ system is designed for up to 600 users and it can be divided into 15 individual sections. Up to 230 devices can be connected and the system offers up to 128 multi-purpose programmable outputs (e.g. home automation).

2. OPERATING THE JABLOTRON 100+ SYSTEM

The security system can be controlled in a number of different ways. To unset the alarm, authorization in the form of user identification is always required. The system detects the identity of the users and allows them to operate those parts of the system which they have been assigned to control. You can choose from different ways of setting with or without authorization. When Standard authorization type is used, you don't have to authorize yourself because it is possible to set the system just by pressing the right segment button on a keypad. The user name, date, and time are recorded and stored in the system memory every time the system is accessed. This information is available indefinitely. Any user can also cancel a triggered alarm (stop sirens from sounding) just by authorization in any part of the system (depending on their access rights). However, that does not automatically unset the system (unless the system's default setting is changed).

Note: Depending on the configuration of the installation and system settings, some of the options described below may not be available. Consult the configuration of the installation with your service technician.

Users and their access rights

CODE AUTHORIZATION	TYPE DESCRIPTION
ARC code	This code has the highest level of authorization to configure the system's behavior and is exclusively allowed to perform the system unblock after a triggered alarm. It can enter Service mode, access all tabs with options including ARC communication to which it can deny access to a Service technician (Service code). As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the ARC code can control all sections and PG outputs used in the system. This code enables to add more Administrators and other users with a lower level of authorization assign them with codes, RFID tags and cards. It also has a permission to erase alarm and tamper alarm memory. **The number of ARC codes is limited only by remaining capacity of the control panel and there is no code set by the factory defaults.**
Service code (Service)	This code can enter Service mode and configure the system's behavior. It has access to all tabs with options including ARC communication unless the access is limited by the ARC technician. As long as the "Administrator-restricted Service/ARC right" parameter remains unchecked, the Service code can control all sections and PG outputs used in the system. It can create users with ARC permission, other Service technicians, Administrators and other users with a lower level of authorization and assign them with access codes, RFID tags and cards. It also has a permission to erase alarm and tamper alarm memory. The number of Service codes is limited only by remaining capacity of the control panel. **By the factory defaults, the code is 1010. The Service user is always on position 0 in the control panel and it cannot be erased.**
Administrator code (Main)	This code has always full access to all sections and is authorized to control all PG outputs. The Administrator can create other Administrator and other codes with a lower level of authorization and assign them with access to sections and PG outputs, access codes, RFID chips and cards. This code has permission to erase the alarm memory. There can be only one main Administrator code which can't be erased. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized to confirm access for ARC and Service technicians. **By the factory defaults, the code is 1234. The main Administrator user is always on position 1 and it cannot be erased.**
Administrator code (Other)	This code has access to sections selected by the main Administrator to which the other Administrator can add new users with the same or lower level of authorization to control sections and PG outputs, assign them with access codes, RFID tags and cards. This code has permission to erase the alarm memory in assigned sections. When "Administrator-restricted Service/ARC right" is enabled, the administrator code must be authorized to confirm access for ARC and Service technicians. The number of Administrator codes (other) is limited only by remaining capacity of the control panel. **There is no code set by the factory defaults.**

CODE AUTHORIZATION	TYPE DESCRIPTION
User code	This code has access to sections and PG control rights assigned by an Administrator. Users can add/delete their RFID tags and access cards and change their own telephone numbers. Users can change their codes provided that the system uses Codes with prefixes. It has permission to erase the alarm memory in assigned sections. Selected users may have their access to sections limited by a schedule. **The number of User codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.**
Set code	This code is allowed only to set a designated section and is allowed to control (ON/OFF) PG outputs which require authorization. Users with this level of authorization are not allowed to change their code and are not allowed to erase the alarm memory. **The number of Set codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.**
PG only code	This code allows the user to control programmable outputs with authorization only. This applies to both switching on and off. Users with this level of authorization are not allowed to change their code and are not allowed to erase the alarm memory. **The number of PG only codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.**
Panic code	This code is allowed only to trigger Panic alarm. A user of this code is not allowed to change it or erase the alarm memory. **The number of Panic codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.**
Guard code	This is a code for a security agency. This level of authorization allows to set the whole system. However, the guard code can unset the system only during alarm or after it expired as long as the alarm memory is still active. A user of this code is not allowed to change it or erase the alarm memory. **The number of Guard codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults..**
Unblocking code	This code is designated to unblock the system after System blocking by alarm. A user of this code is not allowed to change it or erase the alarm memory. **The number of Unblocking codes is limited only by remaining capacity of the control panel. There is no code set by the factory defaults.**

The security of access codes, contactless RFID devices and remote controls:

A control panel enables each user to be assigned with one 4, 6 or 8-digit code and up to two RFID tags for system authorization. User authorization is required during each manipulation operation via keypad, voice menu, a computer, web or mobile apps. Code length affects number of possible combinations and therefore code security.

The number of code combinations depends on the configuration:

Control panel parameters	4 DIGITS	6 DIGITS	8 DIGITS
"Code with a prefix" enabled	= 10^4 = (10.000)	= 10^6 = (1.000.000)	= 10^8 = (100.000.000)
"Code with a prefix" and **"Duress access control"** both disabled	= 10^4 – (Number of users – 1)	= 10^6 – (Number of users – 1)	= 10^8 – (Number of users – 1)
"Code with a prefix" disabled; **"Duress access control"** enabled	≤ 10^4 – ((Number of users – 1) * 3)	≤ 10^6 – ((Number of users – 1) * 3)	≤ 10^8 – ((Number of users – 1) * 3)

Control panel parameters	4 DIGITS	6 DIGITS	8 DIGITS
Using only an **RFID card** with a range of 14 characters (6 constant + 8 variable)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
"Code with a prefix" and **"Card confirmation with a code"** both enabled	= (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 with a prefix" disabled; **"Cardconfirmation with a code"** enabled	= 10^8 * (10^4 – (Number of users – 1))	= 10^8 * (10^6 – (Number of users – 1))	= 10^8 * (10^8 – (Number of users – 1))

Ways to improve protection against guessing the valid code:

:: Using a code with more digits (6 or 8-digit codes),
:: More advanced types of authorization (such as "Card confirmation with a code" or "Double authorization").

Ways of operating the JABLOTRON 100+

On-site:

:: System keypad
:: System keyfob
:: Computer using a USB cable and the J-Link software

Remotely:

:: MyJABLOTRON smartphone application
:: Computer via the MyJABLOTRON web interface
:: Telephone using the voice menu
:: Telephone via SMS
:: Computer via the internet using the J-Link software
:: Dialling-in from an authorized telephone number (only for operating programmable outputs)

JABLOTRON 100+ system may be controlled by a variety of access modules which let you not just control but also display statuses of individual segments. The system can be operated directly (setting or unsetting the system and other automation functions) using two-button segments on the keypad. The segment buttons are clearly labelled and coloured (using traffi c light logic) so that each segment status is distinctly indicated. A segment can also be used to indicate a status (e.g. opened garage door) or to control various automated devices (for example heating or window blinds). The maximum number of segments is 20 for one access module. A segment can also be set up to call for help in an emergency (medical or panic alarm).

2.1. ON-SITE OPERATING

CONTINUOUS GREEN
UNSET | OFF
FLASHES GREEN
ENTRY DELAY

FLASHES RED
ALARM | ALARM MEMORY
CONTINUOUS GREEN
EVERYTHING OK
FLASHES GREEN
CONTROL
FLASHES GREEN 2x EACH 2 s
MAINTANENCE
CONTINUOUS YELLOW
FAULT
FLASHES YELLOW
UNSUCCESSFUL SETTING

CONTINUOUS RED
SET | ON
FLASHES RED
ALARM |
ALARM MEMORY
CONTINUOUS YELLOW
PARTIALLY SET

CARD READER | KEYPAD

The types of access modules and their combinations:

RFID card reader

allows control of the system using segments and user authorization using contactless method (RFID card/tag).

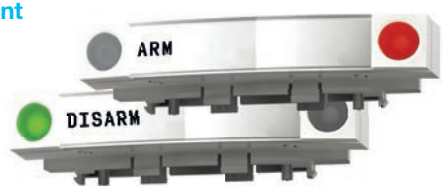
Keypad with a card reader

the user can control the system using segments and authorization, either by entering a code or the contactless method (RFID card/tag), or a combination of both for higher security.

Keypad with an LCD display and a card reader

the user can control the system using segments and authorization, using either a code, the contactless method (RFID card/tag), both code and card/tag for higher security, or by authorizing and using the options available on the keypad's LCD display.

When unsetting the alarm using the segment buttons,
user authorization is always required. When setting the alarm and controlling automated processes using the segment buttons, user authorization is optional for each segment.



Users can authorize
themselves by entering their assigned codes or using their RFID cards/tags. Each user can have one code and up to two RFID chips (cards or tags).

Recommended contactless chips: JABLOTRON 100+, Oasis or other third-party chips compatible with 125 kHz EM. If higher security is required the alarm system can be set up to use confirmed authorization using RFID chips and codes (optional). If the users want to control multiple segments simultaneously, they must authorize themselves and then press segments of the particular sections subsequently. This way the users can for example set the house and unset the garage within one single authorization. If the "Code with a prefix" parameter is enabled, the keypad authorization code can consist of up to eleven digits: a prefix (one to three digits), an asterisk * (which separates the prefix and main code), and a 4,6 or 8-digit code depending on configuration (for example: 123*12345678, or 1*12345678). All users can change their own codes which follow the prefix. The code can be changed from the keypad with the LCD display, the J-Link software or MyJABLOTRON app.

If the "Code with a prefix" parameter is enabled, the users can be allowed to change their code.
If the "Code with a prefix" parameter is disabled, the codes can be changed only by the Administrator.

2.1.2. KEYPAD CODE AUTHORIZATION

Authorization with a user code is done by typing a valid code into a keypad or with an RFID tag.

It is possible to use 4, 6 or 8-digit codes in the system.

The system can be configured to be used with prefix codes or without them (default settings). For alarm systems with a higher number of users the prefix can be enabled. To change this option, please contact the service technician of your alarm system.

Code without a prefix: CCCC

where:

cccc is a 4, 6 or 8-digit code, allowed codes are from 0000 to 99999999

Default control panel code Administrator: **1234; 123456; 12345678;**

Code with a prefix: nnn*cccc

where:

nnn is the prefix, which is the number of the user's position (position 0 to 600)

* is a separator (key *)

cccc is a 4, 6 or 8-digit code, allowed codes are from 0000 to 99999999

Default control panel code Administrator: **1*1234; 1*123456; 1*12345678;**

WARNING: The main Administrator code starts with the prefix **1**

The main Service code starts with the prefix **0**

To change the code type, please contact the service technician of your alarm system.

Structure and description of the internal LCD keypad menu

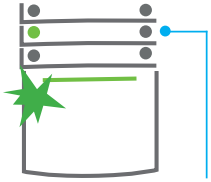
Administrator or User authorization by the code or RFID tag/card

CANCEL WARNING INDICATION	Allows you to cancel alarm/unsuccessful setting indication in all sections to which the user has access rights
SECTION CONTROL	Allows you to control the system's sections to which the user has access rights and are enabled in the internal settings.
PG CONTROL	Allows the user to control PG programmable outputs depending on the user's permissions and according to the internal settings.
EVENT MEMORY	Displays a detailed list of the event memory.
SETTING PREVENTED	Shows a list of triggered detectors preventing setting the system, provided this option is activated in the control panel configuration.
FAULTS IN SYSTEM	Displays a list of all detectors indicating system faults from sections to which the user has access rights.
BYPASSED DETECTORS	Displays a list of all blocked detectors in sections to which a user has access rights.
SYSTEM STATUS	Shows system status (list of triggered detectors, triggered tamper contacts, low batteries, bypassing, etc.).
SETTINGS	Allows editing of users and devices (only when USB is disconnected).
DISPLAY SETTING	Allows adjustment of keypad backlight intensity and display contrast.
MAINTENANCE MODE	Allows the Administrator to switch assigned sections to the Maintenance mode.

2.1.2.1. ALARM SETTING

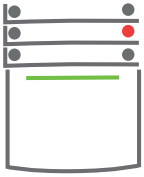
1. Authorize using the keypad.

Sections which can be controlled are lit up and the backlit indication button will start flashing green.



2. Press the right button

(the one which isn't lit up) to set a particular section. It is possible to set more sections subsequently. The delay between sections selection must not be longer than 2 seconds.



3. The command is executed

and the keypad acoustically indicates the exit delay. The section is set now, only the detectors with a "Delayed Zone" reaction provide time to leave the guarded area during the exit delay. The segment button of the set section turns red.

While setting the alarm, if any detector is triggered (e.g. an open window) the system will react in one of the following ways (based on the system configuration):

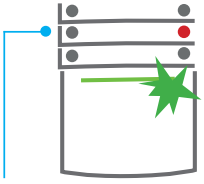
:: Detectors will guard automatically after they switch to a standby mode (default setting).
:: The system will optically indicate triggered detectors with a segment flashing red for 8 seconds and the system will set automatically once this period has expired.
:: Setting the section with triggered detectors is also possible by pressing the segment button on the right side repeatedly. This way a user confirms an intention to set the section with a triggered detector (e.g. an opened window). Otherwise the section with the triggered detector will not be set.
:: A triggered detector will prevent the section from being set. This status is optically indicated by a flashing red segment button. The detector preventing setting will be shown in the menu on the keypad's LCD display.

An unsuccessful setting is indicated by the indication button flashing yellow ("Unsuccessful setting" parameter must be enabled). Consult the installation with a service technician in order to program the desired behavior of the system.

2.1.2.2. ALARM UNSETTING

1. When you enter the building

(triggering a detector with a "Delayed zone" reaction), the system starts indicating entrance delay with a continuous tone and segment button of the section in which the delayed entrance has been triggered flashing green.

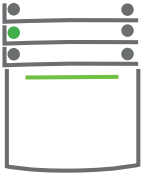


Authorize yourself using the keypad

– the green indication light of the authorization panel starts flashing.

2. Press the left segment button

of the section you want to unset.



3. The command is executed

and the segment buttons turn green to indicate unset sections

Note: If the "Unset section by authorization only during entrance delay" parameter is enabled, then mere authorization will unset such section where the entrance delay has been triggered.

2.1.2.3. DURESS ACCESS CONTROL

This function provides unsetting of the system in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is then reported to selected users (including ARC). Unsetting under duress is executed by adding 1 to the last number in a valid code.

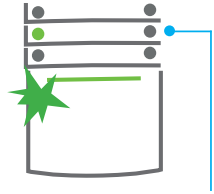
Example for a code with the prefix: Valid code: 2*9999 Code for unsetting under duress: 2*9990

Example for a code without the prefix: Valid code: *9999 Code for unsetting under duress: 9990

2.1.2.4. PARTIAL ALARM SETTING

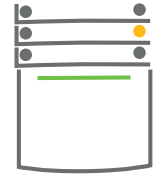
1. Authorize yourself using

the keypad (enter a code or hold a card or a tag up to the reader). The green backlit indication button will start flashing.



2. Press the right segment button

of the selected section.



3. The command is executed,

and the segment button turns yellow to indicate a partially set section.

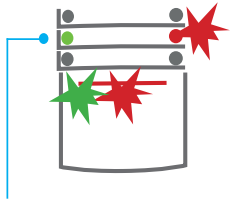
The system can also be configured to be partially set which allows guarding only by certain detectors in a section. Example: At night, it is possible to set the door and window detectors only, while motion detectors inside a house do not react to anything.

To fully set the premises in which partial setting is enabled, the button to set the system has to be pressed twice. After the button is pressed once it fl ashes yellow, when it is pressed a second time it fl ashes red. If the system is partially set – indicated by a continuous yellow light – the entire system can be fully set by authorization and pressing the yellow button. Once the button is pressed, the system will be fully set and the button turns red.

2.1.2.5. TERMINATING A TRIGGERED ALARM

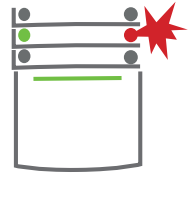
1. Authorize

yourself using the keypad (enter a code, hold a tag up to the reader).



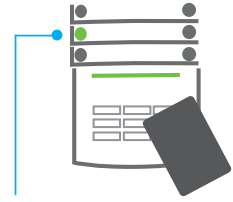
2. Press

the left segment button of the section where the alarm has been triggered.



3. Unsetting is finished

and sirens are silenced. The green flashing button indicates unsetting of the particular section. The red flashing light indicates alarm memory.



4. Authorize

yourslef and press the green button again to cancel the alarm memory indication.

5. The segment

Indicates the unset section with a continuously lit up green button.

A triggered alarm in progress is indicated by a rapidly flashing red segment button and a backlit indication button. You need to authorize yourself using the keypad in order to terminate the alarm. The section remains set, a rapidly flashing red segment button indicates the alarm memory. Indication will keep on flashing even after the system has been unset.

If the alarm memory indication was activated during your absence, search for the cause of the alarm in the event history and be very careful when entering and checking the premises or wait until the security agency arrives (provided your system is connected to an ARC).

The segment alarm memory indication remains on until the system is set once again. Alternatively, it can be cancelled by unsetting the system one more time. Alarm indication can be also cancelled from the main menu from the keypad with an LCD display – Cancel warning indication.

Indication of a triggered tamper alarm can be terminated only by a Service technician or Administrator.

Note: When using the "EN 50131-1, grade 2" system profile, it is always necessary to first authorize yourself and then perform the desired action.

Terminating an alarm using a remote control will also unset the corresponding section.

2.1.2.6. SECTION CONTROL FROM THE MENU OF THE KEYPAD WITH AN LCD DISPLAY

Statuses of sections are displayed in the left top part of the keypad's LCD display. A fully set section Is shown by a number in a rectangle filled with black colour 2; a partially set section is depicted by a framed number 4.

Control from the keypad menu:

:: Authorization by a valid code or an RFID chip.
:: Enter the menu by pressing ENTER.
:: Section Control → ENTER.
:: Select the desired section using arrows.
:: Pressing ENTER repeatedly will change between section statuses partially set / set / unset.
:: Press ESC to exit the menu.

2.1.3. USING THE JA-110E AND JA-150E SYSTEM KEYPADS

Statuses of individual sections are indicated by status indicators A, B, C, D above the LCD display and by the functions buttons. The control panel can be operated directly (setting or unsetting the alarm and other automation functions) using function buttons on the keypad. The function buttons and the status indicators A, B, C, D are colorfully backlit in order to clearly indicate the section status.

:: GREEN – Unset :: YELLOW – Partially Unset :: RED – Set

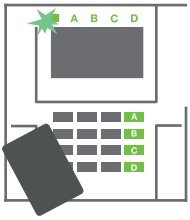
Authorization can be done by entering an access code on the keypad or using an RFID card/tag assigned to a particular user. Each user can have one code and one RFID chip (a card or a tag). If the users want to control multiple sections simultaneously, they must authorize themselves and then press function buttons of the particular sections subsequently. This way the users can unset all sections (for example the house and the garage) within one single authorization.

Structure and description of the internal LCD keypad menu

Administrator or User authorization by the code or RFID tag/card

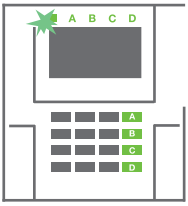
CANCEL WARNING INDICATION	Allows you to cancel alarm/unsuccessful setting indication in all sections to which the user has access rights
SECTION CONTROL	Allows you to control the system's sections to which the user has access rights and are enabled in the internal settings.
PG CONTROL	Allows the user to control PG programmable outputs depending on the user's permissions and according to the internal settings.
EVENT MEMORY	Displays a detailed list of the event memory.
SETTING PREVENTED	Shows a list of triggered detectors preventing setting the system, provided this option is activated in the control panel configuration.
FAULTS IN SYSTEM	Displays a list of all detectors indicating system faults from sections to which the user has access rights.
BYPASSED DETECTORS	Displays a list of all blocked detectors in sections to which a user has access rights.
SYSTEM STATUS	Shows system status (list of triggered detectors, triggered tamper contacts, low batteries, bypassing, etc.).
SETTINGS	Allows editing of users and devices (only when USB is disconnected).
DISPLAY SETTING	Allows adjustment of keypad backlight intensity and display contrast.
MAINTENANCE MODE	Allows the Administrator to switch assigned sections to the Maintenance mode.

2.1.3.1. ALARM SETTING



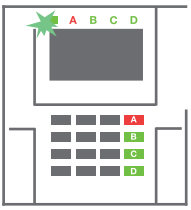
1. Authorize yourself using

the keypad. Function buttons A, B, C, D will light up and the system indicator starts flashing green.



2. Press the function button to set

a particular section. It is possible to set more sections subsequently. The delay between sections selection must not be longer than 2 seconds.



3. The command is executed

and the keypad acoustically indicates the exit delay. The section is set now, only the detectors with a "Delayed Zone" reaction provide time to leave the guarded area during the Exit delay. The status indicator and a function button of

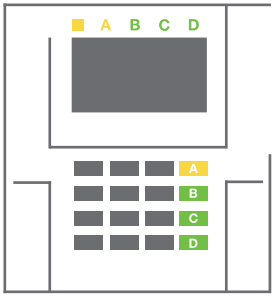
While setting the alarm, if any detector is triggered (e.g. an open window) the system will react (based on the system configuration) in one of the following ways:

:: The control panel will set itself. Triggered detectors will be blocked automatically.*)
:: The system will optically indicate triggered detectors with a function button flashing red for 8 seconds and the control panel will set automatically once this period has expired (triggered detectors will be blocked). *)
:: Setting the section with triggered detectors is also possible by pressing the function button repeatedly. The user must confirm an intention to set the section with a triggered detector (e.g. an opened window). Otherwise the system will not set.
:: A triggered detector will prevent the section from being set. This status is optically indicated by a function button flashing red. The detector preventing setting will be shown on the LCD display menu.

*) **WARNING**: Options a) and b) are not supported by EN 50131, gr.2 (selected control panel system profile).

If a detector with the "Instant zone alarm" reaction is triggered during an exit delay or if a detector with the "Delayed zone alarm" reaction stays triggered after the exit delay has expired, then the control panel will unset again. Unsuccessful setting is indicated by a system indicator flashing yellow, reported to the ARC and indicated by an external siren (applies to the security Grade 2).

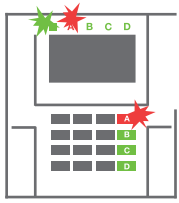
If the control panel is configured to be set without authorization then it is not necessary to authorize yourself. All you have to do is press a function button of a particular section. It is also possible to configure the control panel to be set simply by authorization.



WARNING: Setting without authorization automatically lowers the maximum security level to Grade 1. Consider all possible risks related to using this function.

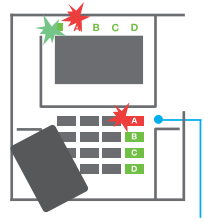
Consult the installation with a project consultant or a service technician in order to program the desired behavior of the alarm system.

2.1.3.2. ALARM UNSETTING



1. When you enter the building

(triggering a detector with a "Delayed zone" reaction), the system starts indicating an entrance delay with a continuous tone, the system indicator and a function button, both flashing red, of the section in which the delayed entrance has been triggered.

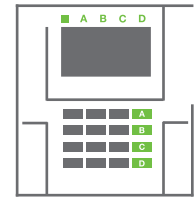


2. Authorize yourself using

the keypad – the system indicator will start flashing green.

3. Press the function buttons

of the sections you want to unset.



4. The command is executed

The function buttons and the system indicator turn green to indicate unset sections.

Note: If the "Unset section by authorization only during entrance delay" parameter is enabled, then mere authorization will unset a section where the entrance delayed has been triggered. This option should be used with caution when using multiple sections.

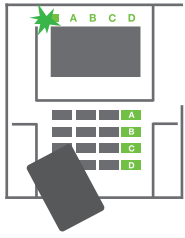
Consult the installation with a service technician in order to program the desired behavior of the system.

2.1.3.3. PARTIAL ALARM SETTING

WARNING: This is an additional function of the alarm system.

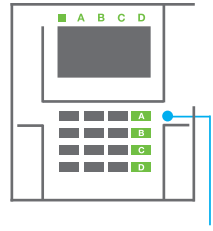
The system can also be configured to be partially set which allows guarding only by certain detectors in a section.

Example: At night, it is possible to set the door and window detectors only, while selected motion detectors will not trigger the alarm when somebody moves inside the section.



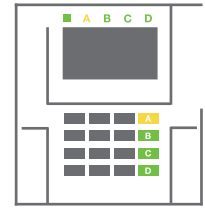
1. Authorize yourself using

the keypad (enter a code or hold an RFID card or tag up to the reader). The system indicator button will start flashing green.



2. Press the function button

of the selected section.



3. The command is executed

and the function button turns permanently yellow to indicate a partially set section.

To set the entire premises in which partial setting is enabled, hold down the button to set the control panel for 2 seconds or press it twice. After the button is pressed once it shows continuous yellow light, after it is pressed a second time it shows continuous red light.

If the system is partially set already – the function button shows a continuous yellow light – the entire system can be fully set by authorization and pressing the yellow button for a longer time. Once the button is pressed, the system will be fully set and the button turns red.

Partial setting can be configured in a way that authorization is not required.

In order to unset the control panel when it is partially set, press the yellow button. The control panel will unset and the button turns green.

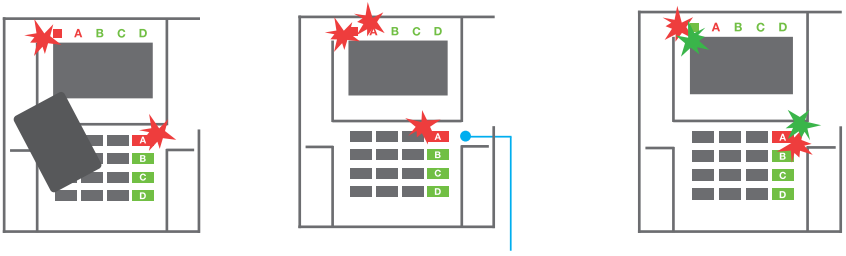
2.1.3.4. DURESS ACCESS CONTROL

Provides unsetting of the control panel in a special mode. The system seemingly unsets, however it triggers a silent panic alarm, which is reported to selected users (including ARC).

Unsetting under duress is executed by adding 1 to the last number in a valid code. Contact your service technician if you want to use this feature.

Example: Valid code: 9999 Code for unsetting under duress: 9990

2.1.3.5. TERMINATING A TRIGGERED ALARM



1. **Authorize yourself using**

   the keypad (enter a code or hold a tag up to the reader).

2. **Press the function button**

   of the section in which the alarm has been triggered.

3. **Unsetting is finished and sirens**

   are silenced. Rapidly alternately flashing function buttons (green/red) and the status indicators indicate the alarm memory.

A triggered alarm in progress is indicated by the status indicator and the function button rapidly flashing red. You need to authorize yourself using the keypad in order to terminate the alarm. The section remains set, a rapidly flashing red function button indicates the alarm memory. Indication will continue flashing even after the system has been unset.

WARNING: If the alarm memory indication was activated during your absence, always enter the building with caution, search for the cause of the alarm in the event history and be very careful when checking the premises or wait until the security agency arrives (provided your system is connected to an Alarm Receiving Centre).

The alarm memory indication remains on until the system is set once again. Alternatively, it can be also cancelled from the keypad menu: Main menu – Cancel warning indication. Indication of a triggered tamper alarm can be terminated only by a Service technician and Administrator.

Note: When using the "Default" system profi le, it is possible to select a particular action by pressing a function button fi rst and then confirm it by authorization using the keypad.

Terminating an alarm using a remote control will also unset the corresponding section.

2.1.3. OPERATING THE SYSTEM WITH A KEYFOB

Keyfobs must be enrolled into the system by the installer. The keyfob can be linked to specific users, which will prevent SMS text message notification to the user who is interacting with the system at the moment (if notification parameters are set up in this way). The keyfob can provide either bi-directional communication, confirming the execution of a command with a colored indicator light, or one-way without any confirmation. Keyfobs control and indicate battery status and are equipped with optical and acoustic indication.

BI-DIRECTIONAL KEYFOB

The button functions are differentiated by lock icons. The closed lock icon sets programmed sections; the opened lock icon unsets them. Correct command execution is confirmed by an LED light; unsetting – green, setting – red. A communication fault (out of the control panel's range) is indicated by a yellow LED light flashing once. The buttons with symbols of full and empty circles can control another section. Buttons of the keyfob can also be configured to control PG outputs in different modes: the first button switches on / the second switches off, each button can have an individual function when impulse or change functions are used. For more functions, it is possible to press two buttons at the same time. This way a 4-button keyfob can have up to 6 individual functions or one PG status output (e.g. turn the lights on and off), alternatively two PG outputs (e.g. a garage door and door lock.

If the system is configured to Set after confirmation the detector will indicate unsuccessful setting with a green LED light if a device is triggered. It is necessary to confirm setting by pressing the lock button again. A set section will be confirmed by a red LED light.

The keyfob buttons can be blocked to prevent accidental pressing. A command will be sent out when a button is pressed repeatedly. A low battery is indicated acoustically (with 3 beeps) and optically with a yellow flashing LED after pressing a button.

For more information, consult configuration of the remote control with your service technician.

ONE-WAY KEYFOBS

One-way keyfobs send a signal every time a button is pressed without receiving feedback from the control panel. Sending a signal is confirmed only by a short flash of the red LED and alternatively with a beep.

2.2. REMOTE OPERATING

The highest comfort for remote operating and management of the system is provided by the MyJABLOTRON service. The MyJABLOTRON web interface is a unique service which allows on-line access to JABLOTRON devices. It allows end-users to monitor and control the system. It is available in a form of a smartphone app and as a web application. The MyJABLOTRON service allows users to:

:: View the current system status,
:: Set/unset the entire system or a part of it,
:: Control programmable outputs,
:: View the event history,
:: Send reports to selected users via SMS, e-mail or PUSH notifications,
:: Capture images from photo verification devices and browse through them in the Photo gallery tab or directly in Recent events,
:: Monitor current temperature or energy consumption, including a history overview on graphic charts,
:: And other useful features.

Depending on your country or region, a web account in MyJABLOTRON can be set up by an authorized JABLOTRON partner. The login name is the user e-mail address. The password for the first log in will be sent to this address. The password can be changed anytime in the user settings.

2.2.1. OPERATING THE SYSTEM USING THE MyJABLOTRON SMARTPHONE APP

Once a user account is created, the user can remotely monitor and control the system via the MyJABLOTRON app for Android and iOS smartphones.

2.2.2. OPERATING THE SYSTEM VIA THE MyJABLOTRON WEB INTERFACE

The JABLOTRON 100+ system can be easily and conveniently operated using your computer via the internet and the MyJABLOTRON web interface, which is accessible from **www.myjablotron.com**.

2.2.3. OPERATING THE SYSTEM USING THE VOICE MENU

The system can be controlled from a phone through a voice menu, which guides the user through a series of options in the preconfigured language. To access the voice menu, you just dial the alarm system's phone number.

Access to the voice menu can be enabled either to all telephone numbers without restrictions or alternatively only to authorized phone numbers stored in the control panel. Depending on the configuration, authorization by entering a valid code on a phone keypad may be required. When the user enters the menu, the system will give an update of the current status of all sections assigned to the user. The caller then can control these sections, either individually or collectively, using phone keypad and available menu options.

The system default is set up to answer incoming calls after three rings (approximately 15 seconds).

2.2.4. OPERATING THE SYSTEM USING SMS COMMANDS

SMS commands can control individual sections and programmable outputs just like keypad segment buttons. The form of text message to operate the system is: CODE_COMMAND. The actual commands are predefi ned (SET/UNSET) with an additional numeric parameter which identifi es a specific section. One SMS can control multiple sections at the same time. In this case, added numbers in the command defi ne sections.

Example of an SMS command used to set sections 2 and 4.

CODE_SET_2_4

The commands to control the programmable outputs can be programmed by a system installer. For example, you may choose BLINDS DOWN as your command to close the blinds on your windows. It is also possible to configure the system not to require a code before a command. In such case the command is simply automatically identified when the system recognizes the user's phone number from which the SMS was sent. Configuration is done by a service technician.

2.2.5. OPERATING THE SYSTEM REMOTELY USING A COMPUTER (J-LINK)

The JABLOTRON 100+ system can be operated remotely using a computer with an installed J-Link software. It can be downloaded from the **www.myjablotron.com** website.

2.2.6. CONTROLLING THE PROGRAMMABLE OUTPUTS (PG)

2.2.6.1. KEYPAD SEGMENT

A PG output switches on by pressing the right button of the segment and switches off by pressing the left button. If the output is configured as a pulse output, it is switched off according to the pre-set time. PG control may or may not be stored in the control panel's event memory. Configuration is done by a service technician.

Authorization is/is not demanded based on the system configuration.

2.2.6.2. USER KEYPAD AUTHORIZATION

It is possible to activate a PG output just by user authorization (entering a code or using an RIFD tag). The PG output must be configured to activate from a designated keypad.

2.2.6.3. FROM THE MENU OF THE KEYPAD WITH AN LCD DISPLAY

After user authorization the programmable outputs can be controlled from the menu of the keypad with an LCD display. The user has access to programmable outputs depending on the user's permissions.

Control from the keypad menu:

:: Authorization by a valid code or an RFID chip.
:: Enter the menu by pressing ENTER.
:: PG Control → ENTER.
:: Select the desired PG group using arrows (1–32), (33–64), (65–96), (97–128) → ENTER.
:: Select the desired PG using arrows → ENTER.
:: Pressing ENTER repeatedly will change the PG statuses (active PG is shown by a PG number in a rectangle fi lled with black colour.
:: Press ESC to exit the menu..

2.2.6.4. REMOTE CONTROL

By pressing an assigned button of a remote control. Bi-directional remote controls confirm activation of PG outputs with an LED indicator.

2.2.6.5. MyJABLOTRON SMARTPHONE APP

By tapping on ON/OFF in the Automation (PG) tab.

2.2.6.6. MyJABLOTRON WEB INTERFACE

By clicking on ON/OFF in the Automation (PG) tab.

2.2.6.7. DIALLING-IN

Each telephone number stored in the system (one user can have one telephone number) can control one PG just by dialling-in (i.e. without establishing a call). Dialling-in consists of dialling the phone number of the SIM card used in the security system and hanging up before the system answers the call. By default, the system will answer the call after the third ring (approximately 15 seconds).

2.2.6.8. SMS MESSAGE

Sending an SMS can switch on/off a particular PG. Authorization is/is not demanded based on the system configuration.

Example: CODE_CONFIGURED TEXT

3. BLOCKING/DISABLING IN THE SYSTEM

3.1. BLOCKING USERS

Any user can be temporarily blocked (e.g. when a user loses a card/tag or his access code is revealed). When user's access is blocked their ID code or card/tag will no longer be accepted by the system. The users will also not receive any SMS alerts or voice reports to their phone.

Only the system administrator or service technician can block a user. One method of taking away access rights is by choosing Settings / Users / User / Bypass and selecting "Yes" on the LCD keypad. Another option is to locally or remotely block a user through the J-Link software by clicking on the user in the Settings / Users / User blocking column.

A blocked (disabled) user will be marked with a red circle until the blocking is cancelled.

3.2. BLOCKING DETECTORS

A detector can be temporarily blocked in a similar way a user can be disabled. A detector is blocked when its activation is temporarily not desirable (for example a motion detector in a room with a pet or disable a siren sounding). The system still performs diagnostics of tamper contacts and sends service events however the alarm function is deactivated.

Only the system administrator or service technician can block a detector. It can be achieved by choosing Settings / Devices / Bypass and selecting Yes on the LCD keypad. Another option is to use the J-Link software by clicking on the detector in the Settings / Diagnostics / Disabled column. A blocked detector is marked with a yellow circle until it is turned back on using the same procedure. A device can be also blocked from MyJABLOTRON smartphone app.

3.3. DISABLING TIMERS

To temporarily disable automated scheduled events in the system, a timer can be disabled. Disabling a scheduled event (e.g. unsetting the system from night guarding at a predetermined time) will prevent execution of that event (e.g. while on vacation).

A timer can be disabled locally or remotely through the J-Link software by clicking on the section in the Settings / Calendar / Blocked column. A disabled timer is marked with a red circle until it is turned back on using the same procedure.

4. CUSTOMIZING THE SYSTEM

4.1. CHANGING A USER ACCESS CODE

If the system is set up without prefixed codes, only the system administrator and the service technician can change the security codes. The system administrator can make changes from both the LCD keypad menu the J-Link software and MyJABLOTRON smartphone app. The code can be changed after authorization by selecting Settings / Users / User / Code. To input a new code, you must enter edit mode (the code will start flashing) by pressing Enter, enter the new code and confirm by pressing Enter again. After completing the changes, they must be confirmed by choosing Save when the system prompts you with "Save Settings?".

If the system is set up with prefix codes, individual users can be allowed to change their codes from the LCD menu on the keypad.

4.2. CHANGING, DELETING OR ADDING AN RFID CARD/TAG

If the system is set up with prefixed codes, users can add, change or delete their RFID tags or cards from the LCD menu on the keypad. These changes are done after authorization by selecting Settings / Users / User / Access card 1 (or 2). To enter a new RFID card/tag, you must enter edit mode (access card 1 or 2 will start to fl ash) by pressing Enter. Then the RFID card/tag must be placed on to the reader or the serial number must be manually entered. After confirming by pressing Enter again, the RFID card / tag is added. To delete an access card, enter "0" into the serial number field. After the changes are complete the change must be saved by selecting Save when the system prompts with Save Settings?

The system administrator and the service technician can add, change and delete RFID cards/tags from both the LCD keypad menu and the J-Link software.

4.3. CHANGING A USERNAME OR PHONE NUMBER

If the system is set up with prefix codes, users can add, change or delete their telephone numbers or change their name from the LCD menu on the keypad. This can be done after authorization by electing Settings / Users / User / Phone. The user must be in edit mode to make changes. This is done by pressing Enter. After making the changes, they must be confirmed by pressing Enter again. To delete a phone number, enter "0" into the phone number field. After the changes are complete the change must be saved by selecting Save when the system prompts with "Save Settings?".

The system administrator and the service technician can add, modify or delete a user phone number or change a user name from both the LCD keypad menu and the J-Link software.

4.4. ADDING/DELETING A USER

Only the system administrator or service technician can add new users to the system (or delete them). New users can be added to the system (or deleted from it) only through the J-Link software, or the F-Link software in the case of a service technician.

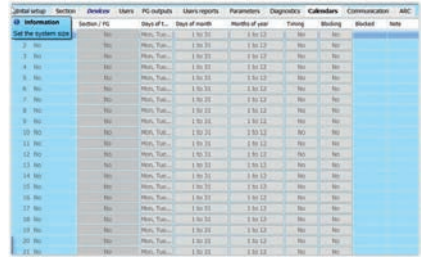
When creating a new user, it is necessary to assign him with access permissions (rights), sections the user may operate, programmable outputs he may control, and what type of authorization will be required.

4.5. CALENDAR EVENTS SET UP

It is possible to configure calendar events (unsetting / setting / partial setting, controlling or blocking PG outputs).

The calendar events can be set up via the J-Link software in the Calendar tab.

For each calendar event, action, section or PG output and event time can be set. Day can be defined by a day of week, month or year. For the selected day you can set up to 4 times to perform an action or to set repeating at regular intervals.



Therefore, calendar events can be customized not only for sections control but also for controlling various technologies in the object using PG outputs.

5. EVENT HISTORY

The security system stores all performed operations and events (setting, unsetting, alarms, faults, messages sent to users and ARCs) in the micro SD card in the system's control panel. Each entry includes the date, time (start and end), and source (cause/origin) of the event.

The different ways of browsing through the system's event history:

5.1. USING THE LCD KEYPAD

Accessing the event history using the keypad requires user authorization. Once authorized, the available options (based on user permissions) are displayed by choosing Event Memory. Records can be viewed using arrows.

5.2. USING THE J-LINK SOFTWARE AND A COMPUTER

The system memory can be browsed using the J-Link software. Events can be downloaded from the control panel in small (about 1,200 events) or larger (about 4,000 events) batches. The events can be filtered in detail, colour-coded for easier orientation, or saved into a fi le in a computer.

5.3. LOGGING INTO MyJABLOTRON (WEB/SMARTPHONE)

All system events can be viewed after logging in the MyJABLOTRON web/smartphone interface. The account shows history in a range which corresponds with the user's permissions.

6. TECHNICAL SPECIFICATIONS

PARAMETER	JA-103K		JA-107K	
Control panel power supply	~ 110 – 230 V/50 – 60 Hz, max. 0.28 A with fuse F1.6 A/250 V Protection class II		~ 110 – 230 V/50 – 60 Hz, max. 0.85 A with fuse F1.6 A/250 V Protection class II	
Back-up battery	12 V; 2.6 Ah (lead gel)		12 V; 7 to 18 Ah (lead gel)	
Maximum battery charging time	48 h		48 h	
BUS voltage (red - black)	12.0 to 13.8 V		12.0 to 13.8 V	
Maximum continuous current consumption from the control panel	1000 mA		2000 mA permanent 3000 mA for 60 minutes (max. 2000 mA for one BUS)	
Max. continuous current consumption for back-up 12 hours	JA-103K – 2.6 Ah back-up battery		JA-107K – 18 Ah back-up battery	
	Without GSM communicator	LAN – OFF: 115 mA LAN – ON: 88 mA	Without GSM communicator	LAN – OFF: 1135 mA LAN – ON: 1107 mA
	With GSM communicator	LAN – OFF: 80 mA LAN – ON: 53 mA	With GSM communicator	LAN – OFF: 1100 mA LAN – ON: 1072 mA
Max. continuous current consumption for back-up 24 hours	Without GSM communicator	LAN – OFF: 21 mA	Without GSM communicator	LAN – OFF: 535 mA LAN – ON: 499 mA
	With GSM communicator	LAN – OFF: 17 mA	With GSM communicator	LAN – OFF: 530 mA LAN – ON: 494 mA
Maximum number of devices	50		230	
LAN communicator	Ethernet interface, 10/100BASE		Ethernet interface, 10/100BASE	

PARAMETER	JA-103K	JA-107K
Dimensions	268 x 225 x 83 mm	357 x 297 x 105 mm
Weight with/without AKU	1844 g/970 g	7027 g/1809 g
Reaction to invalid code entry	Alarm after 10 wrong code entries	
Event memory	Approx. 7 million latest events, including date and time	
Power supply unit	Type A according to EN 50131-6	
	T 031 note: In case of a main power failure is the system backed up for 24 hours and at the same time is a failure report sent to the ARC.	
GSM communicator (2G)	850 / 900 / 1800 / 1900 MHz	
Classification	Security grade 2 according to EN 50131-1	
Operational environment	Environmental class II (indoor general) according to EN 50131-1	
Operational temperature range	-10 °C to +40 °C	
Average operational humidity	75 % RH, non-condensing	
Complies with	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	
Radio operating frequency (with the JA 11xR module)	868.1 MHz	
Radio emissions	ETSI EN 300 220-1,-2 (module R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7	
Safety conformity	EN 62368-1+A11	
Caller identification (CLIP)	ETSI EN 300 089	
Operational conditions	ERC REC 70-03	
Certification body	Trezor Test s.r.o. (no. 3025)	

JABLOTRON ALARMS a.s. hereby declares that the control panels JA-103K a JA-107K are in a compliance with the relevant European Union harmonisation legislation: Directives No: 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU, when used as intended. The original of the conformity assessment can be found www.jablotron.com – Downloads section.

Note: Although these products do not contain any harmful materials we suggest you return these products to the dealer or directly to the producer after use.

INHALTSVERZEICHNIS

REGELMÄSSIGE WARTUNG

:: 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 Systemprofi I „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 Alarme 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 aufblinken) 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.

1. EINFÜHRUNG

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.
Administrator-code (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, Zugriffscodes, 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.

CODE-BERECHTIGUNG	TYPBESCHREIBUNG
Administrator-code (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 Überwachungscodes ist nur durch die Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Entsperren	Dieser Code dient dazu, das System nach der Sperrung durch einen Alarm wieder zu entsperren. Der Benutzer dieses Codes ist nicht berechtigt, den Code zu ändern oder den Alarmspeicher zu löschen. Die Anzahl der Entsperrcodes ist nur durch die Maximalkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.

Die Sicherheit von Zugriffscodes, 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)

Parameter der Zentrale	4 ZIFFERN	6 ZIFFERN	8 ZIFFERN
„Code mit einem Präfix" und **„Erzwungene Zugriffssteuerung"** deaktiviert	= 10^4 – (Anzahl der Benutzer – 1)	= 10^6 – (Anzahl der Benutzer – 1)	= 10^8 – (Anzahl der Benutzer – 1)
„Code mit einem Präfix" deaktiviert; **„Erzwungene Zugriffssteuerung"** aktiviert	≤ 10^4 – ((Anzahl der Benutzer – 1) * 3)	≤ 10^6 – ((Anzahl der Benutzer – 1) * 3)	≤ 10^8 – ((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 – (Anzahl der Benutzer – 1))	= 10^8 * (10^6 – (Anzahl der Benutzer – 1))	= 10^8 * (10^8 – (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

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)

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.

2.1. DER BETRIEB VOR ORT

DAUERHAFT GRÜN
UNSCHARF | AUS
BLINKT GRÜN
EINGANGSVERZÖGERUNG

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 der 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 des Systems 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 Codeträge: 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 MyJABLOTORN-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

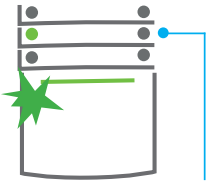
Administratoroder Benutzer-berechtigung über den Code oder RFID-CIP /-Karte

ABBRECHEN DER WARNANZEIGE	Ermöglicht Ihnen, die Anzeige für den Alarm / die erfolglose Scharfschaltung in allen Bereichen zu löschen, für die der Benutzer Zugriffsrechte hat.
BEREICHS-STEUERUNG	Ermöglicht Ihnen, die Bereiche des Systems zu steuern, für die der Benutzer die Zugriffsrechte hat und die in den internen Einstellungen aktiviert sind.
PG-STEUERUNG	Ermöglicht dem Benutzer, programmierbare PG-Ausgänge abhängig von den Berechtigungen des Benutzers und den internen Einstellungen zu steuern.
EREIGNISSPEICHER	Zeigt eine detaillierte Liste des Ereignisspeichers an.
SCHARFSCHALTUNG VERHINDERT	Zeigt eine Liste der aktivierten Melder an, welche die Scharfschaltung des Systems verhindern, sofern diese Option in der Konfiguration der Zentrale aktiviert ist.
FEHLER IM SYSTEM	Zeigt eine Liste aller Melder an, die eine Systemfehler in den entsprechenden Bereichen hinweisen, für die der Benutzer Zugriffsrechte hat.
UMGELEITETE MELDER	Zeigt eine Liste aller blockierten Melder in Bereichen an, für die der Benutzer Zugriffsrechte hat.
SYSTEMSTATUS	Zeigt den Systemstatus an (Liste der ausgelösten Melder, ausgelöste Sabotagekontakte, schwache Batterien, Bypass, usw.).
EINSTELLUNGEN	Ermöglicht die Bearbeitung von Benutzern und Geräten (sofern keine USB-Verbindung besteht).
DISPLAY-EINSTELLUNG	Ermöglicht die Anpassung der Intensität der Hintergrundbeleuchtung und des Kontrastes des Displays.
WARTUNGSMODUS	Ermöglicht dem Administrator zugewiesene Bereiche in den Wartungsmodus zu schalten.

2.1.2.1. SCHARFSCHALTUNG DER ALARMANLAGE

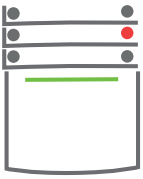
1. Berechtigen Sie sich über die Tastatur. Die Bereiche, die gesteuert werden können, leuchten auf und die hintergrundbeleuchtete Anzeige beginnt grün zu blinken.

2. Drücken Sie die rechte Taste (die, die nicht aufleuchtet) und schalten Sie den jeweiligen



Bereich scharf. Es können mehrere Bereiche hintereinander scharf geschaltet werden. Die Verzögerung zwischen der Bereichsauswahl darf nicht länger als 2 Sekunden betragen.

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.

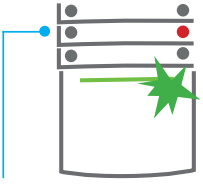
:: Die Scharfschaltung mit ausgelösten und aktivierten Meldern ist auch möglich, indem Sie wiederholt auf die Bereichstaste auf der rechten Seite drücken. Auf diese Weise bestätigt der Benutzer die Absicht, den Bereich mit einem ausgelösten Melder (z. B. einem geöffneten Fenster) scharf zu schalten. 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.

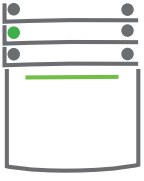
2.1.2.2. UNSCHARFSCHALTUNG DER ALARMANLAGE

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.

Berechtigen Sie sich über die Tastatur – Das grüne Licht auf dem Berechtigungsfeld beginnt zu blinken.



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.

2.1.2.3. ERZWUNGENE ZUGRIFFSSTEUERUNG

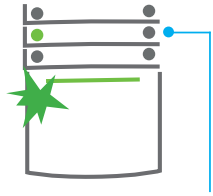
Diese besondere Funktion ermöglicht die Unscharfschaltung des Systems in einem speziellen Modus. Das System wird scheinbar normal unscharf, löst jedoch im Hintergrund einen stillen Panikalarm aus, welcher ausgewählten Benutzern gemeldet wird (einschließlich der AES). Die Unscharfschaltung unter Bedrohung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

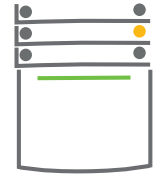
Beispiel eines Codes ohne Präfix: Gültiger Code: 9999
Code für die Unscharfschaltung unter Zwang: 9990

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 Anzeigentaste beginnt zu blinken.



2. Drücken Sie die rechte Bereichstaste des ausgewählten Bereichs.



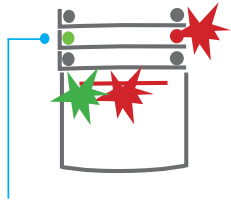
3. Der Befehl wird ausgeführt und die Bereichstaste wird gelb und zeigt einen teilweise scharf geschalteten Bereich an.

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.

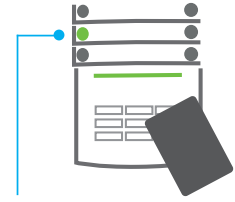
2.1.2.5. BEENDEN EINES AUSGELÖSTEN ALARMS

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 Systemprofi Is „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 LCDDISPLAY

Statuses of sections are displayed in the left top part of the keypad's LCD display. A fully set section Is shown by a number in a rectangle filled with black colour 2; a partially set section is depicted by a framed number 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.

2.1.3. 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

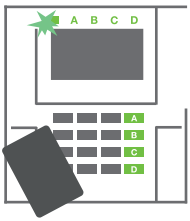
Die Berechtigung kann durch Eingabe eines Zugriffscodes auf der Tastatur oder durch Verwendung einer RFID-Karte / Tag erfolgen, die einem Benutzer zugewiesen wurde. Jeder Benutzer kann einen Code und einen RFID-Chip (eine Karte oder ein Tag) haben. Wenn Benutzer mehrere Bereiche gleichzeitig steuern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

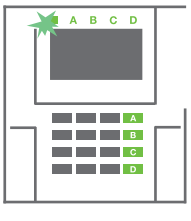
Administratoroder Benutzer-berechtigung über den Code oder RFID-CIP /-Karte

ABBRECHEN DER WARNANZEIGE	Ermöglicht Ihnen, die Anzeige für den Alarm / die erfolglose Scharfschaltung in allen Bereichen zu löschen, für die der Benutzer Zugriffsrechte hat.
BEREICHS-STEUERUNG	Ermöglicht Ihnen, die Bereiche des Systems zu steuern, für die der Benutzer die Zugriffsrechte hat und die in den internen Einstellungen aktiviert sind.
PG-STEUERUNG	Ermöglicht dem Benutzer, programmierbare PG-Ausgänge abhängig von den Berechtigungen des Benutzers und den internen Einstellungen zu steuern.
EREIGNISSPEICHER	Zeigt eine detaillierte Liste des Ereignisspeichers an.
SCHARFSCHALTUNG VERHINDERT	Zeigt eine Liste der aktivierten Melder an, welche die Scharfschaltung des Systems verhindern, sofern diese Option in der Konfiguration der Zentrale aktiviert ist.
FEHLER IM SYSTEM	Zeigt eine Liste aller Melder an, die eine Systemfehler in den entsprechenden Bereichen hinweisen, für die der Benutzer Zugriffsrechte hat.
UMGELEITETE MELDER	Zeigt eine Liste aller blockierten Melder in Bereichen an, für die der Benutzer Zugriffsrechte hat.
SYSTEMSTATUS	Zeigt den Systemstatus an (Liste der ausgelösten Melder, ausgelöste Sabotagekontakte, schwache Batterien, Bypass, usw.).
EINSTELLUNGEN	Ermöglicht die Bearbeitung von Benutzern und Geräten (sofern keine USB-Verbindung besteht).
DISPLAY-EINSTELLUNG	Ermöglicht die Anpassung der Intensität der Hintergrundbeleuchtung und des Kontrastes des Displays.
WARTUNGSMODUS	Ermöglicht dem Administrator zugewiesene Bereiche in den Wartungsmodus zu schalten.

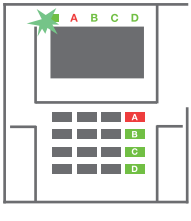
2.1.3.1. SCHARFSCHALTUNG DER ALARMANLAGE



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.



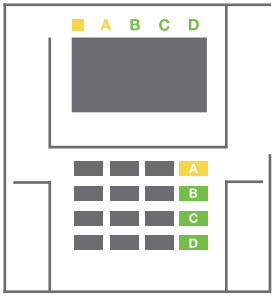
3. Der Befehl wird ausgeführt und die Tastatur zeigt akustisch die Ausgangsverzögerung an. Der Bereich ist jetzt scharf geschaltet. Nur Melder mit der Reaktion einer „Verzögerten Zone" bieten Zeit zum Verlassen des überwachten Bereichs während der Ausgangsverzögerung. Die Statusanzeige und eine Funktionstaste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

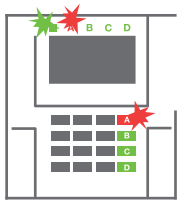


Wenn die Zentrale so konfiguriert ist, dass sie sich ohne Berechtigung scharf schaltet, müssen Sie sich nicht berechtigen. Alles, was Sie tun müssen, ist eine Funktionstaste eines bestimmten Bereichs zu drücken. Es ist auch möglich, die Zentrale so zu konfigurieren, dass sie sich einfach über die Berechtigung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

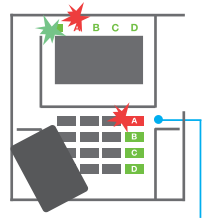
WARNHINWEIS: Eine Scharfschaltung ohne Berechtigung senkt automatisch die Sicherheitsstufe auf Stufe 1. Berücksichtigen Sie daher alle Risiken bei Verwendung dieser Funktion.

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

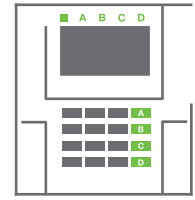
2.1.3.2. UNSCHARFSCHALTUNG DER ALARMANLAGE



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.

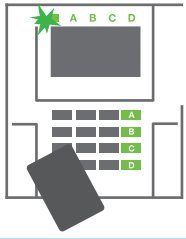
Wenden Sie sich zur Programmierung des gewünschten Systemverhaltens an einen Errichter.

2.1.3.3. TEILWEISE SCHARFSCHALTUNG DES ALARMSYSTEMS

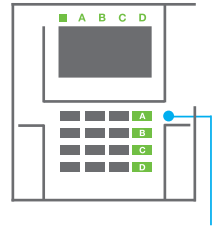
WARNHINWEIS: Dies ist eine zusätzliche Funktion des Alarmsystems.

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

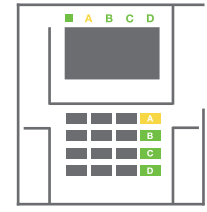
Beispiel: In der Nacht ist es möglich, nur die Tür- und Fenstermelder scharf zu schalten, während die ausgewählten Bewegungsmelder keinen Alarm auslösen, wenn sich jemand innerhalb des Bereichs bewegt.



1. Berechtigen Sie sich über die Tastatur (geben Sie einen Code ein oder halten Sie eine RFIDKarte 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.

2.1.3.4. ERZWUNGENE ZUGRIFFSSTEUERUNG

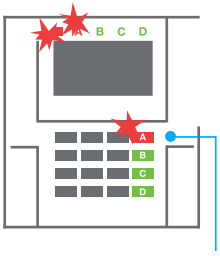
Hier erfolgt eine Unscharfschaltung in einem speziellen Modus. Das System scheint unscharf geschaltet zu sein, jedoch löst es einen stillen Panikalarm aus, der ausgewählten Benutzern gemeldet wird (einschließlich dem AES).

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.

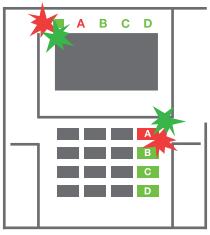
Beispiel: Gültiger Code: 9999 Code zur Unscharfschaltung unter Zwang: 9990

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

Hinweis: Bei Verwendung des „Standard"-Systemprofi l 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.

2.1.3.6. 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). 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.

2.2. 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 eine 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.

2.2.1. 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.

2.2.2. 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 aus haben, bedient werden.

2.2.3. 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.

2.2.4. 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 identifi ziert, wenn das System die Telefonnummer des Benutzers erkennt, von der die SMS gesendet wurde. Die Konfiguration wird von einem Errichter vorgenommen.

2.2.5. 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.myjablotron.com** heruntergeladen werden.

2.2.6. STEUERUNG DER PROGRAMMIERBAREN AUSGÄNGE (PG)

2.2.6.1. 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.

2.2.6.2. BERECHTIGUNG ÜBER DIE TASTATUR EINES BENUTZERS

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

2.2.6.3. VOM MENÜ EINER TASTATUR MIT EINEM LCDDISPLAY

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 angezeigt).
:: Drücken Sie ESC, um das Menü zu verlassen.

2.2.6.4. FERNSTEUERUNG

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

2.2.6.5. MyJABLOTRON-APP FÜR SMARTPHONES

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

2.2.6.6. WEBBASIERTE MyJABLOTRON-SCHNITTSTELLE

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

2.2.6.7. 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 System-Konfiguration 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.

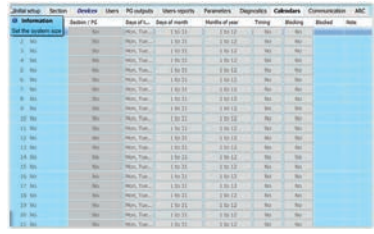
Der Systemadministrator und der Errichter können die Telefonnummer eines Benutzers oder einen Benutzernamen über das LCD-Menü auf der Tastatur hinzufügen, ändern oder löschen.

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 konfi gurieren. 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.

5. EREIGNISVERLAUF

Das Sicherheitssystem speichert alle durchgeführten Aktionen und Ereignisse (Scharfschaltung, Unscharfschaltung, Alarme, Fehler, Nachrichten, die an Benutzer und AESs versendet werden) auf der MicroSD-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.

6. TECHNISCHE PARAMETER

<table>
<tr><th>PARAMETER</th><th colspan="2">JA-103K</th><th colspan="2">JA-107K</th></tr>
<tr><td>Stromzufuhr der Zentrale</td><td colspan="2">~ 110–230 V / 50–60 Hz, max. 0.28 A
mit Sicherung F1.6 A/250 V
Sicherheitsklasse II</td><td colspan="2">~ 110–230 V / 50–60 Hz, max. 0.85 A
mit Sicherung F1.6 A/250 V
Sicherheitsklasse II</td></tr>
<tr><td>Backup-Batterie</td><td colspan="2">12 V; 2.6 Ah (Blei-Gel)</td><td colspan="2">12 V; 7 to 18 Ah (Blei-Gel)</td></tr>
<tr><td>Maximale Ladezeit der Batterie</td><td colspan="4">72 Std.</td></tr>
<tr><td>BUS-Spannung (rot - schwarz)</td><td colspan="4">12,0 bis 13,8V</td></tr>
<tr><td>Maximaler Dauerstromverbrauch von der Zentrale</td><td colspan="2">1000 mA</td><td colspan="2">2000 mA permanent
3000 mA für 60 Minuten
(max. 2000 mA für ein BUS)</td></tr>
<tr><td rowspan="3">Max. Dauerstromverbrauch für einen Backup von 12 Stunden</td><td rowspan="2">Ohne GSM Wähl- & Übertragungs--gerät</td><td rowspan="2">LAN – AUS
115 mA
LAN – EIN
88 mA</td><td colspan="2">Gilt für 18 Ah Backup-Batterie</td></tr>
<tr><td>Ohne GSM Wähl- & Übertragungs -gerät</td><td>LAN – AUS
1135 mA
LAN – EIN
1107 mA</td></tr>
<tr><td>Mit GSM Wähl- & Übertragungs--gerät</td><td>LAN – AUS
80 mA
LAN – EIN
53 mA</td><td>Mit GSM Wähl- & Übertragungs -gerät</td><td>LAN – AUS
1100 mA
LAN – EIN
1072 mA</td></tr>
<tr><td>Maximale Geräteanzahl</td><td colspan="2">50</td><td colspan="2">230</td></tr>
<tr><td>LAN-Kommunikator</td><td colspan="4">ETHERNET SCHNITTSTELLE, 10/100BASE-T</td></tr>
<tr><td>Abmessungen (mm)</td><td colspan="2">268 x 225 x 83 mm</td><td colspan="2">357 x 297 x 105 mm</td></tr>
<tr><td>Gewicht mit / ohne AKU</td><td colspan="2">1844 g/970 g</td><td colspan="2">7027 g/1809 g</td></tr>
<tr><td>Reaktion auf eine ungültige Codeeingabe</td><td colspan="4">Alarm nach 10 falschen Codeeingaben</td></tr>
</table>

PARAMETER	JA-103K	JA-107K
Ereignisspeicher	Ca. 7 Millionen letzte Ereignisse, einschließlich Datum und Zeit	
Netzteil	Typ A (gemäß EN 50131-6)	
GSM-Kommunikator (2G)	850 / 900 / 1800 / 1900 MHz	
Klassifizierung	Sicherheitsstufe 2 / Umgebungsklasse II (gemäß EN 50131-1)	
Betriebsumgebung	Allgemeine Innenbereiche	
Betriebstemperaturbereich	-10 °C bis +40 °C	
Durchschnittliche Betriebs-feuchtigkeit	75 % RH, nicht kondensierend	
Entspricht	EN 50131-1 ed. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 ed. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN 50581	
Funkfrequenz (with the JA-11xR module)	868.1 MHz, JABLOTRON Protokoll	
Funkemissionen	ETSI EN 300 220-1,-2 (Modul R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7	
Sicherheitskonformität	EN 62368-1+A11	
Betriebsbedingungen	ERC REC 70-03	
Zertifizierungsstelle	Trezor Test s.r.o. (no. 3025)	
Rufnummererkennung (CLIP)	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 – 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. JABLOTRON

TABLA DE CONTENIDOS

MANTENIMIENTO PERIÓDICO

:: Es necesario realizar controles de mantenimiento periódicos y oportunos para asegurar un funcionamiento fiable del sistema. La mayor parte del mantenimiento es llevado a cabo por una empresa instaladora al menos una vez al año durante las inspecciones periódicas de mantenimiento.

:: El mantenimiento del usuario consiste principalmente en mantener los dispositivos limpios. El ADMINISTRADOR del sistema puede cambiar el sistema a un modo MANTENIMIENTO para poder abrir los detectores (cambiar baterías) o eliminarlos de la instalación. Consulte la solicitud para configurar en modo MANTENIMIENTO con la empresa instaladora. Si el sistema se configura con el perfil del sistema "EN 50131-1, grade 2", el modo MANTENIMIENTO no está disponible.

:: El sistema se puede cambiar a modo mantenimiento a través del software J-Link o desde el menú del teclado con pantalla LCD. Después de la autorización se puede seleccionar el "Modo mantenimiento" con la selección de las particiones donde el mantenimiento es necesario. En el modo mantenimiento no generará alarmas en las particiones seleccionadas, incluyendo la apertura o eliminación de los detectores de la instalación.

:: El modo mantenimiento se indica mediante el parpadeo verde del botón de activación (2 parpadeos cada 2 segundos) y a través del apagado de los botones de segmento de la partición particular.

:: Tenga cuidado al manipular los dispositivos y evite dañar el plástico y los mecanismos de los detectores. a Por lo general, la cubierta está asegurada con una pestaña que solo necesita empujarse ligeramente hacia dentro del cuerpo del detector con una pequeña herramienta (ej. un destornillador) y después se puede quitar la cubierta. En algunos casos, la pestaña está asegurada con un pequeño tornillo de bloqueo que debe desatornillar primero.

:: Al realizar el cambio de baterías del detector, siempre cambie todas las baterías del detector en particular al mismo tiempo (use baterías del mimo tipo y del mismo fabricante).

:: Algunos dispositivos pueden requerir ser probados (detectores de fuego, por ejemplo). Para más información, por favor contacte con su técnico de servicio.

1. INTRODUCCIÓN

El sistema JABLOTRON 100+ esta disenado para un maximo de 600 usuarios y puede dividirse en 15 particiones independientes. Se pueden conectar hasta 230 dispositivos y el sistema ofrece hasta 128 salidas programables multiproposito (ej. domotica).

2. MANEJO DEL SISTEMA JABLOTRON 100+

El sistema de seguridad se puede controlar de diferentes formas. Para desarmar la alarma, necesita siempre una autorización en forma de identificacion de usuario. El sistema reconoce la identidad de los usuarios y les permite manejar aquellas partes del sistema que les han sido asignadas para controlar. Puede elegir diferentes tipos de armado con o sin autorización. Cuando se utiliza el tipo de autorización Estandar, no tiene que autorizarse ya que es posible armar el sistema solamente presionando el boton de segmento derecho del teclado. El nombre de usuario, la fecha y la hora se registran y guardan en la memoria del sistema cada vez que se accede al mismo. Esta informacion esta disponible indefinidamente. Cualquier usuario puede cancelar la alarma (la sirena deja de sonar) solo con una autorización en cualquier parte del sistema (dependiendo de sus derechos de acceso). Sin embargo, no puede desarmar el sistema automaticamente (a menos que el perfil del sistema se cambie).

Nota: Dependiendo de la configuración de la instalación y ajustes del sistema, algunas opciones descritas a continuación podrían no estar disponibles. Consulte la configuración de la instalación con su técnico de servicio.

Usuarios y permisos de acceso

CÓDIGO DE AUTORIZACIÓN	DESCRIPCIÓN
Código CRA	Este código tiene el nivel más alto de autorización para configurar el comportamiento del sistema y permite exclusivamente realizar un desbloqueo del sistema tras un salto de alarma. Puede entrar en modo Servicio, acceder a todas pestañas con opciones que incluyen la comunicación con CRA, la cual se puede denegar el acceso al técnico de Servicio (código Servicio). Mientras el parámetro "Administrador restringe derechos Servicio/CRA" está desmarcado, el código CRA puede controlar todas las particiones y salidas PG utilizadas por el sistema. Este código permite añadir más Administradores y otros usuarios con un nivel más bajo de autorización y asignarles códigos, tags RFID y tarjetas. También tiene permiso para borrar la memoria de alarmas y alarmas de sabotaje. **El número de códigos CRA está limitado solo por la restante capacidad del panel de control y no hay un código configurado por defecto.**
Código de Servicio (Servicio)	Este código puede entrar en modo Servicio y configurar el comportamiento del sistema. Tiene acceso a todas las pestañas con opciones, incluyendo comunicación CRA a menos que el acceso esté limitado al técnico CRA. Mientras el parámetro "Administrador restringe derechos Servicio/CRA" está desmarcado, el código de Servicio puede controlar todas las particiones y salidas PG utilizadas en el sistema. Puede crear un usuario con permiso CRA, otros técnicos de Servicio, Administradores y otros usuarios con menor nivel de autorización y asignarles códigos de acceso, tags RFID y tarjetas. También tiene permiso para eliminar una memoria de alarma y sabotaje. El número de códigos de Servicio está limitado por la restante capacidad del panel de control. **Por defecto, el código es el 1010. El usuario Servicio siempre está en la posición 0 y no puede ser eliminado.**
Código Administrador (Principal)	Este código tiene siempre acceso total a todas las particiones y está autorizado para controlar todas las salidas PG. El Administrador puede crear otro Administrador y otros usuarios con menor nivel de autorización y asignarles acceso a particiones y salidas PG, códigos de acceso, tags RFID y tarjetas. Tiene permiso para borrar memoria de alarmas. Sólo puede haber un código de Administrador principal, el cual no puede ser borrado. Cuando "Administrador restringe derechos Servicio/CRA" está habilitado, el código de administrador debe autorizarse para confirmar el acceso de la CRA y técnicos de Servicio. **Por defecto, el código es el 1234. El usuario Administrador siempre está en la posición 1 y no puede ser eliminado.**
Código Administrador (Otro)	Este código tiene acceso a las particiones seleccionadas por el Administrador principal, en las cuales el otro Administrador puede añadir nuevos usuarios con el mismo o menor nivel de autorización para controlar particiones y salidas PG, asignarles códigos de acceso, tags RFID y tarjetas. Tiene permiso para borrar memoria de alarmas en las particiones asignadas. Cuando "Administrador restringe derechos Servicio/CRA" está habilitado, el código de administrador debe autorizarse para confirmar el acceso de la CRA y técnicos de Servicio. **El número de códigos de Administrador (otro) está limitado por la restante capacidad del panel de control. No hay código configurado por defecto**.

CÓDIGO DE AUTORIZACIÓN	DESCRIPCIÓN
Código Usuario	Este código tiene acceso a particiones y salidas PG asignadas por un Administrador. Los usuarios pueden añadir/borrar sus tags RFID y tarjetas de acceso, y cambiar sus números de teléfono. Los usuarios pueden cambiar sus propios códigos siempre que el sistema utilice Códigos con prefijo. Tienen permiso para borrar memoria de alarmas en las particiones asignadas. Usuarios específicos podrán tener el acceso a las particiones limitado por horario. **El número de códigos de Usuario está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**
Código Armar	Este código permite solamente armar una partición seleccionada y controlar salidas PG (ON/OFF) que requieran autorización. Los usuarios con este nivel de autorización no pueden cambiar sus propios códigos ni borrar memoria de alarmas. **El número de códigos Armar está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**
Código Solo PG	Permite al usuario controlar salidas programables solamente con autorización. Esto se aplica tanto al encendido como al apagado. Los usuarios con este nivel de autorización no pueden cambiar sus propios códigos ni borrar memoria de alarmas. **El número de códigos Sólo PG está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**
Código Pánico	Este código está permitido solamente para activar una alarma de Pánico. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas. **El número de códigos Pánico está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**
Código Vigilancia	Este es un código para la central receptora. Este nivel de autorización permite armar el sistema entero. Sin embargo, el código de vigilancia solo puede desarmar el sistema durante una alarma o después de una alarma mientras siga activa la memoria de alarmas. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas. **El número de códigos de Vigilancia está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**
Código de Desbloqueo	Este código está diseñado para desbloquear el sistema tras un Bloqueo del sistema por una alarma. Un usuario con este código no puede cambiar su propio código ni borrar memoria de alarmas. **El número de códigos de desbloqueo está limitado por la restante capacidad del panel de control. No hay código configurado por defecto.**

La seguridad de los códigos de acceso, dispositivos RFID sin contacto y mandos a distancia:

Un panel de control permite asignar a cada usuario un código de 4, 6 u 8 dígitos y hasta dos tags RFID para autorizarse en el sistema. Se requiere autorización de usuario durante cada manipulación vía teclado, menú de voz, ordenador, aplicaciones web o móviles. La longitud del código afecta al número de posibles combinaciones y por tanto a la seguridad del código.

El número de combinaciones de códigos depende de la configuración:

Parámetros del panel de control	4 DÍGITOS	6 DÍGITOS	8 DÍGITOS
"Código con prefijo" habilitado	= 10^4 = (10.000)	= 10^6 = (1.000.000)	= 10^8 = (100.000.000)
"Código con prefijo" y **"Código de coacción"** ambos deshabilitados	= 10^4 – (Número de usuarios – 1)	= 10^6 – (Número de usuarios – 1)	= 10^8 – (Número de usuarios – 1)

Parámetros del panel de control	4 DÍGITOS	6 DÍGITOS	8 DÍGITOS
"Código con prefijo" deshabilitado; **"Código de coacción"** habilitado	≤ 10^4 – ((Número de usuarios – 1) * 3)	≤ 10^6 – ((Número de usuarios – 1) * 3)	≤ 10^8 – ((Número de usuarios – 1) * 3)
Usando sólo una **tarjeta RFID** con un rango de 14 caracteres (6 constantes + 8 variables)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
"Código con prefijo" y **"Confirmación de tarjeta con un código"** ambos habilitados	= (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)
"Código con prefijo" deshabilitado; **"Confirmación de tarjeta con un código"** habilitado	= 10^8 * (10^4 – (Número de usuarios – 1))	= 10^8 * (10^6 – (Número de usuarios – 1))	= 10^8 * (10^8 – (Número de usuarios – 1))

Formas de mejorar la protección contra la adivinación de un código válido:

:: Utilizando un código con más dígitos (códigos con 6 u 8 dígitos),
:: Tipos más avanzados de autorización (como "Confirmación de tarjeta con un código" o "Doble autorización").

Formas de controlar el JABLOTRON 100+

En local:

:: Teclado del sistema
:: Mando del sistema
:: Ordenador a través de conexión por cable USB y software J-Link

De forma remota:

:: Aplicación smartphone MyJABLOTRON
:: Ordenador a través del interfaz web MyJABLOTRON
:: Menú de voz usando el teléfono
:: SMS a través del teléfono
:: Ordenador a través de internet con el software J-Link
:: Llamada perdida desde un número de teléfono autorizado (sólo para controlar salidas programables)

El sistema JABLOTRON 100+ puede ser controlado a través de diversos módulos de acceso, los cuales le permiten, no solo controlar, sino también visualizar el estado de cada segmento individual. El sistema se puede controlar directamente (armar o desarmar el sistema y funciones de automatización) usando los segmentos de dos botones del teclado. Los botones de segmento están claramente identificados y coloreados (usando la lógica del semáforo) de manera que el estado de cada segmento está indicado claramente. Un segmento también puede utilizarse para indicar un estado (ej. puerta del garaje abierta) o para controlar diferentes dispositivos automatizados (por ejemplo, la calefacción o las persianas). El número máximo de segmentos que se pueden añadir a un módulo de acceso es de 20. También se puede configurar un segmento para llamar solicitando ayuda en caso de emergencia (alarma médica o de pánico).

2.1. CONTROL EN LOCAL

- **VERDE PERMANENTE**
  DESARMADO | OFF
- **VERDE INTERMITENTE**
  RETRASO DE ENTRADA
- **ROJO INTERMITENTE**
  ALARMA | MEMORIA DE ALARMA
- **VERDE PERMANENTE**
  TODO OK
- **VERDE INTERMITENTE**
  CONTROL
- **VERDE INTERMITENTE 2X CADA 2 S**
  MANTENIMIENTO
- **AMARILLO PERMANENTE**
  FALLO
- **AMARILLO INTERMITENTE**
  ARMADO SIN ÉXITO

- **ROJO PERMANENTE**
  ARMADO | ON
- **ROJO INTERMITENTE**
  ALARMA |
  MEMORIA DE ALARMA
- **AMARILLO PERMANENTE**
  ARMADO PARCIAL
- MÓDULO DE ACCESO
  LECTOR | TECLADO

Los diferentes tipos de módulos de acceso y sus combinaciones

Lector de tarjetas RFID

Permite controlar el sistema a través de los segmentos y autorización por métodos sin contacto (tarjeta / tag RFID).

Teclado con lector de tarjetas

el usuario puede controlar el sistema a través de los segmentos y autorización, tanto introduciendo un código o el método sin contacto (tarjeta / tag RFID), o una combinación de ambas para mayor seguridad.

Teclado con pantalla LCD y lector de tarjetas

el usuario puede controlar el sistema a través de los segmentos y autorización, tanto introduciendo un código, método sin contacto (tarjeta / tag RFID), ambos código y tarjeta / tag para mayor seguridad, o autorizando y utilizando las opciones disponibles en la pantalla LCD del teclado.

Cuando desarmamos la alarma utilizando los botones del segmento siempre se requiere de una autorización de usuario

Para armar la alarma y controlar procesos automatizados a través de los botones del segmento, la autorización de usuario es opcional para cada segmento.

Los usuarios pueden autorizarse introduciendo su código asignado o a través de su tarjeta / tag RFID.

Cada usuario puede disponer de un código y hasta dos chips RFID (tarjetas o tags).

Tags recomendados: JABLOTRON 100+, Oasis u otros de terceros compatibles con 125 kHz EM. Si se requiere una mayor seguridad, el sistema de alarma puede ser armado por un usuario con autorización configurada utilizando tags RFID y códigos (opcional).

Si el usuario quiere controlar múltiples segmentos simultáneamente, debe autorizarse y después presionar los segmentos de las particiones particulares. De esta forma los usuarios pueden, por ejemplo, armar la casa y desarmar el garaje con una sola autorización.

Si el parámetro "Código con prefijo" está habilitado, la autorización por código en el teclado puede consistir en hasta 11 dígitos: un prefijo (de uno a tres dígitos), un asterisco * (que separa el prefijo y el código principal), y un código de 4,6 u 8 dígitos en función de la configuración (por ejemplo: 123*12345678, o 1*12345678). Todos los usuarios pueden cambiar sus propios códigos, que siguen el prefijo. El código puede ser cambiado desde la pantalla LCD del teclado, desde el software J-Link o la app MyJABLOTRON.

Si el parámetro "Código con prefijo" está habilitado, los usuarios pueden estar habilitados para cambiar sus códigos. Si el parámetro "Código con prefijo" está deshabilitado, los códigos solamente pueden ser cambiados por el Administrador.

2.1.2. CÓDIGO DE AUTORIZACIÓN

La autorización de un usuario con código se realiza tecleando un código válido en el teclado o con un tag RFID.

Es posible usa códigos de 4, 6 u 8 dígitos en el sistema.

El sistema puede ser configurado para ser utilizado con códigos con o sin prefijo (ajuste por defecto). Para sistemas de alarma con un mayor número de usuarios se pueden habilitar los prefijos. Para cambiar esta opción, por favor contacte con el técnico de servicio de su sistema de alarma.

Código sin prefijo: CCCC

cccc es un código de 4, 6 u 8 dígitos, códigos permitidos desde 0000 a 99999999

Código de panel de control por defecto Administrador: **1234; 123456; 12345678;**

Código con prefijo: nnn*cccc

nnn es el prefijo, que se corresponde con el número de posición del usuario (posición 0 a 600)

* es un separador (tecla *)

cccc es un código de 4, 6 u 8 dígitos, códigos permitidos desde 0000 a 99999999

Código de panel de control por defecto Administrador: **1*1234; 1*123456; 1*12345678;**

ADVERTENCIA: El código de Administrador principal empieza con el prefijo **1**

El código de Servicio principal empieza con el prefijo **0**

Para cambiar el código, por favor contacte con el técnico de servicio de su sistema de alarma.

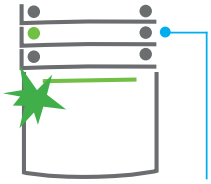
Estructura y descripción del menú interno del teclado LCD

Autorización de Administrador o Usuario a través de código o tarjeta / tag RFID

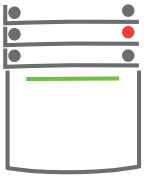
CANCELAR INDICACIÓN DE MEMORIA DE ALARMA	Permite cancelar una indicación de alarma / armado sin éxito en todas las particiones a las que el usuario tiene derecho de acceso.
CONTROL DE PARTICIONES	Permite controlar las particiones del sistema a las que el usuario tiene derecho de acceso y están habilitadas en los ajustes internos.
CONTROL DE PGS	Permite controlar las salidas programables PG a las que el usuario tiene permiso y de acuerdo con los ajustes internos.
MEMORIA DE EVENTOS	Muestra una lista detallada de eventos en memoria.
SE EVITÓ LA CONEXIÓN	Muestra una lista de todos los detectores que evitan el armado del sistema, siempre que esta opción esté activada en la configuración del panel de control.
AVERÍAS DEL SISTEMA	Muestra una lista de todos los detectores que indican fallos en el sistema desde las particiones a las que el usuario tiene derechos.
DETECTORES APAGADOS	Muestra una lista de todos los detectores bloqueados en las particiones a las que el usuario tiene derecho de acceso.
ESTADO DEL SISTEMA	Muestra el estado del sistema (lista de detectores activos, contactos de sabotaje activos, bajas baterías, autobypasses, etc.).
CONFIGURACIÓN	Permite editar usuarios y dispositivos (sólo cuando el USB está desconectado).
AJUSTES DE PANTALLA	Permite ajustar el brillo de la iluminación y el contraste de la pantalla.
MODO MANTENIMIENTO	Permite al Administrador particiones asignadas al modo Mantenimiento.

2.1.2.1. ARMAR LA ALARMA

1. Autorizarse usando el tecla-do. Las particiones que pueden ser controladas se iluminan y el boton indicador retroilumi-nado empezara a parpadear en verde.



2. Presione el botón derecho (uno que no este iluminado) para armar una particion en particular. Es posible armar mas particiones de forma consecutiva. El retraso entre la seleccion de particiones no debe sobrepasar los 2 segun-dos.



3. El comando es ejecutado y el teclado indica acusti-camente el retaso de salida. La particion se arma ahora y solo los detectores con reaccion "Zona retrasada" proporcionan el tiempo para dejar el area vigi-lada durante el retraso de salida. El boton del segmento de la particion armada se enciende en rojo.

Durante el armado de la alarma, si hay algún detector activo (ej. una ventana abierta) el sistema reaccionará de una de las siguientes formas (en base a la configuración del sistema):

:: Los detectores vigilarán automáticamente después de que vuelven a su estado normal (ajuste por defecto).

:: El sistema indicará ópticamente los detectores activos con un parpadeo rojo del segmento durante 8 segundos, tras los cuales el sistema se armará automáticamente.

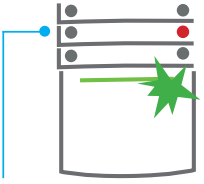
:: El armado de la partición con detectores activos también es posible simplemente pulsando de nuevo el botón de la derecha del segmento. De esta forma el usuario confirma su intención de armar la partición con un detector activo (ej. una ventana abierta). De otro modo, la partición no se armará con un detector activo.

:: Un detector active evitará el armado de la partición. Este estado se indica ópticamente por un parpadeo del botón rojo del segmento. El detector que evita el armado se mostrará en el menú de la pantalla del teclado LCD.

Un armado sin éxito se indica a través del parpadeo amarillo del botón indicador (el parámetro "Armado sin éxito" debe estar habilitado). Consulte con su técnico de servicio a fi n de programar el comportamiento deseado del sistema.

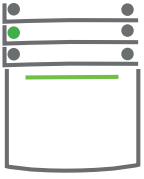
2.1.2.2. DESARMAR LA ALARMA

1. Cuando entra en un edifi cio (activando un detector con reaccion "Zona retrasada"), el sistema empieza a indicar el retraso de entrada con un tono continuo y parpadeo del boton verde del segmento que tiene esa particion asociada, en la



que se ha generado el retraso de entrada.

Autorícese utilizando el teclado – la luz de indicacion verde del panel de autorización empieza a parpadear.



2. Presionar el botón izquierdo del segmento de las particiones que quiere desarmar.

3. El comando se ejecuta y los segmentos se volveran verdes indicando que las parti-ciones estan desarmadas.

Nota: Si el parámetro "Desarmar partición con autorización solo durante el retraso de entrada" está habilitado, entonces la mera autorización desarmará la partición donde se haya generado el retraso de entrada. Consulte con su técnico de servicio a fi n de programar el comportamiento deseado del sistema.

2.1.2.3. ACCESO CON CÓDIGO DE COACCIÓN

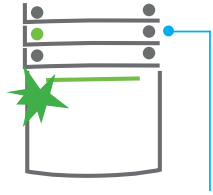
Esta función permite desarmar el sistema de un modo especial. El sistema aparentemente se desarma, sin embargo, también genera una alarma de pánico silencioso, que es reportada a los usuarios seleccionados (incluyendo CRA). El desarmado bajo coacción se lleva a cabo sumando 1 al último número de un código válido.

Ejemplo para un código con prefijo:
Código válido: 2*9999
Código para desarmar bajo coacción: 2*9990

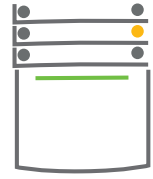
Ejemplo para un código sin prefijo:
Código válido: 9999
Código para desarmar bajo coacción: 9990

2.1.2.4. ARMADO PARCIAL DE LA ALARMA

1. **Autorícese utilizando el teclado** (introduzca un código o pase una tarjeta o tag por el lector). El botón indicador retroiluminado verde empezará a parpadear.



2. **Presione el botón** derecho del segmento de la partición seleccionada.



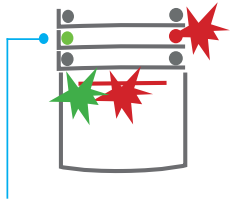
3. **El comando se ejecuta** y el segmento se volverá amarillo indicando que la partición está armada parcialmente.

El sistema también puede configurarse para ser armado de forma parcial, lo que permite la vigilancia solo de ciertos detectores en una partición. Ejemplo: por la noche, es posible armar solamente los detectores de puertas y ventanas, dejando los detectores de movimiento interiores sin ninguna reacción.

Para armar totalmente la partición que tiene el armado parcial habilitado, se tendrá que hacer una doble pulsación en el botón de armar. Tras la primera pulsación del botón parpadeará en amarillo y tras la segunda pulsación parpadeará en rojo. Si el sistema está armado en parcial – indicado por una iluminación continua en amarillo – el sistema se puede armar totalmente a través de una autorización y pulsación del botón amarillo. Una vez que el botón es presionado, el sistema se armará totalmente y el botón se vuelve rojo.

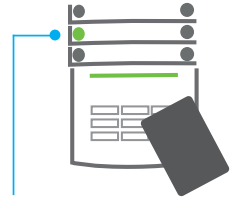
2.1.2.5. FINALIZAR UN SALTO DE ALARMA

1. **Autorícese utilizando** el teclado (introduzca un código o pase una tarjeta o tag por el lector).



2. **Presione el botón** izquierdo del segmento de la particion donde se ha generado una alarma.

3. **Se desarma el sistema** y las sirenas se silencian. El parpadeo del boton verde indica el desarmado de la particion indicada. El parpadeo rojo indica una memoria de alarma.



4. **Autorícese y presione** el boton verde de nuevo para cancelar la indicacion de memoria de alarma.

5. **El segmento indica el desarmado** de la particion con la iluminacion permanente del boton verde.

Un salto de alarma en curso se indica con un parpadeo rápido del botón rojo del segmento e indicación del botón retroiluminado del teclado. Es necesario autorizarse utilizando el teclado para terminar la alarma. La partición continúa armada, y un parpadeo rápido del botón rojo del segmento indica la memoria de alarma. La indicación se mantendrá activada incluso después de que el sistema haya sido desarmado.

Si la indicación de la memoria de alarma fue activada durante su ausencia, busque la causa de la alarma en el historial de eventos y extreme las precauciones al acceder e inspeccione la instalación o espere a que llegue el guardia de seguridad (en caso de que su sistema esté conectado a una Central Receptora de Alarmas).

La indicación de memoria de alarma permanece en el segmento hasta que el sistema se arma de nuevo. También puede ser cancelada desarmando el sistema una vez más. Además, la indicación de memoria de alarma se puede cancelar desde el Menú principal de un teclado con pantalla LCD – Cancelar memoria de alarma.

La indicación de la activación de una alarma de sabotaje solo puede finalizarse a través del técnico de Servicio o Administrador.

Nota: Cuando se utiliza el perfil del sistema "EN 50131-1, grade 2", siempre es necesario autorizarse primero y después realizar la acción deseada.

Terminar una alarma utilizando un mando a distancia también desarmará la partición correspondiente.

2.1.2.6. CONTROL DE UNA PARTICIÓN DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD

Los estados de las particiones se muestran en la parte superior izquierda de la pantalla. Un armado total de una partición se muestra a través de un número en un rectángulo con el fondo color negro 2; un armado parcial se representa a través de un número enmarcado 4.

Control desde el menú del teclado:

:: Autorícese a través de un código válido o un chip RFID.
:: Acceda al menú pulsando ENTER.
:: Control de particiones → ENTER.
:: Seleccione la partición deseada utilizando las flechas.
:: Pulsando ENTER repetidamente cambiará los estados de la partición (armado parcial / armado / desarmado).
:: Pulse ESC para salir al menú.

2.1.3. UTILIZANDO LOS TECLADOS DEL SISTEMA JA-110E Y JA-150E

Los estados de cada partición individual son indicados por los indicadores de estado A, B, C, D sobre el display LCD y los botones de función. El panel de control se puede manejar directamente (armar o desarmar la alarma y otras funciones de automatización) utilizando los botones de función del teclado. Los botones de función y los indicadores de estado A, B, C, D están retroiluminados para indicar claramente el estado de la partición.

:: VERDE – Desarmado :: AMARILLO – Armado parcial :: ROJO – Armado

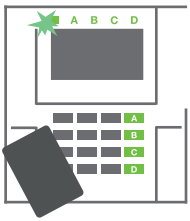
La autorización se puede señalizar introduciendo un código de acceso en el teclado o utilizando una tarjeta/tag RFID asignada al usuario en particular. Cada usuario puede tener un código y un chip RFID (tarjeta o tag). Si el usuario quiere controlar múltiples particiones simultáneamente, debe autorizarse y después presionar los botones de función de las particiones particulares consecutivamente. De esta forma el usuario puede desarmar todas las particiones (por ejemplo, la casa y el garaje) con una simple autorización.

Estructura y descripción del menú interno del teclado LCD

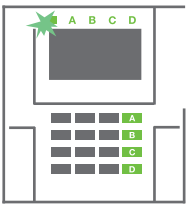
Autorización de Administrador o Usuario a través de código o tarjeta / tag RFID

CANCELAR INDICACIÓN DE MEMORIA DE ALARMA	Permite cancelar una indicación de alarma / armado sin éxito en todas las particiones a las que el usuario tiene derecho de acceso.
CONTROL DE PARTICIONES	Permite controlar las particiones del sistema a las que el usuario tiene derecho de acceso y están habilitadas en los ajustes internos.
CONTROL DE PGS	Permite controlar las salidas programables PG a las que el usuario tiene permiso y de acuerdo con los ajustes internos.
MEMORIA DE EVENTOS	Muestra una lista detallada de eventos en memoria.
SE EVITÓ LA CONEXIÓN	Muestra una lista de todos los detectores que evitan el armado del sistema, siempre que esta opción esté activada en la configuración del panel de control.
AVERÍAS DEL SISTEMA	Muestra una lista de todos los detectores que indican fallos en el sistema desde las particiones a las que el usuario tiene derechos.
DETECTORES APAGADOS	Muestra una lista de todos los detectores bloqueados en las particiones a las que el usuario tiene derecho de acceso.
ESTADO DEL SISTEMA	Muestra el estado del sistema (lista de detectores activos, contactos de sabotaje activos, bajas baterías, autobypasses, etc.).
CONFIGURACIÓN	Permite editar usuarios y dispositivos (sólo cuando el USB está desconectado).
AJUSTES DE PANTALLA	Permite ajustar el brillo de la iluminación y el contraste de la pantalla.
MODO MANTENIMIENTO	Permite al Administrador particiones asignadas al modo Mantenimiento.

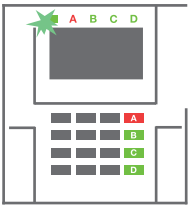
2.1.3.1. ARMAR LA ALARMA



1. Autorícese utilizando el teclado. Los botones de función A, B, C, D de particiones que tiene permitidos controlar se encenderán y el indicador del sistema empezará a parpadear en verde.



2. Presione el botón de función para armar la partición particular. Es posible armar más particiones consecutivamente. El retraso entre la selección de las particiones no debe ser mayor a 2 segundos.



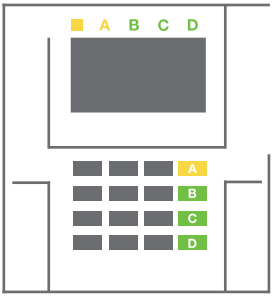
3. El comando se ejecuta y el teclado indica acústicamente el retraso de salida. La partición está ahora armada, solo los detectores con reacción "Zona retrasada" proporcionan tiempo para dejar el área vigilada durante el retraso de salida.
El indicador de estado y el botón de función de armado de la partición se encenderán en rojo.

Durante el armado de la alarma, si hay algún detector activo (ej. una ventana abierta) el sistema reaccionará de una de las siguientes formas (en base a la configuración del sistema):

:: El panel de control se armará. Los detectores activos serán bloqueados automáticamente. *).
:: El sistema indicará ópticamente los detectores activos con un parpadeo rojo del botón de función durante 8 segundos, tras los cuales el panel de control se armará automáticamente (los detectores activos serán bloqueados). *)
:: Armar la partición con detectores activos también es posible simplemente presionando el botón de función de nuevo. El usuario debe confirmar la intención de armar la partición con un detector activo (ej. una ventana abierta). De otro modo el sistema no se armará.
:: Un detector active evitará el armado. Este estado se indica ópticamente por un parpadeo rojo del botón de función. El detector que evita el armado se mostrará en el menú de la pantalla del teclado LCD.

*) **ADVERTENCIA**: Las opciones a) y b) no son compatibles con EN 50131, grade. 2 (perfil de sistema del panel de control)

Si un detector con la reacción "Alarma de zona instantánea" se activa durante un retraso de salida o si un detector con reacción "Alarma de zona retrasada" permanece activo una vez finalizado el retraso de salida, el panel de control se desarmará de nuevo. Se indicará un armado sin éxito a través del indicador del sistema parpadeando en amarillo, se reportará a la CRA y se indicará a través de la sirena externa (aplica para seguridad Grado 2).

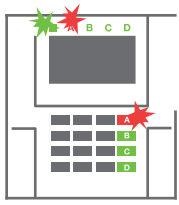


Si el panel de control está configurado para armar sin autorización, entonces no es necesario autorizarse. Todo lo que tiene que hacer es presionar el botón de función de la partición particular. Es posible configurar el panel de control para armar simplemente a través de autorización.

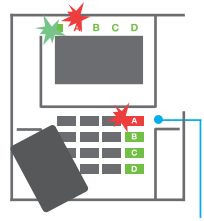
ADVERTENCIA: Armar automáticamente sin autorización disminuye el frado máximo de seguridad a Grado 1. Considere todos los posibles riesgos al utilizar esta función.

Consulte la instalación con un consultor de proyecto o un técnico de servicio para programar el comportamiento deseado del sistema de alarma.

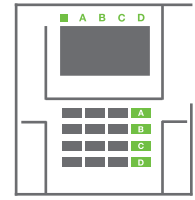
2.1.3.2. DESARMAR LA ALARMA



1. Cuando entre en el inmueble (activando un detector con reacción "Zona retrasada"), el sistema empieza a indicar el retraso de entrada con un tono continuo, el indicador de sistema y un botón de función, ambos parpadeando en rojo, de la partición en que se ha generado el retraso de entrada.



2. Autorícese utilizando el teclado – el indicador de sistema empezará a parpadear en verde.



3. El Presione los botones de función de las particiones que quiere desarmar.

4. Comando es ejecutado. Los botones de función y el indicador de sistema se vuelven verdes indicando las particiones desarmadas.

Nota: Si el parámetro "Desarmar partición a través de autorización solo durante el retraso de entrada" está habilitado, entonces la mera autorización desarmará la partición donde se haya generado el retraso de entrada. Esta opción se debe utilizar con precaución cuando se utilizan múltiples particiones.

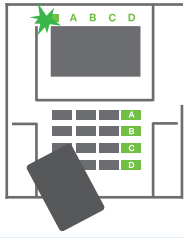
Consulte la instalación con un técnico de servicio para programar el comportamiento deseado del sistema de alarma.

2.1.3.3. ARMADO PARCIAL DE LA ALARMA

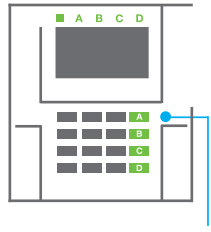
ADVERTENCIA: Esta es una función adicional del sistema de alarma.

El sistema también puede ser configurado para ser armado parcialmente, lo que permite que solo ciertos detectores vigilen en una partición.

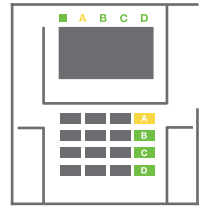
Ejemplo: Por la noche, es posible armar solamente los detectores de puerta y ventanas, mientras los detectores de movimiento seleccionados no generarán una alarma cuando alguien se mueva dentro de la partición.



1. Autorícese utilizando el teclado (introduzca un código o pase una tarjeta o tag por el lector). El botón indicador de sistema empezará a parpadear en verde.



2. Presione el botón de función de la partición seleccionada.



3. El comando es ejecutado y el botón de función se vuelve permanentemente amarillo para indicar el armado parcial de la partición.

Para armar totalmente la instalación en la cual está habilitado el armado parcial, mantenga presionado el botón para armar el panel de control durante 2 segundos o presiónelo dos veces. Después de presionar una vez el botón este se muestra continuamente iluminado en amarillo, tras la segunda pulsación se muestra iluminado continuamente en rojo.

Si el sistema ya está armado en parcial – el botón de función se muestra continuamente iluminado en amarillo – el sistema se puede armar totalmente a través de una autorización y presionando el botón amarillo durante un tiempo más largo. Una vez soltado el botón, el sistema estará totalmente armado y el botón se vuelve rojo.

El armado parcial puede ser configurado de tal manera que no se requiera autorización.

Para desarmar el panel de control cuando está parcialmente armado, presione el botón amarillo. El panel de control se desarmará y el botón se vuelve verde.

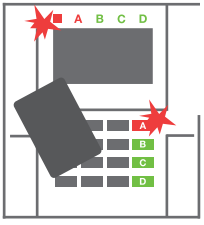
2.1.3.4. CONTROL DE ACCESO POR COACCIÓN

Le permite desarmar el panel de control de un modo especial. El sistema aparentemente se desarma, sin embargo, genera una alarma de pánico silencioso que es reportada a los usuarios seleccionados (incluyendo CRA).

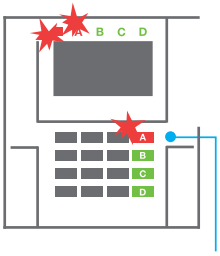
El desarmado bajo coacción se lleva a cabo sumando 1 al último número de un código válido. Contacte con su técnico de servicio si quiere utilizar esta funcionalidad.

Ejemplo: Código válido: 9999 Código para desarmar bajo coacción: 9990

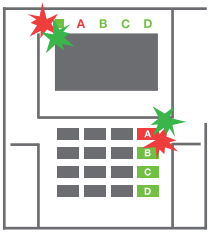
2.1.3.5. FINALIZAR UN SALTO DE ALARMA



1. **Autorícese utilizando el teclado** (introduzca un código o pase una tarjeta o tag por el lector).



2. **Presione el botón** de función de la partición en la cual se ha generado la alarma.



3. **Se desarma el sistema** y las sirenas se silencian. Los botones de función parpadean alternativamente (verde/rojo) y los indicadores de estado indican la memoria de alarma.

Un salto saldo de alarma en curso se indica por el parpadeo rojo del indicador estado y el botón de función. Es necesario autorizarse utilizando el teclado para terminar la alarma. La partición continúa armada, y un parpadeo rápido rojo del botón de función indica la memoria de alarma. La indicación se mantendrá activa incluso después de que el sistema haya sido desarmado.

ADVERTENCIA: Si la indicación de la memoria de alarma fue activada durante su ausencia, extreme siempre las precauciones al acceder, busque la causa de la alarma en el historial de eventos y tenga mucho cuidado al inspeccionar la instalación o espere a que llegue el guardia de seguridad (en caso de que su sistema esté conectado a una Central Receptora de Alarmas).

La indicación de memoria de alarma permanece en el sistema hasta que el sistema se arma de nuevo. Alternativamente, puede ser cancelada desde el menú del teclado. Menú principal – Cancelar memoria de alarma. La indicación de una alarma de sabotaje solo puede finalizarse a través de un técnico de Servicio o un Administrador.

Nota: Cuando se utiliza el perfil del sistema "Por defecto", es posible seleccionar una acción en particular y presionar un botón de función primero y después confirmarla a través de autorización utilizando el teclado.

Terminar una alarma utilizando un mando a distancia también desarmará la partición correspondiente.

2.1.3.6. MANEJANDO EL SISTEMA CON UN MANDO A DISTANCIA

El mando debe estar asignado al sistema por su instalador. Puede estar asociado a usuarios específicos lo que evitará notificaciones por SMS al usuario que está interactuando con el sistema (si los parámetros de notificaciones están configurados de esa manera). Los mandos controlan e indican el estado de su batería y están equipados con un indicador óptico y acústico.

MANDOS BIDIRECCIONALES

Las funciones del botón se diferencian por los iconos del candado. El candado cerrado arma las particiones programadas; el icono con el candado abierto las desarma. La ejecución correcta de un comando se confirma a través del LED; desarmado – verde, armado – rojo. Un fallo de comunicación (fuera de rango del panel de control) se indica a través de un parpadeo amarillo del LED. Los botones con símbolos de círculo y circunferencia pueden controlar otra partición. Los botones del mando también pueden configurarse para controlar salidas PG de diferentes modos: el primer botón activa/ el Segundo desactiva, cada botón puede tener una función individual cuando se utilicen las funciones impulso o cambio. Para más funciones, es posible presionar los dos botones al mismo tiempo. De esta forma, el mando de 4 botones puede tener hasta 6 funciones individuales o estados de salidas PG (ej. encender y apagar luces), alternativamente dos salidas PG (ej. una puerta de garaje y cerradura eléctrica).

Si el sistema está configurado para Armar después de confirmación (capítulo 2.1.1) el detector indicará el armado sin éxito con el encendido del LED verde si el dispositivo está activado. Es necesario confirmar el armado presionando el botón del candado cerrado de nuevo. El armado de la partición será confirmado a través del LED rojo.

Los botones del mando se pueden bloquear para evitar pulsaciones accidentales. El comando será enviado entonces cuando se presione el botón repetidamente. La indicación de batería baja se indica acústicamente (con 3 tonos) y ópticamente con un parpadeo amarillo del LED después de la presionar un botón.

Para más información consulte la configuración del mando con su técnico de servicio.

MANDOS UNIDIRECCIONALES

Los mandos unidireccionales envían una señal cada vez que se pulsa un botón sin recibir confirmación por parte del panel de control. El envío de la señal se confirma solamente por un parpadeo corto rojo del LED y con un tono.

2.2. CONTROL EN REMOTO

El servicio MyJABLOTRON proporciona la mayor comodidad para controlar y administrar el sistema de forma remota. El interfaz web MyJABLOTRON es el único servicio que permite el acceso on-line a los dispositivos JABLOTRON. Esto permite al usuario final monitorizar y controlar el sistema. Está disponible tanto en forma de app para smartphone como en aplicación web. El servicio MyJABLOTRON permite a los usuarios:

:: Ver el estado actual del sistema,
:: Armar / desarmar el sistema al complete o parte de él,
:: Control de salidas programables,
:: Ver el historial de eventos,
:: Envío de reportes a usuarios seleccionados vía SMS, e-mail o notificaciones PUSH,
:: Captura de imágenes desde dispositivos de foto-verificación y navegar a través de la pestaña Galería de fotos o directamente en los Eventos recientes,
:: Monitorizar temperatura actual o consumo de energía, incluyendo una historia de registros o gráficos,
:: Y otras características útiles.

Dependiendo de su país o región, un socio JABLOTRON autorizado puede crearle una cuenta web para MyJABLOTRON. El login es la dirección email del usuario. La contraseña para el primer inicio de sesión se enviará a ese email. Esta contraseña puede cambiarse en los ajustes del usuario en cualquier momento.

2.2.1. MANEJANDO EL SISTEMA USANDO LA APP PARA SMARTPHONE MyJABLOTRON

Una vez que se ha creado la cuenta de usuario, el usuario puede monitorizar y controlar el sistema a través de la app MyJABLOTRON para Smartphones Android e iOS.

2.2.2. MANEJANDO EL SISTEMA A TRAVÉS DEL INTERFAZ WEB MyJABLOTRON

El sistema JABLOTRON puede manejarse fácil y convenientemente utilizando su ordenador a través de internet y el interfaz web MyJABLOTRON, que está accesible desde www.myjablotron.com.

2.2.3. MANEJANDO EL SISTEMA USANDO EL MENÚ DE VOZ

El sistema puede controlarse desde un teléfono mediante un simple menú de voz, el cual guía al usuario a través de una serie de opciones en el lenguaje configurado previamente. Para acceder al menú de voz solamente tiene que llamar al número de teléfono de su sistema de alarma.

El acceso al menú de voz se puede habilitar para todos los números sin restricciones o solamente para números de teléfono autorizados y guardados en el panel de control. Dependiendo de la configuración, se requerirá autorizarse introduciendo un código válido a través del teclado del teléfono. Cuando el usuario entra en el menú, el sistema le dará información actualizada del estado actual de todas las particiones asignadas al usuario. El remitente de la llamada puede controlar esas particiones, tanto individual como colectivamente, utilizando el teclado del teléfono y las opciones del menú disponibles.

Por defecto, el sistema está configurado para responder las llamadas entrantes después de tres tonos (aproximadamente 15 segundos).

2.2.4. MANEJANDO EL SISTEMA A TRAVÉS DE COMANDOS SMS

Los comandos SMS pueden controlar particiones individuales y salidas programables igual que los botones de un segmento del teclado. La forma del mensaje de texto para manejar el sistema es: CODIGO_COMANDO. Los comandos actuales están predefinidos (ARMAR/DESARMAR) con un parámetro numérico adicional que identifica una partición específica.

Un SMS puede controlar múltiples particiones al mismo tiempo. En ese caso, añada los números de las particiones en el comando Ejemplo de un comando SMS para armar las particiones 2 y 4:

CODIGO_CONECTAR_2_4

Los comandos para manejar salidas programables pueden ser programados por el instalador del sistema. Por ejemplo, podría elegir CERRAR PERSIANAS como su comando para cerrar las persianas de sus ventanas. También es posible configurar el sistema para que no se requiera un código antes de un comando. En este caso el comando es simplemente identificado automáticamente una vez que el sistema reconoce el número de teléfono del usuario desde el que fue enviado el SMS. Esta configuración es realizada por un técnico de servicio.

2.2.5. MANEJO DEL SISTEMA REMOTAMENTE USANDO UN ORDENADOR (J-LINK)

El sistema JABLOTRON 100+ puede ser controlado remotamente utilizando un ordenador con el software J-Link. Se puede descargar desde la sección “Descargas” de la página **www.myjablotron.com**.

2.2.6. CONTROL DE SALIDAS PROGRAMABLES (PG)

2.2.6.1. SEGMENTO DEL TECLADO

Una salida PG se puede activar pulsando el botón derecho de un segmento y desactivarla pulsando el botón izquierdo. Si la salida está configurada como impulso, se desactivará una vez pase el tiempo preconfigurado. El control de la PG puede ser guardado, o no, en la memoria de eventos del panel de control. Esta configuración la realiza el técnico de servicio.

Puede requerir autorización, o no, en base a la configuración del sistema.

2.2.6.2. AUTORIZACIÓN DE UN USUARIO EN EL TECLADO

Es posible activar una salida PG solamente con la autorización de un usuario (introduciendo un código o utilizando tag RFID). La salida PG debe ser configurada para activarse desde un teclado asignado.

2.2.6.3. DESDE EL MENÚ DEL TECLADO CON PANTALLA LCD

Después de la autorización del usuario se pueden controlar las salidas programables desde el menú del teclado con pantalla LCD. El usuario tendrá acceso a las salidas programables dependiendo de sus permisos.

Control desde el menú del teclado:

:: Autorícese con un código válido o un chip RFID.
:: Acceda al menú pulsando ENTER.
:: Control PG → ENTER.
:: Seleccione el grupo de PGs deseado utilizando las flechas (1–32), (33–64), (65–96), (97–128) → ENTER.
:: Seleccione la PG deseada utilizando las flechas → ENTER.
:: Presionando ENTER repetidamente cambiará el estado de la PG (el estado activo de la PG se muestra con el número de la PG un rectángulo con el fondo color negro .
:: Presionar ESC para salir al menú.

2.2.6.4. MANDO

A través de la pulsación de un botón asignado en el mando. El mando bidireccional confirma la activación de una salida PG con el indicador LED.

2.2.6.5. APP PARA SMARTPHONE MyJABLOTRON

Pulsando ON/OFF en la pestaña Automatización (PG).

2.2.6.6. INTERFAZ WEB MyJABLOTRON

Pulsando ON/OFF en la pestaña Automatización (PG).

2.2.6.7. LLAMADA PERDIDA

Cada número de teléfono almacenado en el sistema (un usuario puede tener un número de teléfono) puede controlar la PG a través de una llamada perdida (sin establecer la llamada). La llamada perdida consiste en llamar al número de la tarjeta SIM utilizada por el sistema de seguridad y colgar antes de que el sistema conteste la llamada. Por defecto, el sistema contestará la llamada después de tres tonos (aproximadamente 15 segundos).

2.2.6.8. MENSAJE SMS

Enviando un SMS puede activar/desactivar una PG en particular. Puede requerir autorización, o no, en base a la configuración del sistema.

Ejemplo: CODIGO_TEXTO CONFIGURADO

3. BLOQUEANDO/DESHABILITANDO EL SISTEMA

3.1. BLOQUEO DE USUARIOS

Cualquier usuario puede ser temporalmente bloqueado (ej. cuando un usuario pierde su tarjeta/tag o se revela su código). Cuando se bloquea un usuario, su código ID o tarjeta/tag no serán aceptados por el sistema. El usuario tampoco recibira ninguna alerta por mensaje de texto ni informe de voz en su telefono.

Solo el administrador del sistema o el técnico de servicio pueden bloquear un usuario. Un metodo para retirar permisos de acceso es a través del teclado LCD, seleccionando Configuración / de los usuarios / Usuario / Bypass y seleccionar "SI". Otra opción es bloquear un usuario, local o remotamente, utilizando el software J-Link en Ajustes / Usuarios / Bloqueo de usuarios.

Un usuario bloqueado (deshabilitado) se marcara con un circulo rojo hasta que el bloqueo sea cancelado.

3.2. BLOQUEO DE DETECTORES

Un detector puede bloquearse temporalmente de un modo similar al de un usuario. Un detector se desactiva cuando no su activación no es deseada temporalmente (por ejemplo, un detector de movimiento en una habitación con una mascota o deshabilitar el sonido de una sirena). El sistema todavía supervise el estado del contacto de sabotaje y envía eventos de servicio, pero la función de alarma está desactivada.

Sólo el administrador o el técnico de servicio pueden bloquear un detector. Se puede realizar a través del teclado LCD seleccionando Configuración / Dispositivos periféricos / bypass y seleccionar "SI". Otra opción es utilizar el software J-Link, pulsando en Ajustes/ Diagnóstico / Deshabilitar en el detector individual. Un detector bloqueado se marcará con un círculo amarillo hasta que se cancele el bloqueo utilizando el mismo procedimiento. También se puede bloquear un detector a través de la app para smartphone MyJABLOTRON.

3.3. DESHABILITAR CALENDARIO

Para deshabilitar eventos programados automáticamente por el calendario del Sistema, se puede deshabilitar ese calendario. Deshabilitando un evento de calendario (ej. desarmar el sistema para vigilancia nocturna a una hora predeterminada) se detendrá la ejecución de ese evento (ej. durante las vacaciones).

El calendario se puede deshabilitar local o remotamente a través del software J-Link seleccionando Ajustes / Calendarios / Bloqueado. Un calendario deshabilitado se marcará con un círculo rojo hasta que se vuelva a habilitar utilizando el mismo procedimiento.

4. PERSONALIZANDO EL SISTEMA

4.1. CAMBIAR CÓDIGO DE ACCESO DE USUARIO

Si el sistema esta configurado con códigos sin prefijo, solamente el administrador y el técnico de servicio pueden cambiar los códigos de seguridad. El administrador del sistema puede realizar los cambios tanto desde el menu del teclado LCD como desde el software J-Link y la app para smartphone MyJABLOTRON. El código puede cambiarse tras la autorización seleccionando Configuración / de los usuarios / Usuario / Código. Para introducir un nuevo código debe entrar en modo editar presionando Enter (el código empezara a parpadear), introducir el nuevo código y confirmarlo presionando Enter de nuevo. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique ".Guardar configuraciones?"

Si el sistema esta configurado con códigos con prefijo, los usuarios individuales pueden ser habilitados para cambiar sus propios códigos desde el menu del teclado LCD.

4.2. CAMBIAR, ELIMINAR O AÑADIR TARJETA/TAG RFID

Si el sistema esta configurado con códigos sin prefijo, solamente el administrador y el técnico de servicio pueden cambiar los códigos de seguridad. El administrador del sistema puede realizar los cambios tanto desde el menu del teclado LCD como desde el software J-Link y la app para smartphone MyJABLOTRON. El Código puede cambiarse tras la autorizacion seleccionando Configuración / de los usuarios / Usuario / Código. Para introducir un nuevo código debe entrar en modo editar presionando Enter (el código empezara a parpadear), introducir el nuevo código y confirmarlo presionando Enter de nuevo. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique ".Guardar configuraciones?".

Si el sistema esta configurado con códigos con prefijo, los usuarios individuales pueden ser habilitados para cambiar sus propios códigos desde el menu del teclado LCD.

4.3. CAMBIAR NOMBRE DE USUARIO O NÚMERO DE TELÉFONO

Si el sistema esta configurado con códigos con prefijo, los usuarios pueden números, cambiar o borrar sus números de telefono o cambiar sus nombres a través del menu del teclado LCD. Esto se puede realizar tras autorizarse, seleccionando Configuración / de los usuarios / Usuario / tel. El usuario debe entrar en modo editar para hacer los cambios. Esto se hace pulsando Enter. Despues de hacer los cambios, deben confirmarse pulsando Enter de nuevo. Para borrar un numero de telefono introduzca "0" en el campo del numero de telefono. Una vez realizados los cambios, estos deben ser confirmados seleccionando Guardar cuando el sistema le indique "¿Guardar configuraciones?"

El administrador del sistema y el técnico de servicio pueden añadir, cambiar y eliminar números de teléfono o nombres de usuarios tanto desde el menú del teclado LCD como desde el software J-Link.

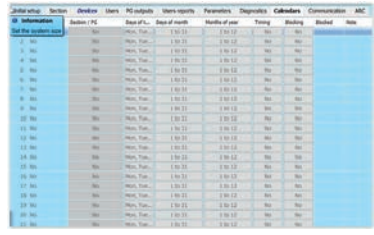
4.4. AÑADIR/ELIMINAR UN USUARIO

Sólo el administrador del Sistema o el técnico de servicio pueden añadir nuevos usuarios al Sistema (o eliminarlos). Los nuevos usuarios pueden ser añadidos al sistema (o eliminados de él) solamente a través del software J-Link, o el software F-Link en el caso del técnico.

Al crear un nuevo usuario, es necesario asignarle permisos de acceso (derechos), particiones que el usuario puede manejar, salidas programables que puede controlar y el tipo de autorización que será necesaria.

4.5. AJUSTES DE EVENTOS POR CALENDARIO

Es posible configurar eventos por calendario (desarmar/armar/ armar parcialmente, control o bloqueo de salidas PG). Los calendarios se pueden configurar a través del J-Link en la pestaña Calendarios.



Para cada evento de calendario se puede activar, partición o salida PG y el tiempo del evento. El día se puede definir como un día de semana, mes o año. Para el día seleccionado puede configurar hasta 4 eventos para realizar una acción o armado de partición en intervalos regulares.

Por lo tanto, los eventos de calendario se pueden personalizar no solo para el control de particiones sino también para controlar varias tecnologías en el objeto utilizando salidas PG.

5. HISTORIAL DE EVENTOS

El sistema de seguridad almacena todas las acciones realizadas y eventos (armados, desarmados, alarmas, fallos, mensajes enviados a usuarios y CRAs) en la tarjeta micro SD del panel de control del sistema. Cada entrada incluye la fecha, hora (inicio y fi n), y fuente (causa / origen) del evento.

Las diferentes vías de buscar a través del historial de eventos del sistema:

5.1. UTILIZANDO EL TECLADO LCD

El acceso al historial de eventos a través del teclado requiere la autorización del usuario. Una vez autorizado, se mostraran las opciones disponibles (en base a los permisos del usuario) y podra encontrar Memorias de eventos. Los registros pueden verse utilizando las flechas.

5.2. UTILIZANDO EL SOFTWARE J-LINK Y UN ORDENADOR

La memoria del sistema puede visualizarse utilizando el software J-Link. Los eventos se pueden descargar del panel de control en grupos reducidos (sobre 1,200 eventos) o grandes (sobre 4,000 eventos). Pueden ser filtrados en detalle, marcados en colores para una identificacion mas sencilla o guardados en un archivo de su ordenador.

5.3. INICIANDO SESIÓN EN MyJABLOTRON (WEB/SMARTPHONE)

Todos los eventos del sistema pueden verse despues de iniciar sesion en el interfaz web/Smartphone MyJABLOTRON. La cuenta muestra el historial en el rango que corresponde a los permisos de los usuarios.

6. ESPECIFICACIONES TÉCNICAS

PARÁMETRO	JA-103K		JA-107K	
Alimentación del panel de control	~ 110–230 V / 50–60 Hz, máx. 0.28 A con fusible F1.6 A/250 V Protección clase II		~ 110–230 V / 50–60 Hz, máx. 0.85 A con fusible F1.6 A/250 V Protección clase II	
Batería de respaldo	12 V; 2.6 Ah (gel de plomo)		12 V; 7 a 18 Ah (gel de plomo)	
Tiempo de carga máx. para batería	72 h			
Voltaje BUS (rojo - negro)	12,0 a 13,8V			
Consumo máx. corriente continua desde el panel de control	1000 mA		2000 mA permanente 3000 mA en 60 minutos (máx. 2000 mA en un BUS)	
Consumo máx. corriente continua para 12 horas de respaldo	Sin comunicador GSM	LAN – OFF 115 mA LAN – ON 88 mA	Válido para batería de respaldo 18 Ah	
			Sin comunicador GSM	LAN – OFF 1135 mA LAN – ON 1107 mA
	Con comunicador GSM	LAN – OFF 80 mA LAN – ON 53 mA	Con comunicador GSM	LAN – OFF 1100 mA LAN – ON 1072 mA
Número máx. de dispositivos	50		230	
Comunicador LAN	INTERFAZ ETHERNET, 10/100BASE-T			
Dimensiones	268 x 225 x 83 mm		357 x 297 x 105 mm	
Peso con/sin AKU	1844 g/970 g		7027 g/1809 g	

PARÁMETRO	JA-103K	JA-107K
Reacción ante entrada de código incorrecto	Alarma tras 10 entradas de código incorrecto	
Memoria de eventos	Apróx. Últimos 7 millones de eventos, incluyendo fecha y hora	
Unidad de alimentación	Tipo A (de acuerdo con EN 50131-6)	
Comunicador GSM (2G)	850 / 900 / 1800 / 1900 MHz	
Clasificación	Seguridad grado 2 / Entorno clase II (de acuerdo con EN 50131-1)	
Entorno de operación	Interior general	
Rango de temperatura de operación	-10 °C a +40 °C	
Humedad media de operación	75 % RH, non-condensing	
Cumple con	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	
Frecuencia de operación de radio (con el módulo JA 11xR)	868.1 MHz, protocolo JABLOTRON	
Emisiones radio	ETSI EN 300 220-1,-2 (módulo R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7	
Conformidad de seguridad	EN 62368-1+A11	
Condiciones de operación	ERC REC 70-03	
Organismo certificador	Trezor Test s.r.o. (no. 3025)	
Identificación de llamada (CLIP)	ETSI EN 300 089	

JABLOTRON ALARMS a.s. declara mediante la presente que los paneles de control JA-103K y JA-107K cumplen con la legislación relevante de la Unión Europea: Directivas No: 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU, cuando se utiliza como se indica. La declaración original se puede encontrar en www.jablotron.com – sección Descargas.

Nota: Aunque estos productos no contienen materiales nocivos para la salud le recomendamos devolver el producto a su distribuidor o directamente al fabricante tras su uso.

TABLE DES MATIÈRES

MAINTENANCE PÉRIODIQUE

:: I est nécessaire d'avoir des contrôles de maintenance réguliers et opportuns afin de garantir un fonctionnement fi able du système. La plupart des travaux de maintenance sont réalisés par une société d'installation au moins une fois par an au cours des inspections de maintenance périodiques.

:: Les tâches de maintenance de l'utilisateur consistent à maintenir propres les périphériques individuels. L'ADMINISTRATEUR du système peut passer en mode MAINTENANCE pour pouvoir ouvrir les détecteurs (changer les piles) ou les retirer de l'installation. Voir avec l'entreprise d'installation la demande relative à l'établissement du mode MAINTENANCE. Si le système est configuré sur le profil système « EN 50131-1, niveau 2 », le mode MAINTENANCE n'est pas disponible.

:: Le système peut être commuté sur le mode maintenance via le logiciel J-Link ou depuis le menu du clavier avec écran LCD. Après autorisation, un « mode Maintenance » peut être sélectionné avec le choix des sections où la maintenance est requise. En mode Maintenance, aucune alarme ne sera déclenchée dans les sections sélectionnées, y compris l'ouverture ou le retrait des détecteurs de l'installation.

:: Le mode Maintenance est signalé par la touche d'activation clignotant en vert (2 clignotements toutes les 2 secondes) et par les deux touches éteintes du segment de la section particulière.

:: Lors de la manipulation des périphériques, il faut veiller à ne pas endommager le plastique et les mécanismes des détecteurs.

:: Avant de retirer le capot, la languette fixant généralement le capot doit être légèrement enfoncée dans le corps du détecteur avec un petit outil (par exemple un tournevis). Dans certains cas, la languette est sécurisée avec une petite vis de verrouillage qui doit être dévissée en premier.

:: Lors du remplacement des piles dans le détecteur, toujours remplacer toutes les piles du détecteur en même temps (utiliser des piles du même type et du même fabricant).

:: Certains appareils peuvent nécessiter des tests (détecteurs d'incendie, par exemple). Pour de plus amples informations, contacter le technicien de service.

1. INTRODUCTION

Le système JABLOTRON 100+ est conçu pour 600 utilisateurs au maximum et peut être divisé en 15 sections distinctes. Jusqu'à 230 détecteurs peuvent être connectés et le système propose jusqu'à 128 usages multiples des sorties programmables (par exemple la domotique).

2. UTILISATION DU SYSTÈME JABLOTRON 100+

Le système de sécurité peut être commandé de différentes manières. Pour désarmer l'alarme, une autorisation sous forme d'identification de l'utilisateur est toujours requise. Le système détecte l'identité des utilisateurs et leur permet d'utiliser les zones du système pour lesquelles la commande leur a été attribuée. Il est possible de choisir différents types d'armement, avec ou sans autorisation. Lorsque le type d'autorisation standard est utilisé, il n'est nul besoin de s'autoriser soi-même, le système pouvant être armé en appuyant simplement sur la touche adéquate du segment sur le clavier. Le nom de l'utilisateur, la date et l'heure sont enregistrés et sauvegardés dans la mémoire du système à chaque accès au système. Cette information est disponible sans limite de temps. Tout utilisateur peut également annuler une alarme déclenchée (arrêt des sirènes) par simple autorisation dans n'importe quelle zone du système (en fonction de ses droits d'accès). Cela ne désarmera toutefois pas automatiquement le système (à moins que le paramétrage par défaut de celui-ci ne soit modifié).

Remarque: selon la configuration des paramètres de l'installation et du système, certaines des options décrites ci-dessous peuvent ne pas être disponibles. Consulter la configuration de l'installation avec le technicien de service.

Utilisateurs et leurs droits d'accès

CODE D'AUTORISATION	DESCRIPTION DU TYPE
Code de télésurveillance (ARC)	Ce code dispose du plus haut niveau d'autorisation pour configurer le comportement du système et est exclusivement h dges et des cartes RFID. Il permet également d'effacer l'alarme et la mémoire d'alarme de sabotage. Le nombre de codes de télésurveillance n'est limité dans le système que par la capacité restante de la centrale et aucun code de télésurveillance n'est prédéfini par défaut.
Code Service (Service)	Ce code peut accéder au mode Service et configurer le comportement du système. Il peut accéder à tous les onglets et options, y compris la communication avec la télésurveillance, sauf si l'accès est limité par un technicien de la télésurveillance. Tant que le paramètre « Droit restreint d'administrateur - Service / Télésurveillance » reste décoché, le code Service peut commander toutes les sections et les sorties PG utilisées dans le système. Il peut créer des utilisateurs dotés d'une permission ARC, d'autres techniciens de service, des administrateurs et d'autres utilisateurs avec un niveau inférieur d'autorisation qui leur est attribué par des codes, des badges et des cartes RFID. Il permet également d'effacer l'alarme et la mémoire d'alarme de sabotage. Le nombre de codes Service est uniquement limité par la capacité restante de la centrale. Par défaut, le code est 1010. L'utilisateur Service occupe toujours la position 0 dans la centrale et il ne peut être effacé.
Code Administrateur (Principal)	Ce code donne toujours l'accès complet à toutes les sections et est autorisé à commander toutes les sorties PG. L'administrateur peut créer un autre administrateur et d'autres codes avec un niveau inférieur d'autorisation et leur attribuer un accès aux sections et aux sorties PG, des codes d'accès, des puces et des cartes RFID. Ce code permet d'effacer la mémoire d'alarme. Il ne peut y avoir qu'un seul code Administrateur principal, qui ne peut être effacé. Lorsque le paramètre « Droit restreint d'administrateur - Service / Télésurveillance » est activé, le code Administrateur doit être autorisé pour confirmer l'accès. Par défaut, le code est 1234. L'utilisateur Administrateur principal occupe toujours la position 1 et il ne peut être effacé.
Code Administrateur (Autre)	Ce code permet l'accès aux sections choisies par l'Administrateur principal pour lesquelles un autre administrateur peut ajouter de nouveaux utilisateurs avec un niveau d'autorisation similaire ou inférieur pour commander les sections et les sorties PG, leur attribuer des codes d'accès, des badges et des cartes RFID. Ce code donne l'autorisation d'effacer la mémoire d'alarme dans les sections attribuées. Lorsque le paramètre « Droit restreint d'administrateur - Service / Télésurveillance » est activé, le code Administrateur doit être autorisé pour confirmer l'accès aux techniciens de service et à la télésurveillance. Le nombre de codes Administrateur (autre) est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.

CODE D'AUTORISATION	DESCRIPTION DU TYPE
Code d'utilisateur	Ce code donne l'accès, du fait des droits attribués par un administrateur, aux commandes de sections et PG. Les utilisateurs peuvent ajouter / supprimer leurs badges RFID et leurs cartes d'accès et modifier leurs propres numéros de téléphone. Les utilisateurs peuvent modifier leurs codes à condition que le système utilise des codes préfixés. Il donne l'autorisation d'effacer la mémoire d'alarme dans les sections attribuées. Les utilisateurs sélectionnés peuvent voir leur accès aux sections limité par un calendrier. Le nombre de codes d'utilisateur est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.
Code d'armement	Ce code est autorisé uniquement pour armer une section désignée et est autorisé à commander les sorties PG (MARCHE/ARRÊT) qui nécessitent une autorisation. Les utilisateurs avec ce niveau d'autorisation ne sont pas autorisés à modifier leur code et ne sont pas autorisés à effacer la mémoire d'alarme. Le nombre de codes d'armement est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.
Code PG seulement	Ce code permet à l'utilisateur de commander les sorties programmables par seule autorisation. Cela concerne aussi bien la mise sous tension que hors tension. Les utilisateurs avec ce niveau d'autorisation ne sont pas autorisés à modifier leur code et ne sont pas autorisés à effacer la mémoire d'alarme. Le nombre de codes PG est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.
Code Détresse	Ce code est uniquement autorisé pour déclencher une alarme de détresse. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Détresse est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.
Code Surveillance	Ce code est destiné à une agence de sécurité. Ce niveau d'autorisation permet d'armer l'ensemble du système. Cependant, le code Surveillance peut désarmer le système uniquement lors d'une alarme ou ultérieurement après l'expiration, tant que la mémoire d'alarme est toujours active. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Surveillance est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.
Code Déblocage	Ce code sert à débloquer le système après le verrouillage du système par une alarme. Un utilisateur de ce code ne peut pas le modifier ou effacer la mémoire d'alarme. Le nombre de codes Déblocage est uniquement limité par la capacité restante de la centrale. Il n'y a pas de code défi ni par défaut.

Sécurité des codes d'accès, des dispositifs sans contact RFID et des commandes à distance :

Une centrale permet à chaque utilisateur de se voir attribuer un code à 4, 6 ou 8 chiffres et jusqu'à deux badges RFID pour l'autorisation du système. L'autorisation de l'utilisateur est requise lors de chaque manipulation via le clavier, le menu vocal, un ordinateur, Internet ou des applications mobiles. La longueur du code impacte le nombre de combinaisons possibles et donc la sécurité du code.

Le nombre de combinaisons du code dépend des configurations suivantes :

Paramètres de la centrale	4 CHIFFRES	6 CHIFFRES	8 CHIFFRES
Code avec préfixe » activé	= 10^4 = (10.000)	= 10^6 = (1.000.000)	= 10^8 = (100.000.000)
« Code avec préfixe » et **« Contrôle d'accès par contrainte »** désactivés	= 10^4 – (Nombre d'utilisateurs – 1)	= 10^6 – (Nombre d'utilisateurs – 1)	= 10^8 – (Nombre d'utilisateurs – 1)

Paramètres de la centrale	4 CHIFFRES	6 CHIFFRES	8 CHIFFRES
« Code avec préfixe » désactivé ; **« Contrôle d'accès par contrainte »** activé	≤ 10^4 – ((Nombre d'utilisateurs – 1) * 3)	≤ 10^6 – ((Nombre d'utilisateurs – 1) * 3)	≤ 10^8 – ((Nombre d'utilisateurs – 1) * 3)
Par seule utilisation d'un **badge RFID** dans une plage de 14 caractères (6 constants + 8 variables)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
« Code avec préfixe » et **« Confirmation de la carte avec un code »** activés	= (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 avec préfixe » désactivé ; **« Confirmation de la carte avec un code »** activé	= 10^8 * (10^4 – (Nombre d'utilisateurs – 1))	= 10^8 * (10^6 – (Nombre d'utilisateurs – 1))	= 10^8 * (10^8 – (Nombre d'utilisateurs – 1))

Méthodes d'amélioration de la protection contre la reconnaissance d'un code valide :

:: Utilisation d'un code avec plusieurs chiffres (codes à 6 ou 8 chiffres)
:: Des types plus avancés d'autorisation, tels que les « Confirmation de la carte avec un code » ou « Double autorisation ».

Modes de fonctionnement du système JABLOTRON 100+

Sur le site :

:: Clavier du système
:: Commande du système
:: Ordinateur par l'intermédiaire d'un câble USB et du programme J-Link

À distance :

:: MyJABLOTRON - Application pour mobiles
:: Ordinateur via l'interface Internet MyJABLOTRON
:: Téléphone à l'aide du menu vocal
:: Téléphone à l'aide de SMS
:: Ordinateur - via Internet à l'aide du programme J-Link
:: Numérotation à partir d'un numéro de téléphone autorisé (uniquement pour le fonctionnement des sorties programmables)

Le système JABLOTRON 100+ peut être commandé par de nombreux modules d'accès qui permettent non seulement de contrôler, mais aussi d'afficher les états des segments individuels. Le système peut être utilisé directement (armement ou désarmement du système et des fonctions d'automatisation) en utilisant les segments à deux touches du clavier. Les touches étiquetées des segments sont, de manière claire, signalées par une couleur (en utilisant la logique de signalisation) de sorte que l'état de chaque segment est indubitablement visible. Un segment peut également être utilisé pour indiquer un état (par ex. une porte de garage ouverte) ou commander divers dispositifs automatisés (par ex. le chauffage ou les volets). Il y a au maximum 20 segments pour un module d'accès. Un segment peut également être configuré pour appeler à l'aide en cas d'urgence (alarme relative à un état de santé ou de détresse).

2.1. EXPLOITATION SUR SITE

VERT CONTINU
DÉSARMÉ | ÉTEINT
VERT CLIGNOTANT
ENTRÉE TEMPORISÉE

ROUGE CLIGNOTANT
ALARME | MÉMOIRE D'ALARME
VERT CONTINU
OK
VERT CLIGNOTANT
COMMANDE
CLIGNOTE EN VERT 2X TOUTES LES 2 SECONDES
MAINTENANCE
JAUNE CONTINU
DÉFAILLANCE
CLIGNOTEMENT JAUNE
DÉFAILLANCE DE L'ARMEMENT

ROUGE CONTINU
ARMÉ | ALLUMÉ
ROUGE CLIGNOTANT
ALARME |
MÉMOIRE D'ALARME

JAUNE CONTINU
ARMÉ PARTIELLEMENT

LECTEUR DE CARTE | CLAVIER

Les différents types de modules d'accès et leurs combinaisons :

Lecteur de carte RFID

Permet de commander le système en utilisant des segments et un dispositif sans contact d'autorisation de l'utilisateur (carte / badge RFID).

Clavier avec lecteur de carte

L'utilisateur peut commander le système avec les segments et une autorisation, en saisissant un code d'accès, avec un dispositif sans contact (carte / badge RFID) ou par combinaison des deux méthodes pour une meilleure sécurité.

Clavier avec affichage LCD et lecteur de carte

L'utilisateur peut commander le système avec les segments et une autorisation, en utilisant un code, un dispositif sans contact (carte / badge RFID), le code et les carte / badge pour une meilleure sécurité ou en autorisant et en utilisant les options disponibles sur l'écran LCD du clavier.

Lors du désarmement de l'alarme à l'aide des touches du segment, l'autorisation de l'utilisateur est toujours requise. Lors de l'armement de l'alarme et de la commande des procédures automatisées en utilisant les touches du segment, l'autorisation de l'utilisateur est facultative pour chaque Segment.

Un utilisateur peut s'autoriser lui-même en saisissant son code attribué ou en utilisant ses carte / badge RFID. Chaque utilisateur peut avoir un code et jusqu'à deux puces RFID (cartes ou badges).

Puces sans contact recommandées : JABLOTRON 100+, Oasis ou autres puces tierces compatibles avec EM 125 kHz. En cas de nécessité d'un niveau de sécurité supérieur, le système d'alarme peut être configuré pour utiliser la double méthode d'autorisation avec des puces RFID et des codes (fonction en option). Si les utilisateurs veulent commander plusieurs segments simultanément, ils doivent s'autoriser eux-mêmes puis enclencher ultérieurement les segments des sections particulières. De cette façon, les utilisateurs peuvent par exemple armer le domicile et désarmer le garage avec une autorisation unique. Si le paramètre « Code avec préfixe » est activé, Le code d'autorisation du clavier peut comprendre jusqu'à onze chiffres : un préfixe (de un à trois chiffres), un astérisque * (qui sépare le préfixe du code principal) et un code à 4, 6 ou 8 chiffres en fonction de la configuration (par exemple : 123*12345678 ou 1*12345678). Tous les utilisateurs peuvent modifier leur propre code qui suit le préfixe. Le code peut être modifié à partir du clavier doté de l'écran LCD, du logiciel J-Link ou de l'application MyJABLOTRON.

Si le paramètre « Code avec préfixe » est activé, les utilisateurs peuvent être autorisés à modifier leur code. Si le paramètre « Code avec préfixe » est désactivé, les codes ne peuvent être modifiés que par l'administrateur.

2.1.2. AUTORISATION AVEC UN CODE SUR LE CLAVIER

L'autorisation avec un code d'utilisateur est donnée par la saisie d'un code valide sur le clavier ou avec un badge RFID. L'autorisation avec un code d'utilisateur est donnée par la saisie d'un code valide sur le clavier ou avec un badge RFID.

Il est possible d'utiliser des codes à 4, 6 ou 8 chiffres dans le système.

Le système peut être configuré pour être utilisé avec des codes dotés ou non d'un préfixe (réglage par défaut). Pour les systèmes d'alarme dotés d'un nombre important d'utilisateurs, le préfixe peut être activé. Pour modifier cette option, contacter le technicien de service de votre système d'alarme.

Code sans préfixe : CCCC

cccc est un code à 4, 6 ou 8 chiffres, les codes autorisés étant compris entre 0000 et 99999999

Code par défaut de la centrale Administrateur : **1234; 123456; 12345678;**

Code sans préfixe : nnn*cccc

nnn est le préfixe correspondant au numéro de la position de l'utilisateur (position 0 à 600)

* est le séparateur (touche *)

cccc est un code à 4, 6 ou 8 chiffres, les codes autorisés étant compris entre 0000 et 99999999

Code par défaut de la centrale — Administrateur : **1*1234; 1*123456; 1*12345678;**

AVERTISSEMENT : Le code Administrateur principal commence par le préfixe **1**

Le code Service commence avec le préfixe **0**

Pour modifier le type de code, contacter le technicien de service de votre système d'alarme.

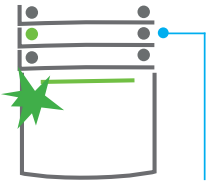
Structure et description du menu du clavier LCD interne

Autorisation Administrateur ou Utilisateur avec un code ou des badge / carte RFID

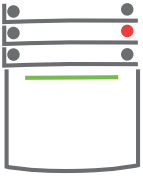
ANNULER L'INDICATION D'AVERTISSEMENT	Permet l'effacement de l'indication des alarme / défaillance d'armement dans toutes les sections pour lesquelles l'utilisateur détient des droits d'accès.
COMMANDE DE LA SECTION	Permet de commander les sections du système pour lesquelles l'utilisateur détient des droits d'accès et qui sont activées dans les paramètres internes.
COMMANDE PG	Permet à l'utilisateur de commander les sorties programmables PG en fonction des autorisations de l'utilisateur et des paramètres internes.
MÉMOIRE ÉVÈNEMENTIELLE	Affiche la liste détaillée de la mémoire évènementielle.
ARMEMENT EMPÊCHÉ	Affiche la liste des détecteurs déclenchés empêchant l'armement du système, à condition que cette option soit activée dans les paramètres de la centrale.
DÉFAILLANCES DANS LE SYSTÈME	Affiche une liste de tous les détecteurs indiquant les défaillances du système à partir des sections pour lesquelles l'utilisateur détient des droits d'accès.
DÉTECTEURS DÉRIVÉS	Affiche la liste de tous les détecteurs bloqués dans les sections pour lesquelles l'utilisateur détient des droits d'accès.
STATUT DU SYSTÈME	Affiche le statut du système (liste des détecteurs déclenchés, des contacts de sabotage déclenchés, du niveau faible des batteries, des dérivations, etc.).
PARAMÉTRAGES	Permet l'édition des utilisateurs et des périphériques (uniquement en cas de déconnexion USB).
RÉGLAGE DE L'AFFICHAGE	Permet de régler la luminosité du rétro-éclairage du clavier et le contraste de l'affichage.
MODE SERVICE	Permet à l'administrateur de basculer les sections attribuées sur le mode Service.

2.1.2.1. ARMEMENT DE L'ALARME

1. Autoriser à l'aide du clavier.
Les sections qui peuvent être commandées sont allumées et la touche d'indication rétroéclairée commencera à clignoter en vert.



2. Appuyer sur la touche droite (celle qui n'est pas allumée) pour armer une section particulière. Il est possible d'armer plusieurs sections par la suite. Le délai entre la sélection des sections ne doit pas être supérieur à 2 secondes.



3. La commande est exécutée et le clavier signale par voie acoustique la temporisation de sortie. La section est maintenant armée, seuls les détecteurs avec une réaction « Zone temporisée » donnent le temps de quitter la zone protégée pendant la temporisation de sortie. La touche du segment de la section armée passe au rouge.

Pendant l'armement de l'alarme, si un quelconque détecteur est activé (par ex. une fenêtre ouverte), le système va réagir (en fonction de la configuration du système) de l'une des manières suivantes :

:: Les détecteurs passeront automatiquement en mode de surveillance après être passés en mode Veille (réglage par défaut).

:: Le système signalera par voie optique les détecteurs déclenchés par un segment clignotant en rouge pendant 8 secondes et le système armera automatiquement une fois ladite période expirée.

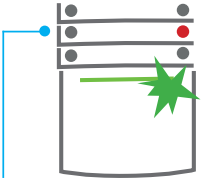
:: L'armement de la section avec des détecteurs déclenchés est également possible en enclenchant de manière répétée la touche du segment située à droite. L'utilisateur confirme ainsi l'intention d'armer la section avec un détecteur déclenché (par ex. une fenêtre ouverte). Le cas échéant, la section avec le détecteur déclenché ne sera pas armée.

:: Le détecteur déclenché empêchera alors l'armement de la section. Cet état est signalé par voie optique avec la touche du segment clignotant en rouge. Le détecteur empêchant l'armement sera signalé sur le menu de l'écran LCD du clavier.

Une défaillance d'armement est indiquée par la touche de signalisation clignotant en jaune (le paramètre « Défaillance d'armement » doit être activé). Indiquer les choix de l'installation au technicien de service afin de programmer le comportement requis pour le système.

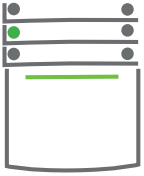
2.1.2.2. DÉSARMEMENT DE L'ALARME

1. En entrant dans le bâtiment (déclenchement d'un détecteur avec une réaction « Zone temporisée »), le système commence à signaler la temporisation d'entrée par une tonalité continue et le clignotement de la touche verte du segment



de la section dans laquelle la temporisation d'entrée a été déclenchée.

S'autoriser à l'aide du clavier – le voyant indicateur vert du panneau exclusivement dges et commence à clignoter.



2. Enclencher la touche gauche du segment de la section devant être désarmée.

3. La commande est exécutée et les touches du segment passent au vert pour indiquer le désarmement des sections.

Remarque : si le paramètre « Désarmer la section par autorisation uniquement durant la temporisation d'entrée » est activé, la simple autorisation désarmera la section où la temporisation d'entrée a été déclenchée. Indiquer les choix de l'installation au technicien de service afin de programmer le comportement requis pour le système.

2.1.2.3. COMMANDE D'ACCÈS SOUS LA CONTRAINTE

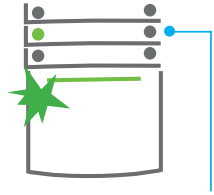
Cette fonction désarme le système dans un mode particulier. Le système est apparemment désarmé, mais il déclenche une alarme de détresse silencieuse, qui est signalée aux utilisateurs sélectionnés (y compris la télésurveillance). Le désarmement sous la contrainte est réalisé en ajoutant 1 au dernier numéro du code valide.

Exemple pour un code avec préfixe :
Code valide : 2*9999
Code de désarmement sous la contrainte : 2*9990

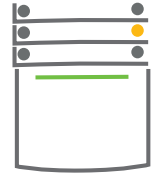
Exemple pour un code sans préfixe :
Code valide : 9999
Code de désarmement sous la contrainte : 9990

2.1.2.4. ARMEMENT PARTIEL DE L'ALARME

1. **S'autoriser à l'aide du clavier** (saisir un code ou placer un badge ou une carte sur le lecteur). La touche d'indication rétroéclairée verte se met à clignoter.



2. **Enclencher la touche droite** du segment de la section choisie.



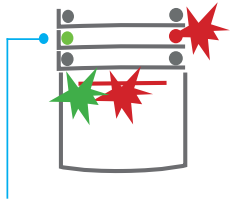
3. **La commande est exécutée** et la touche du segment passe au jaune pour signaler la section partiellement désarmée.

Le système peut également être configuré pour être partiellement armé, ce qui permet la surveillance partielle par certains détecteurs dans une section. Exemple : la nuit, il est possible d'armer uniquement les détecteurs de portes et de fenêtres, alors que les détecteurs de mouvement à l'intérieur du domicile ne réagissent pas.

Pour armer la totalité des locaux dans lesquels l'armement partiel est activé, la touche d'armement du système doit être enclenchée deux fois. Après le premier enclenchement de la touche, elle clignote en jaune, après le second, elle clignote en rouge. Si le système est partiellement armé - signalé en continu par le voyant jaune - l'ensemble du système peut être totalement armé par autorisation et en enclenchant la touche jaune. Une fois que la touche est enclenchée, le système sera entièrement armé et la touche passera au rouge.

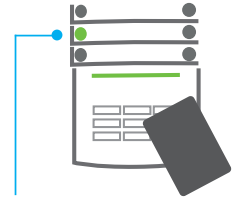
2.1.2.5. ARRÊT D'UNE ALARME DÉCLENCHÉE

1. **S'autoriser soi-même** à l'aide du clavier (saisir un code, placer un badge sur le lecteur).



2. **Enclencher la touche** gauche du segment de la section dans laquelle l'alarme a été déclenchée.

3. **Le désarmement se termine** et les sirènes sont réduites au silence. La touche verte clignotante indique le désarmement de la section particulière. La lumière rouge clignotante indique la mémoire d'alarme.



4. **S'autoriser soi-même** et appuyer à nouveau sur la touche verte pour annuler l'indication de la mémoire d'alarme.

5. **Le segment indique** la section désarmée avec une touche verte allumée en permanence.

Une alarme déclenchée en cours est signalée par un clignotement rouge rapide de la touche du segment et la touche d'indication rétroéclairée. Il faut s'autoriser soi-même à l'aide du clavier afin de mettre fi n à l'alarme. La section reste armée, la touche rouge du segment clignotant rapidement indique la mémoire d'alarme. Le clignotement de signalisation continuera même après le désarmement du système.

Si l'indication de mémoire d'alarme a été activée lors d'une absence, rechercher l'origine de l'alarme dans l'historique événementiel et être très prudent en entrant et en vérifant les locaux ou attendre jusqu'à ce que l'agence de sécurité arrive (à condition que le système soit connecté à une télésurveillance).

L'indicateur mémoriel d'alarme du segment reste allumé jusqu'à ce que le système soit armé une fois de plus. Il peut être stoppé à défaut en désarmant le système une fois de plus. L'indication d'alarme peut également être annulée à partir du menu principal du clavier doté d'un écran LCD - Annuler l'indication d'avertissement.

L'indication d'une alarme de sabotage déclenchée ne peut être annulée que par un technicien de service ou un administrateur.

Remarque : lorsque le profil système « EN 50131-1, niveau 2 » est utilisé, il est toujours nécessaire de s'autoriser soi-même en premier lieu puis de mettre en oeuvre l'action souhaitée.

L'arrêt d'une alarme à l'aide d'une télécommande désarmera également la section correspondante.

2.1.2.6. COMMANDE D'UNE SECTION À PARTIR DU MENU DU CLAVIER AVEC ÉCRAN LCD

Les états des sections sont affi chés dans la partie supérieure gauche de l'écran LCD du clavier. Une section entièrement armée est indiquée par un numéro dans un rectangle noir 2 ; une section partiellement armée est représentée par un numéro encadré 4 .

Commande à partir du menu du clavier :

:: Autorisation par un code valide ou une puce RFID
:: Entrer dans le menu en appuyant sur ENTER
:: Commande de la section → ENTER
:: Sélectionner la section souhaitée à l'aide des flèches
:: Les statuts des sections partiellement armé / armé / désarmé seront modifiés en appuyant sur ENTER à plusieurs reprises.
:: Appuyer sur ESC pour quitter le menu.

2.1.3. UTILISATION DES CLAVIERS DU SYSTÈME JA-110E ET JA-150E

Les états des sections individuelles sont indiqués par les indicateurs d'état A, B, C, D au-dessus de l'affichage LCD et par les touches fonctionnelles. La centrale peut être utilisée directement (armement ou désarmement de l'alarme et des autres fonctions d'automatisation) en utilisant les touches fonctionnelles sur le clavier. Les touches fonctionnelles et les indicateurs d'état A, B, C, D colorés sont rétroéclairés afin d'indiquer clairement l'état de la section.

:: VERT – Désarmé :: JAUNE – Partiellement désarmé :: ROUGE – Armé

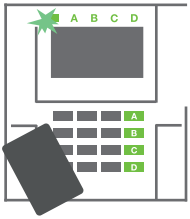
L'autorisation peut être donnée en saisissant un code d'accès sur le clavier ou en utilisant des carte / badge RFID attribuées à un utilisateur particulier. Chaque utilisateur peut avoir un code et une puce RFID (une carte ou un badge). Si les utilisateurs veulent commander plusieurs sections simultanément, ils doivent s'autoriser eux-mêmes puis enclencher par la suite les touches fonctionnelles des sections particulières. Les utilisateurs peuvent ainsi désarmer toutes les sections (par exemple le domicile et le garage) avec une autorisation unique.

Structure et description du menu du clavier LCD interne

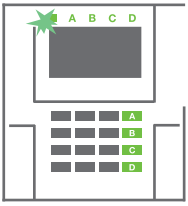
Autorisation Administrateur ou Utilisateur avec un code ou des badge / carte RFID

ANNULER L'INDICATION D'AVERTISSEMENT	Permet l'effacement de l'indication des alarme / défaillance d'armement dans toutes les sections pour lesquelles l'utilisateur détient des droits d'accès.
COMMANDE DE LA SECTION	Permet de commander les sections du système pour lesquelles l'utilisateur détient des droits d'accès et qui sont activées dans les paramètres internes.
COMMANDE PG	Permet à l'utilisateur de commander les sorties programmables PG en fonction des autorisations de l'utilisateur et des paramètres internes.
MÉMOIRE ÉVÈNEMENTIELLE	Affiche la liste détaillée de la mémoire évènementielle.
ARMEMENT EMPÊCHÉ	Affiche la liste des détecteurs déclenchés empêchant l'armement du système, à condition que cette option soit activée dans les paramètres de la centrale.
DÉFAILLANCES DANS LE SYSTÈME	Affiche une liste de tous les détecteurs indiquant les défaillances du système à partir des sections pour lesquelles l'utilisateur détient des droits d'accès.
DÉTECTEURS DÉRIVÉS	Affiche la liste de tous les détecteurs bloqués dans les sections pour lesquelles l'utilisateur détient des droits d'accès.
STATUT DU SYSTÈME	Affiche le statut du système (liste des détecteurs déclenchés, des contacts de sabotage déclenchés, du niveau faible des batteries, des dérivations, etc.).
PARAMÉTRAGES	Permet l'édition des utilisateurs et des périphériques (uniquement en cas de déconnexion USB).
RÉGLAGE DE L'AFFICHAGE	Permet de régler la luminosité du rétro-éclairage du clavier et le contraste de l'affichage.
MODE SERVICE	Permet à l'administrateur de basculer les sections attribuées sur le mode Service.

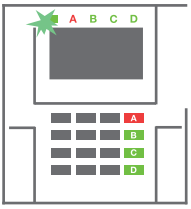
2.1.3.1. ARMEMENT DE L'ALARME



1. S'autoriser soi-même avec le clavier. Les touches fonctionnelles A, B, C, D des sections pour lesquelles il existe une autorisation de commande s'allument et le voyant du système commence à clignoter en vert.



2. Appuyer sur la touche fonctionnelle pour armer une section particulière. Il est possible d'armer plusieurs sections par la suite. Le délai entre le choix des sections ne doit pas être supérieur à 2 secondes.



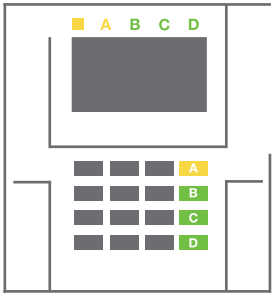
3. La commande est exécutée et le clavier signale par voie acoustique la temporisation de sortie. La section est maintenant armée, seuls les détecteurs avec une réaction « Zone temporisée » donnent le temps de quitter la zone protégée pendant la temporisation de sortie. L'indicateur d'état et la touche fonctionnelle de la section armée passent au rouge.

Pendant l'armement de l'alarme, si un quelconque détecteur est déclenché (par ex. une fenêtre ouverte), le système va réagir (en fonction de la configuration du système) de l'une des manières suivantes :

:: La centrale s'armera d'elle-même. Les détecteurs déclenchés seront bloqués automatiquement. *)
:: Le système signalera par voie optique les détecteurs déclenchés par une touche fonctionnelle clignotant en rouge pendant 8 secondes et la centrale armera automatiquement une fois ladite période expirée (les détecteurs déclenchés seront bloqués). *)
:: L'armement de la section avec des détecteurs déclenchés est également possible en enclenchant de manière répétée la touche fonctionnelle. L'utilisateur doit confirmer l'intention d'armer la section avec un détecteur déclenché (par ex. une fenêtre ouverte). Le cas échéant, le système ne s'armera pas.
:: Le détecteur déclenché empêchera alors l'armement de la section. Ce statut est indiqué par voie optique via la touche fonctionnelle clignotant en rouge. Le détecteur empêchant l'armement sera signalé sur le menu de l'écran LCD.

*) **ATTENTION** : les options a) et b) ne sont pas prises en charge par la norme EN 50131, niveau 2 (profil du système de la centrale sélectionné).

Si un détecteur avec la réaction « Alarme de zone instantanée » est déclenché pendant la temporisation de sortie ou si un détecteur avec la réaction « Alarme de zone temporisée » reste déclenché après l'expiration du délai de sortie, la centrale sera alors à nouveau désarmée. L'échec de l'armement est indiqué par un voyant du système clignotant en jaune, signalé à la télésurveillance et indiqué par une sirène externe (conformément au niveau 2 de sécurité).

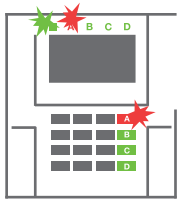


Si la centrale est configurée pour être armée sans autorisation, il n'est alors pas nécessaire de s'autoriser soi-même. Il faut simplement appuyer sur la touche fonctionnelle d'une section particulière. Le technicien de service peut également configurer la centrale pour être armée uniquement par autorisation.

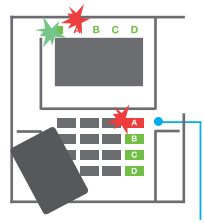
AVERTISSEMENT : l'armement sans autorisation abaisse automatiquement le niveau de sécurité maximal au niveau 1. Prendre en considération tous les risques éventuels liés à l'utilisation de cette fonction.

Indiquer les choix de l'installation au technicien de service ou au responsable du projet afin de programmer le comportement requis pour le système.

2.1.3.2. DÉSARMEMENT DE L'ALARME

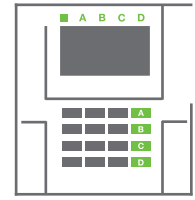


1. **En entrant dans le bâtiment** (déclenchement d'un détecteur avec une réaction « Zone temporisée »), le système commence à signaler la temporisation d'entrée par une tonalité continue, le voyant du système et la touche fonctionnelle, les deux clignotant en rouge,



de la section dans laquelle la temporisation d'entrée a été déclenchée.

2. **S'autoriser en utilisant le clavier -** le voyant du système commencera à clignoter en vert.



3. **Enclencher les touches** fonctionnelles des sections devant être désarmées.

4. **La commande est exécutée.** Les touches fonctionnelles et le voyant du système passent au vert pour signaler le désarmement des sections.

Remarque : si le paramètre « Désarmer la section par autorisation uniquement durant la temporisation d'entrée » est activé, la simple autorisation désarmera la section où la temporisation d'entrée a été déclenchée. Cette option doit être utilisée avec prudence lors de l'utilisation de plusieurs sections.

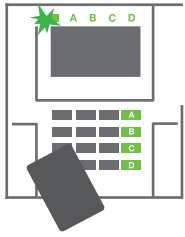
Indiquer les choix de l'installation au technicien de service afin de programmer le comportement requis pour le système.

2.1.3.3. ARMEMENT PARTIEL DE L'ALARME

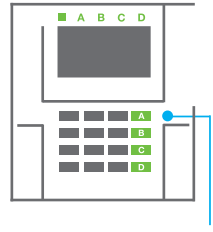
ATTENTION : il s'agit d'une fonction supplémentaire du système d'alarme.

Le système peut également être configuré pour être partiellement armé, ce qui permet la surveillance partielle par certains détecteurs dans une section.

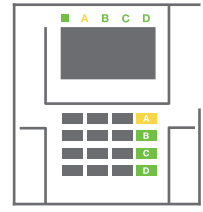
Exemple : la nuit, il est possible d'armer uniquement les détecteurs de portes et de fenêtres, les détecteurs de mouvement sélectionnés ne déclenchant pas l'alarme lorsque quelqu'un se déplace dans la section.



1. **S'identifier à l'aide du clavier** (saisir un code ou placer un badge ou une carte RFID sur le lecteur). La touche du voyant du système commencera à clignoter en vert.



2. **Enclencher la touche fonctionnelle** de la section choisie.



3. **La commande est exécutée** et la touche fonctionnelle passe au jaune en continu pour signaler l'armement partiel de la section.

Pour armer la totalité des locaux dans lesquels l'armement partiel est activé, la touche d'armement de la centrale doit être maintenue 2 secondes ou enclenchée deux fois. Après le premier enclenchement de la touche, elle s'allume en jaune, après le second, elle passe en continu au rouge.

Si le système est déjà partiellement armé - la touche fonctionnelle est allumée en jaune en continu - l'ensemble du système peut être totalement armé par autorisation et en enclenchant plus longtemps la touche jaune. Une fois que la touche est enclenchée, le système sera entièrement armé et la touche passera au rouge.

L'armement partiel peut être configuré de façon à ce que l'autorisation ne soit pas nécessaire.

Pour désarmer la centrale en cas d'armement partiel, appuyer sur la touche jaune. La centrale sera désarmée et la touche passera au vert

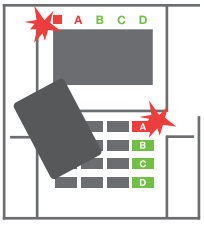
2.1.3.4. COMMANDE D'ACCÈS SOUS LA CONTRAINTE

Cela désarme la centrale d'une manière particulière. Le système est apparemment désarmé, mais il déclenche une alarme de détresse silencieuse, qui est signalée aux utilisateurs sélectionnés (y compris la télésurveillance).

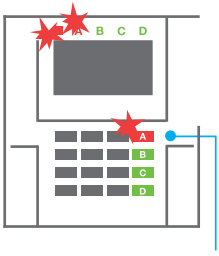
Le désarmement sous la contrainte est réalisé en ajoutant 1 au dernier numéro du code valide. Contacter le technicien de service pour utiliser cette fonctionnalité.

Exemple : Code valide: 9999 Code de désarmement sous la contrainte : 9990

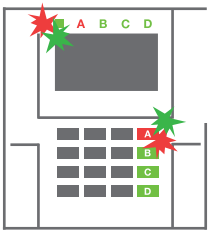
2.1.3.5. ARRÊT D'UNE ALARME DÉCLENCHÉE



1. S'identifier à l'aide du clavier (saisir un code, placer un badge sur le lecteur).



2. Enclencher la touche fonctionnelle de la section dans laquelle l'alarme a été déclenchée.



3. Le désarmement se termine et les sirènes sont réduites au silence. Les touches fonctionnelles, clignotant rapidement et alternativement (vert / rouge), et les indicateurs d'état signalent la mémoire d'alarme.

Une alarme déclenchée en cours est signalée par l'indicateur d'état et la touche fonctionnelle clignote rapidement en rouge. Il faut s'identifier à l'aide du clavier afin de mettre fin à l'alarme. La section reste armée, la touche fonctionnelle rouge clignotant rapidement signale la mémoire d'alarme. Le voyant continuera à clignoter même après le désarmement du système.

ATTENTION : si l'indication de mémoire d'alarme a été activée lors d'une absence, être toujours très prudent en entrant dans le bâtiment, rechercher l'origine de l'alarme dans l'historique événementiel et faire preuve d'une grande prudence en vérifiant les locaux ou attendre jusqu'à ce qu'un agent de sécurité arrive (à condition que le système soit connecté à une télésurveillance).

L'indicateur mémoriel d'alarme reste allumé jusqu'à ce que le système soit armé une fois de plus. Il peut être annulé à défaut à partir du menu du clavier. Menu principal - Annuler l'indication d'avertissement. L'indication d'une alarme de sabotage déclenchée ne peut être annulée que par un technicien de service et un administrateur.

Remarque : en cas d'utilisation du profil « par défaut » du système, il est possible de sélectionner une action particulière en appuyant sur une touche fonctionnelle puis de confirmer par autorisation à l'aide du clavier.

L'arrêt d'une alarme à l'aide d'une télécommande désarmera également la section correspondante.

2.1.3.6. UTILISATION DU SYSTÈME AVEC UNE TÉLÉCOMMANDE

Les télécommandes doivent être attribuées dans le système par l'installateur. La télécommande peut être liée à des utilisateurs spécifiques, ce qui évite les notifications SMS à l'utilisateur interagissant avec le système (si les paramètres de notification sont définis en conséquence). Les télécommandes contrôlent et signalent le statut de la batterie et sont équipées d'un dispositif de signalisation optique et acoustique.

COMMANDE BIDIRECTIONNELLE

Les touches fonctionnelles sont différenciées par des icônes de verrouillage. L'icône du cadenas fermé arme les sections programmées ; l'icône du cadenas ouvert les désarme. La bonne exécution de la commande est confirmée par un voyant LED ; désarmement - vert, armement - rouge. Une défaillance de communication (hors de portée de la centrale) est signalée par un voyant LED jaune clignotant une fois. Les touches avec des symboles de cercles pleins et vides peuvent commander une autre section. Les touches de la télécommande peuvent également être configurées pour commander les sorties PG dans différents modes : la première touche active / la seconde désactive, chaque touche pouvant avoir une fonction individuelle lorsque les fonctions d'impulsion ou de modification sont utilisées. Pour de plus amples fonctionnalités, il est possible d'appuyer sur deux touches en même temps. Une télécommande à 4 touches peut ainsi avoir jusqu'à 6 fonctions individuelles ou un état de sortie PG (par ex. allumer et éteindre les lumières), ou à défaut deux sorties PG (par ex. le verrouillage du garage et de la porte).

Si le système est configuré sur Armer après confirmation, le détecteur signalera l'échec de l'armement avec le voyant LED vert si un périphérique est déclenché. Il est nécessaire de confirmer l'armement en appuyant de nouveau sur la touche de verrouillage. L'armement de la section sera confirmé par un voyant LED rouge.

Les touches de la télécommande peuvent être bloquées pour prévenir un enclenchement accidentel. Une commande sera envoyée quand une touche est enclenchée à plusieurs reprises.

Une batterie faible est signalée par voie acoustique (avec 3 bips) et optique par clignotement d'un voyant LED jaune après enclenchement de la touche.

Pour de plus amples informations, consulter la configuration de la télécommande avec le technicien de service.

TÉLÉCOMMANDES UNIDIRECTIONNELLES

Les télécommandes unidirectionnelles envoient un signal à chaque enclenchement de touche, sans recevoir de rétroaction de la centrale. L'envoi d'un signal n'est confirmé que par un court clignotement de la LED rouge et à défaut, avec un bip.

2.2. FONCTIONNEMENT À DISTANCE

Le service MyJABLOTRON offre le meilleur confort d'utilisation et de gestion à distance du système. L'interface Internet MyJABLOTRON est un service unique qui permet d'accéder en ligne aux périphériques JABLOTRON. Cela permet aux utilisateurs finaux de surveiller et de commander le système. Une application mobile et une application Internet permettent également d'assurer ce service. Le service MyJABLOTRON permet aux utilisateurs de réaliser les points suivants :

:: Visualiser l´état actuel du système.
:: Armer/ désarmer entièrement ou partiellement le système.
:: Commander des sorties programmables.
:: Afficher l'historique évènementiel.
:: Envoyer des notifications aux utilisateurs choisis par SMS, e-mail ou notification PUSH.
:: Réaliser des captures d'images à partir de détecteurs de vérification photographique et naviguer par leur intermédiaire dans l'onglet Galerie photos ou directement dans les événements récents.
:: Surveiller la température ou la consommation d'énergie réelle, y compris la visualisation de l'historique dans un graphique.
:: Ainsi que d'autres fonctionnalités utiles.

En fonction du pays ou de la région, un compte Internet est créé dans MyJABLOTRON par un partenaire agréé JABLOTRON. L'identifiant est l'adresse e-mail de l'utilisateur. Le mot de passe pour la première connexion sera envoyé à cette adresse. Le mot de passe peut être modifié à tout moment dans les paramètres de l'utilisateur.

2.2.1. UTILISATION DU SYSTÈME À L'AIDE DE L'APPLICATION MOBILE MyJABLOTRON

Une fois qu'un compte utilisateur est créé, l'utilisateur peut surveiller et commander le système à distance via l'application MyJABLOTRON pour les mobiles tournant sous Android et iOS.

2.2.2. UTILISATION DU SYSTÈME À L'AIDE DE L'INTERFACE INTERNET MyJABLOTRON

Le système JABLOTRON 100+ peut facilement et commodément être commandé par l'ordinateur via Internet et l'interface dédiée MyJABLOTRON, accessible sur www.myjablotron.com.

2.2.3. UTILISATION DU SYSTÈME À L'AIDE DU MENU VOCAL

Le système peut être commandé à partir d'un téléphone à travers un menu vocal, qui guide l'utilisateur via une série d'options dans la langue sélectionnée par défaut. Pour accéder au menu vocal, il suffi t de composer le numéro de téléphone du système d'alarme.

L'accès au menu vocal peut être activé pour tout appel entrant sans restriction ou pour n'accepter que les numéros de téléphone autorisés sauvegardés dans la centrale. Selon la configuration, l'autorisation par saisie d'un code valide sur un clavier de téléphone peut être nécessaire. Une fois l'utilisateur entré dans le menu, le système informera quant au statut réel de toutes les sections attribuées à l'utilisateur. L'appelant peut alors commander ces sections, individuellement ou collectivement, en utilisant son clavier téléphonique et les options du menu disponibles.

La valeur par défaut du système consiste à répondre aux appels entrants après trois sonneries (environ 15 secondes).

2.2.4. UTILISATION DU SYSTÈME PAR LES COMMANDES SMS

Les commandes SMS peuvent contrôler les sections individuelles et les sorties programmables de la même façon que les touches du segment du clavier. Le texte du message permettant de commander le système est le suivant : CODE_COMMANDE. Les commandes réelles sont prédéfinies (ARMER / DÉSARMER) avec un paramètre numérique supplémentaire qui identifie une section spécifique. Un SMS peut commander plusieurs sections en même temps. Dans ce cas, l'ajout de numéros dans la commande arme des sections.

Exemple d'une commande SMS utilisée pour armer les sections 2 et 4.
CODE_ARMER_2_4

Les commandes de contrôle des sorties programmables peuvent être programmées par l'installateur du système. Il est par exemple possible de choisir VOLETS FERMÉS pour la commande afin de fermer les volets des fenêtres. Il est également possible de configurer le système de sorte à ne pas exiger de code avant une commande. Dans ce cas, la commande est simplement automatiquement identifiée lorsque le système reconnaît le numéro de téléphone de l'utilisateur à partir duquel le SMS a été envoyé. La configuration se fait par un technicien de service.

2.2.5. UTILISATION DU SYSTÈME À DISTANCE À L'AIDE D'UN ORDINATEUR (J-LINK)

Le système JABLOTRON 100+ peut être utilisé à distance à l'aide d'un ordinateur équipé du logiciel J-Link installé. Le programme doit être téléchargé à partir de la section « Téléchargements » du site internet **www.myjablotron.com**.

2.2.6. CONTRÔLE DES SORTIES PROGRAMMABLES (PG)

2.2.6.1. SEGMENT DU CLAVIER

Une sortie PG est activée en enclenchant la touche sur le côté droit du segment et est désactivée en enclenchant la touche sur le côté gauche. Si la sortie est configurée comme une sortie d'impulsion, elle est désactivée en fonction d'un temps prédéfini. La commande PG peut éventuellement être stockée dans la mémoire évènementielle de la centrale. La configuration est réalisée par un technicien de service.

L'autorisation est éventuellement requise en fonction de la configuration du système.

2.2.6.2. AUTORISATION SUR LE CLAVIER DE L'UTILISATEUR

Il est possible d'activer une sortie PG par simple autorisation de l'utilisateur (saisie d'un code ou utilisation d'un badge RIFD). La sortie PG doit être configurée de sorte à être activée à partir d'un clavier désigné.

2.2.6.3. À PARTIR DU MENU DU CLAVIER DOTÉ D'UN ÉCRAN LCD

Après autorisation de l'utilisateur, les sorties programmables peuvent être commandées à partir du menu du clavier doté d'un écran LCD. L'utilisateur a accès aux sorties programmables en fonction de ses autorisations.

Commande à partir du menu du clavier :

:: Autorisation par un code valide ou une puce RFID
:: Entrer dans le menu en appuyant sur ENTER
:: Commande PG → ENTER
:: Sélectionner le groupe PG requis à l'aide des flèches (1-32), (33-64), (65-96), (97-128) → ENTER.
:: Sélectionner la PG souhaitée à l'aide des flèches ENTER.
:: Appuyer plusieurs fois sur ENTER pour modifier le statut PG (la PG active est indiquée par un numéro PG dans un rectangle de couleur noire .
:: Appuyer sur ESC pour quitter le menu.

2.2.6.4. COMMANDE À DISTANCE

Il faut enclencher une touche attribuée d'une télécommande. Les télécommandes bidirectionnelles confirment l'activation des sorties PG par l'entremise d'un voyant indicateur LED.

2.2.6.5. APPLICATION MOBILE MyJABLOTRON

En enclenchant Marche / Arrêt dans l'onglet Automatisation (PG).

2.2.6.6. INTERFACE INTERNET MyJABLOTRON

En cliquant sur Marche / Arrêt dans l'onglet Automatisation (PG).

2.2.6.7. PAR NUMÉROTATION

Chaque numéro de téléphone mémorisé dans le système (un utilisateur peut avoir un numéro de téléphone) peut commander par simple numérotation (donc sans passer d'appel) une PG. Le système de numérotation consiste à composer le numéro de téléphone de la carte SIM utilisée dans le système de sécurité et à raccrocher avant que l'appel ne soit pris par le système. Par défaut, le système répondra à l'appel après la troisième sonnerie (environ 15 secondes).

2.2.6.8. MESSAGE SMS

L'envoi d'un SMS peut activer / désactiver une PG particulière. L'autorisation est éventuellement requise en fonction de la configuration du système.
Exemple : CODE_TEXTE CONFIGURÉ

3. BLOCAGE / NEUTRALISATION DU SYSTÈME

3.1. BLOCAGE DES UTILISATEURS

N'importe quel utilisateur peut être temporairement bloque (par ex. quand un utilisateur perd ses carte / badge ou son code d'accès est decouvert). Lorsque l'accès d'un utilisateur est bloque, son code d'identification ou ses carte / badge ne seront plus acceptes par le système. Les utilisateurs ne recevront plus aucune alerte textuelle ou de message vocal sur leur téléphone.

Seul l'administrateur du systeme ou le technicien de service peut bloquer un utilisateur. Une methode visant a retirer les droits d'accès consiste a selectionner « Oui » sur le clavier LCD dans Parametres / Utilisateurs / Utilisateur / Derivation. Une autre option consiste a bloquer localement ou a distance un utilisateur par l'intermediaire du programme J-Link en cliquant sur l'utilisateur dans la colonne Parametres / Utilisateurs / Blocage de l'utilisateur.

Un utilisateur bloque (neutralise) sera identifie par un cercle rouge jusqu'a ce que le blocage soit annule.

3.2. BLOCAGE DES DÉTECTEURS

Un detecteur peut etre temporairement desactive d'une maniere similaire a celle utilisee pour bloquer un utilisateur. Un detecteur est bloque lorsque son activation est temporairement non desiree (par exemple un detecteur de mouvement dans une piece ou se trouve un animal domestique ou la desactivation acoustique d'une sirene). Le systeme effectue toujours le diagnostic des contacts de sabotage et envoie des evenements de service des que la fonction d'alarme est desactivee.

Seul l'administrateur du systeme ou un technicien de service peuvent bloquer un detecteur. Il faut pour cela choisir Oui sur le clavier LCD dans Parametres / Peripheriques / Derivation. Une autre option consiste a utiliser le logiciel J-Link en cliquant sur le detecteur dans la colonne Parametres / Diagnostics / Desactivation. Un detecteur bloque est identifie par un cercle jaune jusqu'a son deblocage par la meme procedure. Un peripherique peut egalement etre bloque a partir de l'application mobile MyJABLOTRON.

3.3. DÉSACTIVATION DES MINUTERIES

Pour désactiver temporairement les événements programmés et automatisés dans le système, la minuterie peut être désactivée. La désactivation d'un événement programmé (par ex. le désarmement du système pour la ronde de nuit à un moment prédéterminé) empêchera l'exécution d'un tel évènement (par ex. en congé).

Une minuterie peut être désactivée localement ou à distance par l'intermédiaire du programme J-Link en cliquant sur la section dans la colonne Paramètres / Calendrier / Blocage. Une minuterie désactivée est identifiée par un cercle rouge jusqu'à ce qu'elle soit réactivée par la même procédure.

4. PERSONNALISATION DU SYSTÈME

4.1. MODIFICATION DU CODE D'ACCÈS DE L'UTILISATEUR

Si le système est configuré sans code préfixé, seul l'administrateur système et le technicien de service peuvent modifier les codes de sécurité. L'administrateur système peut apporter des modifications à la fois à partir du menu du clavier LCD du logiciel J-Link et de l'application mobile MyJABLOTRON. Le code peut être modifié après l'autorisation en sélectionnant Paramètres / Utilisateurs / Utilisateur / Code. Pour saisir un nouveau code, il faut passer en mode d'édition (le code commencera à clignoter) en appuyant sur Enter, saisir le nouveau code et confirmer en appuyant de nouveau sur Enter. Les modifications réalisées doivent être confirmées en choisissant Sauvegarder lorsque le système affiche « Sauvegarder les paramètres ? ».

Si le système est configuré avec des codes préfixés, les utilisateurs individuels peuvent modifier leur code à partir du menu LCD du clavier.

4.2. MODIFICATION, SUPPRESSION OU AJOUT DE CARTE / BADGE RFID

Si le système est configuré sans code préfixé, seul l'administrateur système et le technicien de service peuvent modifier les codes de sécurité. L'administrateur système peut apporter des modifications à la fois à partir du menu du clavier LCD du logiciel J-Link et de l'application mobile MyJABLOTRON. Le code peut être modifié après l'autorisation en sélectionnant Paramètres / Utilisateurs / Utilisateur / Code. Pour saisir un nouveau code, il faut passer en mode d'édition (le code commencera à clignoter) en appuyant sur Enter, saisir le nouveau code et confirmer en appuyant de nouveau sur Enter. Les modifications réalisées doivent être confirmées en choisissant Sauvegarder lorsque le système Affiche « Sauvegarder les paramètres ? ».

Si le système est configuré avec des codes préfixés, les utilisateurs individuels peuvent modifier leur code à partir du menu LCD du clavier.

4.3. MODIFICATION D'UN NOM D'UTILISATEUR OU D'UN NUMÉRO DE TÉLÉPHONE

Si le système est configuré avec des codes préfixés, les utilisateurs peuvent ajouter, modifier ou supprimer leur numéro de téléphone ou modifier leur nom à partir du menu LCD du clavier. Cela peut être réalisé après l'autorisation en sélectionnant Paramètres / Utilisateurs / Utilisateur / Téléphone. L'utilisateur doit être en mode d'édition pour réaliser des modifications. Il faut pour cela appuyer sur Enter. Les modifications réalisées doivent être confirmées en appuyant à nouveau sur Enter. Pour supprimer un numéro de téléphone, saisir « 0 » dans le champ du numéro de téléphone. Les modifications réalisées doivent être confirmées par le choix Sauvegarder lorsque le système Affiche « Sauvegarder les paramètres ? ».

L'administrateur système et le technicien de service peuvent ajouter, modifier ou supprimer le numéro de téléphone d'un utilisateur ou modifier le nom d'un utilisateur à partir du menu du clavier doté d'un écran LCD et de J-Link.

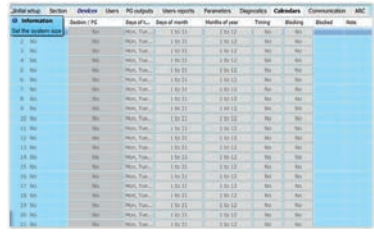
4.4. AJOUT / SUPPRESSION D'UN UTILISATEUR

Seul l'administrateur du système ou un technicien de service peuvent ajouter de nouveaux utilisateurs dans le système (ou les supprimer). Les nouveaux utilisateurs ne peuvent être ajoutés dans le système (ou supprimés de celui-ci) que dans le programme J-Link, ou le programme F-Link pour un technicien.

Lors de la création d'un nouvel utilisateur, il est nécessaire de lui attribuer des autorisations d'accès (droits) aux sections que l'utilisateur peut exploiter, aux sorties programmables qu'il peut commander et le type d'autorisation qui sera requis.

4.5. CONFIGURATION DU CALENDRIER ÉVÈNEMENTIEL

Il est possible de configurer jusqu'à 10 événements calendaires (désarmement / armement / armement partiel, commande ou blocage des sorties PG). Les événements calendaires peuvent être configurés par l'intermédiaire du logiciel J-Link dans l'onglet Calendrier.



Pour chaque événement de calendrier, l'action, la section ou la sortie PG et l'heure de l'événement peuvent être définies. Le jour peut être défini par un jour de la semaine, du mois ou de l'année. Pour le jour sélectionné, il est possible de définir jusqu'à 4 horaires pour une action ou une répétition à intervalles réguliers.

Les événements calendaires peuvent donc être personnalisés non seulement pour la commande des sections, mais également pour le contrôle à l'aide des sorties PG des diverses technologies des locaux.

5. HISTORIQUE ÉVÉNEMENTIEL

Le système de sécurité enregistre l'ensemble des opérations et des événements réalisés (armement,

désarmement, alarmes, défaillances, messages envoyés aux utilisateurs et aux centres de télé-surveillance) sur la carte SD de la centrale du système. Chaque entrée comprend la date, l'heure (début et fin) et la source (cause / origine) de l'événement.

Les différentes façons de parcourir l'historique des événements du système:

5.1. UTILISATION DU CLAVIER LCD

L'accès à l'historique évènementiel à l'aide du clavier nécessite l'autorisation de l'utilisateur. Une fois l'autorisation réalisée, les options disponibles (en fonction des restrictions de l'utilisateur) sont affichées en choisissant Mémoire évènementielle. Les enregistrements peuvent être visualisés à l'aide des flèches.

5.2. UTILISATION DE J-LINK ET D'UN ORDINATEUR

La mémoire du système peut être consultée en utilisant le programme J-Link. Les événements peuvent être téléchargés par lots de petite taille (environ 1 200 événements) ou grande taille (environ 4 000 événements) à partir de la centrale. Les événements peuvent être filtrés en détail, codés en couleur pour faciliter l'orientation, ou sauvegardés dans un fi chier dans un ordinateur.

5.3. CONNEXION À MyJABLOTRON (INTERNET / MOBILE)

Tous les événements du système peuvent être visualisés après la connexion à l'interface Internet / mobile MyJABLOTRON. Le compte Affiche l'historique dans l'envergure qui correspond aux autorisations de l'utilisateur.

6. CARACTÉRISTIQUES TECHNIQUES

<table>
<tr><th>PARAMÈTRES</th><th colspan="2">JA-103K</th><th colspan="2">JA-107K</th></tr>
<tr><td>Alimentation de la centrale</td><td colspan="2">~ 110-230 V/50-60 Hz,
max. 0,28 A avec fusible F1,6 A/250 V
Classe de protection II</td><td colspan="2">~ 110-230 V / 50-60 Hz,
,max. 0,85 A avec fusible F1,6 A/250 V
Classe de protection II</td></tr>
<tr><td>Batterie de secours</td><td colspan="2">12 V ; 2,6 Ah (Plomb Gel)</td><td colspan="2">12 V ; 7 à 18 Ah (Plomb Gel)</td></tr>
<tr><td>Durée maximale de recharge de la batterie</td><td colspan="4">72 h</td></tr>
<tr><td>Tension BUS (rouge - noir)</td><td colspan="4">12,0 à 13,8V</td></tr>
<tr><td>Consommation de courant continu max. à partir de la centrale :</td><td colspan="2">1000 mA</td><td colspan="2">2000 mA en continu
(3000 mA pendant 60 minutes)
(max 2000 mA pour un BUS)</td></tr>
<tr><td rowspan="2">Consommation de courant continu max. pour la sauvegarde 12 heures</td><td rowspan="2">Sans Transmetteur GSM</td><td rowspan="2">LAN désactivé
115 mA
LAN activé
88 mA</td><td colspan="2">Valable pour une batterie de secours 18 Ah</td></tr>
<tr><td>Sans Transmetteur GSM</td><td>LAN désactivé
1135 mA
LAN activé
1107 mA</td></tr>
<tr><td>Avec Transmetteur GSM</td><td>LAN désactivé
80 mA
LAN activé
53 mA</td><td>Avec Transmetteur GSM</td><td>LAN désactivé
1100 mA
LAN activé
1072 mA</td></tr>
<tr><td>Nombre maximal de périphériques</td><td colspan="2">50</td><td colspan="2">230</td></tr>
</table>

PARAMÈTRES	JA-103K	JA-107K
Transmetteur LAN	INTERFACE ETHERNET, 10/100BASE-T	
Dimensions	268 x 225 x 83 mm	357 x 297 x 105 mm
Poids avec / sans accumulateur	1844 g/970 g	7027 g/1809 g
Réaction à la saisie d'un code invalide	Alarme après 10 saisies erronées du code	
Mémoire évènementielle	Environ 7 millions d'évènements antérieurs, y compris la date et l'heure	
Source d'alimentation :	Type A (Conformément à la norme EN 50131-6)	
Transmetteur GSM (2G)	850 / 900 / 1800 / 1900 MHz	
Classification	Niveau de sécurité 2 / Classe environnementale II (conformément à EN 50131-1)	
Environnement de service	Intérieur, général	
Plage des températures de service	-10 °C to +40 °C	
Humidité opérationnelle moyenne	75 % RH, sans condensation	
Conforme à	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	
Fréquence opérationnelle (avec le module JA 11xR)	868,1 MHz, protocole JABLOTRON	
Émissions radio	ETSI EN 300 220-1,-2 (module R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 éd. 2+A1, EN 55032 éd. 2, ETSI EN 301 489-7	
Conformité de la sécurité	EN 62368-1+A11	
Conditions d'exploitation	ERC REC 70-03	
Organisme de certification	Trezor Test s.r.o. (no. 3025)	
Identification de l'appelant (CLIP)	ETSI EN 300 089	

JABLOTRON ALARMS a.s. déclare par la présente que les centrales JA-103K et JA-107K sont conformes à la législation d'harmonisation correspondante de l'Union européenne : directives n° : 2014/53/UE, 2014/35/UE, 2014/30/UE, 2011/65/UE dans le cadre d'une utilisation conforme. L'original de la déclaration de conformité se trouve sur www.jablotron.com – Section Téléchargement.

Remarque : le produit, même s'il ne comprend aucune matière nocive, devrait être rapporté au vendeur ou directement au fabricant après utilisation.

INDICE

MANUTENZIONE PERIODICA

:: È necessario assicurare controlli di manutenzione regolari e puntuali al fi ne di garantire l'affidabilità del funzionamento del sistema. La maggior parte delle operazioni di manutenzione viene eseguita dalla ditta di manutenzione almeno una volta all'anno durante le ispezioni di manutenzione periodica.

:: La manutenzione da parte dell'utente risiede soprattutto nel tener puliti i singoli dispositivi. L'AMMINISTRATORE del sistema può portare il sistema in modalità MANUTENZIONE al fi ne di poter aprire i rilevatori (cambio batterie) o rimuoverli dall'installazione. Consultare la società di installazione per quanto concerne l'eventuale richiesta di impostazione della modalità MANUTENZIONE. Se il sistema è configurato secondo il profilo sistema "EN 50131-1, grado 2", la modalità MANUTENZIONE non è disponibile.

:: Il sistema può essere portato in modalità manutenzione attraverso il software J-Link oppure tramite il menu della tastiera con display LCD. Dopo l'autorizzazione, è possibile selezionare la "Modalità manutenzione" con una selezione delle sezioni dove la manutenzione è richiesta. In modalità manutenzione non viene innescato alcun allarme nelle sezioni selezionate, compresa apertura o rimozione dei rilevatori dall'installazione.

:: La modalità manutenzione è indicata dal lampeggio verde del pulsante di attivazione (2 lampeggi ogni 2 secondi) e dallo spegnimento dei due pulsanti segmento della data sezione.

:: Nel maneggiare il dispositivo fare attenzione ad evitare il danneggiamento delle parti in plastica e dei meccanismi dei rilevatori.

:: Il coperchio è generalmente protetto da un fermo che va leggermente conficcato nel corpo del rilevatore con l'ausilio di un piccolo strumento (per es. cacciavite); quindi il coperchio può essere tranquillamente estratto. In alcuni casi il fermo è fissato con una piccola vite di fissaggio (che va dunque dapprima svitata).

:: Durante la sostituzione delle batterie nel rilevatore, sostituire sempre tutte le batterie del dato rilevatore (utilizzare batterie dello stesso tipo e dello stesso produttore).

:: Per alcuni dispositivi possono essere richiesti dei test (per esempio, rilevatori d'incendio). Per ulteriori informazioni si prega di contattare il tecnico dell'assistenza.

1. INTRODUZIONE

Il sistema JABLOTRON 100+ è progettato per un uso fi no a 600 utenti e può essere diviso in 15 sezioni singole. È possibile connettere fi no a 230 dispositivi e il sistema offre un massimo di 128 uscite programmabili multifunzionali (per esempio, automazione domestica).

2. UTILIZZO DEL SISTEMA JABLOTRON 100+

Il sistema di sicurezza può essere comandato in vari modi diversi. Per disinstallare l'allarme, viene sempre richiesta un'autorizzazione sotto forma di identificazione utente. Il sistema rileva l'identità degli utenti e consente loro di gestire quelle parti del sistema che sono state loro affidate.
È possibile scegliere tra diverse modalità di inserimento con o senza autorizzazione. Quando si utilizza l'autorizzazione standard, non è necessario autorizzare se stessi, dato che è possibile inserire il sistema premendo semplicemente il pulsante segmento destro sulla tastiera. Il nome utente, la data e l'orario sono registrati e salvati nella memoria del sistema ogni volta che si effettua l'accesso al sistema. Le informazioni sono a disposizione a tempo indeterminato. Ciascun utente ha anche la possibilità di cancellare gli allarmi innescati (tacitamento sirena) mediante semplice autorizzazione in qualsiasi parte del sistema (in base ai rispettivi diritti d'accesso). Tuttavia, in questa maniera non si va automaticamente a disinserire il sistema (a meno che non sia cambiata l'impostazione predefinita del sistema).

Nota: A seconda della configurazione dell'installazione e delle impostazioni di sistema, alcune delle opzioni descritte oltre potrebbero non essere disponibili. Consultare il proprio tecnico di assistenza per la configurazione dell'installazione.

Utenti e diritti d'accesso

AUTORIZZAZIONE CON CODICE	DESCRIZIONE DEL TIPO
Codice ARC	Questo codice ha il più alto livello di autorizzazione per configurare il comportamento del sistema; consente, in maniera esclusiva, di eseguire lo sblocco del sistema dopo l'innesco di un allarme. Permette di accedere alla modalità «Service» e a tutte le tabelle con le opzioni, compresa la comunicazione ARC, con la possibilità di negare l'accesso ad un tecnico di assistenza (codice «Service»). Se non viene selezionato il parametro «Assistenza limitata-Amministratore/diritto ARC», il codice ARC è in grado di comandare tutte le sezioni e uscite PG impiegate nel sistema. Questo codice consente di aggiungere più amministratori ed altri utenti con livello più basso di autorizzazione, assegnando loro codici, etichette RFID e schede. Consente anche di cancellare allarmi e memoria allarme tamper. Il numero di codici ARC è limitato soltanto dalla capacità residua della centrale e non vi sono codici che siano predefiniti di fabbrica.
Codice «Service»	Questo codice permette di accedere alla modalità «Service» e configurare il comportamento del sistema. Consente di accedere a tutte le tabelle con le opzioni, compresa comunicazione ARC, a meno che l'accesso non sia stato limitato da un tecnico ARC. Se non viene selezionato il parametro «Assistenza limitata-Amministratore/ diritto ARC», il codice «Service» è in grado di comandare tutte le sezioni e uscite PG impiegate nel sistema. Può creare utenti con permesso ARC, altri tecnici di assistenza, amministratori ed altri utenti con livello più basso di autorizzazione, assegnando loro codici di accesso, etichette RFID e schede. Consente anche di cancellare allarmi e memoria allarme tamper. Il numero di codici «Service» è limitato soltanto dalla capacità residua della centrale. Il codice predefinito di fabbrica è 1010. L'utente «Service» è sempre in posizione 0 nella centrale e non può essere cancellato.
Codice amministratore (Principale)	Questo codice vanta sempre un accesso totale a tutte le sezioni ed è autorizzato a comandare tutte le uscite PG. L'amministratore può creare altri amministratori ed altri utenti con un livello più basso di autorizzazione, assegnando loro la possibilità di accedere alle sezioni e alle uscite PG, codici di accesso, chip RFID e schede. Questo codice ha anche la possibilità di cancellare la memoria allarmi. Vi può essere soltanto un codice amministratore principale e non può essere cancellato. Se viene selezionato il parametro «Assistenza limitata-Amministratore/ diritto ARC», il codice amministratore deve essere autorizzato per la conferma dell'accesso per l'ARC e per i tecnici dell'assistenza. Il codice predefinito di fabbrica è 1234. L'utente Amministratore principale è sempre in posizione 1 e non può essere cancellato.

AUTORIZZAZIONE CON CODICE	DESCRIZIONE DEL TIPO
Codice amministratore (Altro)	Questo codice dà accesso alle sezioni selezionate dall'amministratore principale; qui gli altri amministratori possono aggiungere nuovi utenti con lo stesso livello o con un livello più basso di autorizzazione per il comando delle sezioni e delle uscite PG, assegnando loro codici di accesso, etichette RFID e schede. Questo codice offre anche la possibilità di cancellare la memoria allarmi nelle sezioni assegnate. Se viene selezionato il parametro «Assistenza limitata--Amministratore/diritto ARC», il codice amministratore deve essere autorizzato per la conferma dell'accesso per l'ARC e per i tecnici dell'assistenza. Il numero di codici di tipo Amministratore (Altro) è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Codice utente	Questo codice consente l'accesso secondo i diritti di comando sezioni e uscite PG secondo quanto deciso dall'amministratore. Gli utenti possono aggiungere/eliminare le proprie etichette RFID e schede d'accesso e modificare i propri numeri di telefono. Gli utenti possono modificare i propri codici, a condizione che il sistema impieghi codici con prefissi. Hanno anche la possibilità di cancellare la memoria allarmi nelle sezioni assegnate. Gli utenti selezionati possono avere un accesso alle sezioni limitato da un programma temporale. Il numero di codici di tipo Utente è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Impostare codice	Questo codice è utilizzabile solo per inserire una determinata sezione e per il controllo delle uscite PG (ON/ OFF) che richiedono un'autorizzazione. Gli utenti con questo livello di autorizzazione non hanno la possibilità di modificare il proprio codice o di cancellare la memoria allarmi. Il numero di codici di tipo «Set» è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Codice solo PG	Questo codice consente agli utenti di comandare le uscite programmabili unicamente con autorizzazione. Ciò vale sia per l'accensione che per lo spegnimento. Gli utenti con questo livello di autorizzazione non hanno la possibilità di modificare il proprio codice o di cancellare la memoria allarmi. Il numero di codici di tipo «Solo PG» è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Codice Panico	Questo codice consente di innescare l'allarme panico. Gli utenti con questo codice non hanno la possibilità di modificare il codice o di cancellare la memoria allarmi. Il numero di codici di tipo «Panico» è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Codice Guard	Si tratta di un codice per agenzie di sicurezza. Questo livello di autorizzazione consente di inserire l'intero sistema. Tuttavia, il codice «Guard» è in grado di disinserire il sistema soltanto nel corso di un allarme o al termine di un allarme, a patto che la memoria allarme sia ancora attiva. Gli utenti con questo codice non hanno la possibilità di modificare il codice o di cancellare la memoria allarmi. Il numero di codici di tipo «Guard» è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.
Codice Sblocco	Questo codice serve a sbloccare il sistema dopo un eventuale blocco del sistema dovuto ad allarme. Gli utenti con questo codice non hanno la possibilità di modificare il codice o di cancellare la memoria allarmi. Il numero di codici «Sblocco» è limitato soltanto dalla capacità residua della centrale. Non vi sono codici di questo tipo che siano predefiniti di fabbrica.

Sicurezza dei codici d'accesso, dispositivi RFID senza contatto e comandi a distanza:

Una centrale consente l'assegnazione a ciascun utente di un codice a 4, 6 o 8 cifre e fi no a due etichette RFID per l'autorizzazione al sistema. L'autorizzazione utente è richiesta nel corso di qualsiasi operazione d'impiego mediante tastiera, menu vocale, computer, web o applicazioni mobili. La lunghezza del codice influisce sul numero di combinazioni possibili e dunque sulla sicurezza del codice stesso.

Il numero delle combinazioni del codice dipende dalla configurazione:

Parametri della centrale	4 CIFRE	6 CIFRE	8 CIFRE
"Codice con prefisso" abilitato	= 10^4 = (10.000)	= 10^6 = (1.000.000)	= 10^8 = (100.000.000)

Parametri della centrale	4 CIFRE	6 CIFRE	8 CIFRE
"Codice con prefisso" e **"Controllo accesso in situazioni critiche"** entrambi disabilitati	= 10^4 – (Numero di utenti – 1)	= 10^6 – (Numero di utenti – 1)	= 10^8 – (Numero di utenti – 1)
"Codice con prefisso" disabilitato; **"Controllo accesso in situazioni critiche"** abilitato	≤ 10^4 – ((Numero di utenti – 1) * 3)	≤ 10^6 – ((Numero di utenti – 1) * 3)	≤ 10^8 – ((Numero di utenti– 1) * 3)
Con utilizzo esclusivamente di **scheda RFID** con un range di 14 caratteri (6 costanti + 8 variabili)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
"Codice con prefisso" e **"Conferma scheda con codice"** entrambi abilitati	= (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)
"Codice con prefisso" disabilitato; **"Conferma scheda con codice"** abilitato	= 10^8 * (10^4 – (Numero di utenti – 1))	= 10^8 * (10^6 – (Numero di utenti – 1))	= 10^8 * (10^8 – (Numero di utenti – 1))

Come migliorare la protezione contro il pericolo che qualcuno indovini il codice giusto:

:: Utilizzare un codice con tante cifre (a 6 o 8 cifre),
:: Tipi più avanzati di autorizzazione (come «Conferma scheda con codice» o «Doppia autorizzazione»).

Modalità d'impiego di JABLOTRON 100+

On-site:

:: Tastiera di sistema
:: Portachiavi di sistema
:: Computer con cavo USB e software J-Link

A distanza::

:: Applicazione smartphone MyJABLOTRON
:: Computer via interfaccia web MyJABLOTRON
:: Telefono con menu vocale
:: Cellulare – via SMS
:: Computer - via internet tramite software J-Link
:: Chiamata da numero di telefono autorizzato (solo per uscite programmabili operative)

Il sistema JABLOTRON 100+ può essere gestito da diversi moduli di accesso che consentono non solo di comandare ma anche di visualizzare gli stati dei singoli segmenti. Il sistema può essere gestito direttamente (inserendo e disinserendo il sistema o altre funzioni di automazione) con l'ausilio dei segmenti a doppio pulsante sulla tastiera. I pulsanti dei segmenti sono chiaramente contrassegnati e colorati (con logica a semaforo). Pertanto ciascuno stato del segmento è indicato in maniera ben distinta. Un segmento può anche essere impiegato per indicare uno stato (per esempio, porta del garage aperta) o per comandare vari dispositivi automatizzati (per esempio, riscaldamento o tapparelle). Il numero massimo di segmenti è pari a 20 per un singolo modulo di accesso. I segmenti possono anche essere impostati per chiamate di emergenza (emergenza medica o allarme panico).

2.1. OPERAZIONI ON-SITE

VERDE FISSO
UNSET | OFF

VERDE LAMPEGGIANTE
RITARDO ENTRATA

ROSSO LAMPEGGIANTE
ALLARME | MEMORIA ALLARME

VERDE FISSO
TUTTO OK

VERDE LAMPEGGIANTE
PANNELLO DI

VERDE LAMPEGGIANTE
2X OGNI 2 S
MANUTENZIONE

GIALLO FISSO
GUASTO

GIALLO LAMPEGGIANTE
IMPOSTAZIONE NON A BUON FINE

ROSSO FISSO
SET | ON

ROSSO LAMPEGGIANTE
ALLARME |
MEMORIA ALLARME

GIALLO FISSO
PARZIALMENTE
INSERITO

LETTORE SCHEDA |
TASTIERA

Tipi di moduli d'accesso e rispettive combinazioni:

Lettore scheda RFID

consente la gestione del sistema mediante segmenti e autorizzazione senza contatto (scheda/etichetta RFID).

Tastiera con lettore scheda

l'utente ha la possibilità di gestire il sistema mediante segmenti e autorizzazioni, ricorrendo all'inserimento di un codice o con metodo senza contatto (scheda/etichetta RFID), oppure mediante combinazione di entrambe queste opzioni, per un livello maggiore di sicurezza.

Tastiera con display LCD e lettore schede

l'utente è in grado di gestire il sistema mediante segmenti e autorizzazione, utilizzando un codice, una modalità senza contatto (scheda/etichetta RFID), entrambi i suddetti elementi per maggior sicurezza, oppure autorizzando e sfruttando le opzioni disponibili sul display LCD della tastiera.

Quando si disinserisce l'allarme utilizzando i pulsanti del rispettivo segmento, viene sempre richiesta l'autorizzazione utente. Quando si imposta l'allarme e durante la gestione dei processi automatizzati mediante i pulsanti dei segmenti, l'autorizzazione utente è invece facoltativa per ciascun singolo segmento.

Gli utenti possono autorizzare se stessi inserendo i propri codici assegnati oppure usando le proprie schede/ cartellini RFID. Ogni utente può avere un unico codice e un massimo di due chip RFID (schede o etichette).

Chip senza contatto consigliati: JABLOTRON 100+, Oasis o chip di terzi compatibili con 125 kHz EM. Se si richiede maggior sicurezza, è possibile impostare il sistema allarme sfruttando l'autorizzazione confermata, mediante chip RFID e codici (opzionale). Se gli utenti desiderano gestire più segmenti contemporaneamente, è necessario che diano l'autorizzazione a se stessi e che premano poi successivamente i segmenti delle sezioni in questione. In questa maniera gli utenti possono, per esempio, configurare le impostazioni relative alla casa e annullare quelle del garage con una singola autorizzazione. Se è abilitato il parametro "Codice con prefisso", il codice autorizzazione tastiera può comprendere un massimo di undici cifre: un prefisso (da una a tre cifre), un asterisco * (per separare il prefisso e il codice principale) e poi un codice di 4, 6 o 8 cifre a seconda della configurazione (per esempio: 123*12345678, o 1*12345678). Tutti gli utente hanno la possibilità di modificare i propri codici dopo il prefisso. Il codice può essere modificato dalla tastiera con il display LCD, mediante software J-Link oppure con l'applicazione MyJABLOTRON.

Se è abilitato il parametro "Codice con prefisso", gli utenti possono essere autorizzati a modificare il proprio codice. Se è disabilitato il parametro "Codice con prefisso", i codici possono essere modificati dall'amministratore.

2.1.2. AUTORIZZAZIONE CODICE TASTIERA

L'autorizzazione con un codice utente è eseguita inserendo un codice valido sulla tastiera oppure mediante etichetta RFID.

Nel sistema si possono utilizzare codici a 4, 6 o 8 cifre.

Il sistema può essere configurato per l'uso con o senza codici con prefisso (impostazioni predefinite). Per i sistemi di allarme con numero di utenti elevato è possibile abilitare il prefisso. Per modificare quest'opzione si prega di rivolgersi al tecnico dell'assistenza del proprio sistema di allarme.

Codice senza prefisso: CCCC

cccc è un codice a 4, 6 o 8 cifre, i codici consentiti vanno da 0000 a 99999999

Codice della centrale predefinito Amministratore: **1234; 123456; 12345678;**

Codice senza prefisso: nnn*cccc

nnn è un prefisso che indica il numero della posizione dell'utente (posizione da 0 a 600)

* è un separatore (tasto *)

cccc è un codice a 4, 6 o 8 cifre, i codici consentiti vanno da 0000 a 99999999

Codice della centrale predefinito Amministratore: **1*1234; 1*123456; 1*12345678;**

AVVERTENZA: Il codice dell'amministratore principale inizia con il prefisso **1**

Il codice «Service» principale inizia col prefisso **0**

Per modificare il tipo di codice si prega di rivolgersi al tecnico dell'assistenza del proprio sistema di allarme.

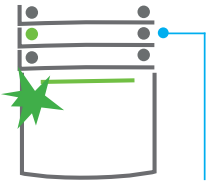
Struttura e descrizione del menu interno della tastiera LCD

Autorizzazione amministratore o utente mediante codice o scheda / etichetta RFID

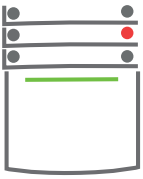
CANCELLA INDICAZIONE DI AVVERTIMENTO	Permette di cancellare un'indicazione di allarme o impostazione errata, in tutte le sezioni cui l'utente è autorizzato ad accedere
COMANDO SEZIONI	Permette di gestire le sezioni del sistema cui l'utente è autorizzato ad accedere e che sono abilitate nelle impostazioni interne.
COMANDO PG	Consente all'utente di comandare le uscite programmabili PG a seconda delle autorizzazioni utente e delle impostazioni interne.
MEMORIA EVENTI	Mostra elenco dettagliato della memoria eventi.
INSERIMENTO EVITATO	Mostra un elenco di rilevatori innescati per evitare l'inserimento del sistema, a condizione che questa opzione sia attivata nella configurazione della centrale.
GUASTI NEL SISTEMA	Mostra un elenco di tutti i rilevatori che indicano guasti al sistema, a partire dalle sezioni cui l'utente è autorizzato ad accedere.
RILEVATORI BYPASSATI	Mostra un elenco di tutti i rilevatori bloccati nelle sezioni cui l'utente è autorizzato ad accedere.
STATO SISTEMA	Mostra lo stato del sistema (elenco dei rilevatori innescati, contatti tamper innescati, batterie quasi scariche, bypass, ecc.).
IMPOSTAZIONI	Permette la modifica di utenti e dispositivi (solo quando l'USB è disconnesso).
IMPOSTAZIONE DEL DISPLAY	Permette la regolazione dell'intensità della retroilluminazione della tastiera e del contrasto del display.
MOD. MANUTENZIONE	Consente all'amministratore di commutare le sezioni assegnate in modalità Manutenzione.

2.1.2.1. IMPOSTAZIONE ALLARMI

1. Autorizza mediante tastiera. Le sezioni gestibili sono illuminate e il pulsante indicazione retroilluminato inizia a lampeggiare in verde.



2. Premere il pulsante destro (quello non illuminato) per impostare una sezione in particolare. Si possono impostare anche più sezioni contemporaneamente. L'intervallo di tempo tra la selezione delle sezioni non può superare 2 secondi.



3. Il comando viene eseguito e la tastiera indica acusticamente il ritardo uscita. A questo punto la sezione è impostata. Solo i rilevatori con una «zona ritardata» forniscono il tempo necessario per uscire dalla zona protetta durante il tempo di ritardo uscita. Il pulsante segmento della sezione impostata diventa rosso.

Durante l'impostazione di un allarme, se si innesca uno qualsiasi dei rilevatori (per esempio una finestra aperta), il sistema reagirà in una delle seguenti maniere (a seconda della configurazione del sistema):

:: I rilevatori assicurano protezione automaticamente dopo il loro passaggio in modalità stand-by (modalità predefinita).

:: Il sistema indica otticamente i rilevatori innescati tramite lampeggio in rosso di un segmento per 8 secondi; dopo di che il sistema si imposta automaticamente allo scadere di questo intervallo di tempo.

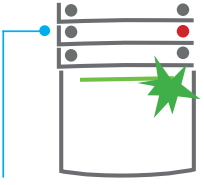
:: È anche possibile impostare una sezione con rilevatori innescati, premendo il pulsante segmento sul lato destro ripetutamente. In questo modo l'utente conferma la propria intenzione di impostare la sezione con il rilevatore innescato (per esempio: finestra aperta). Altrimenti la sezione con il rilevatore innescato non sarà impostata.

:: Un rilevatore innescato fa sì che la sezione non venga inserita. Questo stato è indicato otticamente da un pulsante segmento lampeggiante in rosso. Il rilevatore che non permette l'impostazione è indicato nel menu sul display della tastiera.

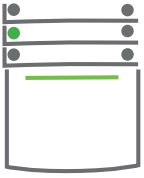
L'eventuale inserimento non riuscito è indicato mediante il lampeggio del pulsante giallo (è necessario però che sia abilitato il parametro "Inserimento non riuscito"). Consultare un tecnico di assistenza per l'installazione, al fi ne di programmare il comportamento desiderato del sistema.

2.1.2.2. DISINSERIMENTO DELL'ALLARME

1. All'entrata nell'edificio (con innesco di un rilevatore con reazione «zona ritardata»), il sistema si avvia indicando il ritardo entrata, emettendo un suono fisso e facendo lampeggiare in verde il pulsante segmento della sezione in cui l'entrata



ritardata è stata innescata. Autorizzare se stessi mediante tastiera – la spia verde del pannello autorizzazione inizia a lampeggiare.



2. Premere il pulsante segmento sinistro della sezione che si desidera disinserire.

3. Il comando viene eseguito e i pulsanti segmento diventano verdi, ad indicare l'avvenuto disinserimento della sezione.

Nota: Se è abilitato il parametro «Disinserire sezione mediante autorizzazione solo durante ritardo entrata», la sola autorizzazione basterà a disinserire la data sezione laddove il ritardo entrata è stato innescato.

2.1.2.3. CONTROLLO ACCESSO IN SITUAZIONI CRITICHE

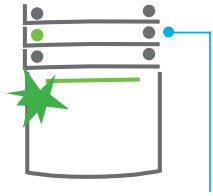
Questa funzione consente di disinserire il sistema in modalità speciale. Il sistema apparentemente si disinserisce; in realtà però innesca un allarme panico silenzioso, che viene quindi trasmesso agli utenti selezionati (compreso ARC). Il disinserimento in situazioni critiche viene eseguito aggiungendo un 1 all'ultimo numero, ad un codice valido.

Esempio di codice con prefisso:
Codice valido: 2*9999
Codice per disinserimento in situazioni critiche: 2*9990

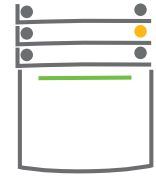
Esempio di codice senza prefisso:
Codice valido: 9999
Codice per disinserimento in situazioni critiche: 9990

2.1.2.4. IMPOSTAZIONE ALLARMI PARZIALE

1. Autorizzare se stessi con la tastiera (inserire un codice o leggere una scheda o etichetta con l'apposito lettore). La spia verde retroilluminata inizia a lampeggiare.



2. Premere il pulsante segmento destro della sezione selezionata.



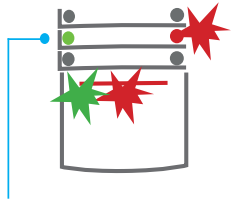
3. Il comando viene eseguito e il pulsante segmento diventa giallo, ad indicare che la sezione è stata parzialmente inserita.

Il sistema può anche essere configurato come parzialmente impostato (solo alcuni rilevatori nella sezione svolgeranno la propria funzione protettiva). Esempio: Di notte è possibile impostare unicamente i rilevatori della porta e delle fi nestre, mentre i rilevatori all'interno dell'abitazione sono disabilitati.

Per impostare interamente le strutture in cui l'inserimento parziale è abilitato, bisogna premere due volte il pulsante per l'inserimento del sistema. Alla prima pressione il pulsante inizia a lampeggiare in giallo; alla seconda pressione lampeggerà in rosso. Se il sistema era già in inserimento parziale (luce gialla fissa), l'intero sistema può essere completamente inserito mediante autorizzazione e premendo il pulsante giallo. Una volta schiacciato il pulsante, il sistema sarà completamente inserito e il pulsante diventerà rosso.

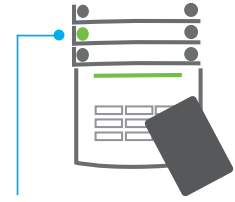
2.1.2.5. CESSAZIONE DI UN ALLARME INNESCATO

1. Autorizzare se stessi con la tastiera (inserire un codice, leggere un'etichetta con l'apposito lettore).



2. Premere il pulsante segmento sinistro della sezione in cui l'allarme è stato innescato.

3. Il disinserimento è completato e le sirene sono tacitate. Il pulsante verde lampeggiante indica il disinserimento di una sezione concreta. La spia rossa lampeggiante indica memoria allarmi.



4. Autorizzare se stessi e premere il pulsante verde ancora una volta al fi ne di cancellare l'indicazione memoria allarmi.

5. Il segmento indica la sezione disinserita mediante pulsante verde a luce fissa.

L'allarme innescato in corso è indicato da un lampeggio rapido del pulsante segmento rosso e da pulsante indicazione retroilluminato. Per poter far cessare l'allarme bisogna dapprima autorizzare se stessi mediante tastiera. La sezione resta inserita; il lampeggio rapido in rosso del pulsante segmento indica memoria allarmi. La spia continuerà a lampeggiare anche dopo il disinserimento del sistema.

Se durante la vostra assenza si è attivata la spia memoria allarmi, bisognerà ricercare la causa dell'allarme nella cronologia eventi. Prestare particolare attenzione nell'accedere e nel controllare le strutture oppure attendere l'arrivo dell'agenzia di sicurezza (se il vostro sistema è connesso ad un ARC).

La spia memoria allarmi per il dato segmento resta accesa, finché il sistema non viene reinserito. In maniera alternativa, è possibile effettuare la cancellazione disinserendo di nuovo il sistema. L'indicazione allarme può anche essere cancellata dal menu principale mediante una tastiera con display LCD – Cancella indicazione avvertimento.

L'indicazione di un allarme tamper innescato può essere cancellata soltanto da un tecnico dell'assistenza o amministratore.

Nota: Quando si usa il profilo sistema "EN 50131-1, grado 2" è sempre necessario autorizzare dapprima la propria persona e in seguito eseguire l'azione desiderata.

La cessazione di un allarme mediante comando a distanza disinserirà anche la sezione corrispondente.

2.1.2.6. COMANDO SEZIONE DAL MENU DELLA TASTIERA CON DISPLAY LCD

Gli stati delle sezioni sono visualizzati nella parte alta a sinistra del display LCD della tastiera. La sezione completamente inserita è illustrata da un numero in un rettangolo riempito in nero 2 ; la sezione parzialmente inserita è contrassegnata da un numero incorniciato 4 .

Controllo mediante menu tastiera:

:: Autorizzazione tramite codice valido o chip RFID.
:: Accedere al menu premendo ENTER.
:: Controllo sezione → ENTER.
:: Selezionare la sezione desiderata con l'ausilio delle frecce.
:: Premere ripetutamente ENTER per passare da uno stato sezione ad un altro (parzialmente inserita / inserita / disinserita).
:: Premere ESC per uscire dal menu.

2.1.3. MEDIANTE TASTIERE SISTEMA JA-110E E JA-150E

Gli stati delle singole sezioni sono segnalati dagli indicatori di stato A, B, C, D sopra il display LCD e dai pulsanti di funzione. La centrale può essere gestita direttamente (inserendo e disinserendo gli allarmi o altre funzioni di automazione) con l'ausilio dei pulsanti di funzione sulla tastiera. I pulsanti di funzione e gli indicatori di stato A, B, C, D sono muniti di retroilluminazione cromatica al fi ne di segnalare inequivocabilmente lo stato della sezione.

:: VERDE – Disinserito :: GIALLO – Parzialmente disinserito :: ROSSO – Inserito

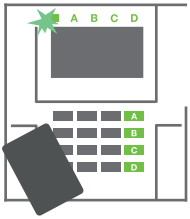
L'autorizzazione può essere effettuata digitando un codice d'accesso sulla tastiera oppure utilizzando una scheda/ targhetta RFID assegnata ad un particolare utente. Ciascun utente può avere un unico codice e un unico chip RFID (una scheda oppure una targhetta). Se gli utenti desiderano gestire più sezioni contemporaneamente, è necessario che diano l'autorizzazione a se stessi e che premano poi successivamente i pulsanti funzione delle sezioni in questione. In questa maniera gli utenti possono annullare tutte le sezioni (per esempio casa e garage) con una singola autorizzazione.

Struttura e descrizione del menu interno della tastiera LCD

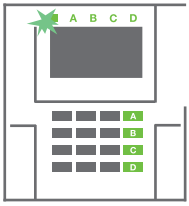
Autorizzazione amministratore o utente mediante codice o scheda / etichetta RFID

CANCELLA INDICAZIONE DI AVVERTIMENTO	Permette di cancellare un'indicazione di allarme o impostazione errata, in tutte le sezioni cui l'utente è autorizzato ad accedere
COMANDO SEZIONI	Permette di gestire le sezioni del sistema cui l'utente è autorizzato ad accedere e che sono abilitate nelle impostazioni interne.
COMANDO PG	Consente all'utente di comandare le uscite programmabili PG a seconda delle autorizzazioni utente e delle impostazioni interne.
MEMORIA EVENTI	Mostra elenco dettagliato della memoria eventi.
INSERIMENTO EVITATO	Mostra un elenco di rilevatori innescati per evitare l'inserimento del sistema, a condizione che questa opzione sia attivata nella configurazione della centrale.
GUASTI NEL SISTEMA	Mostra un elenco di tutti i rilevatori che indicano guasti al sistema, a partire dalle sezioni cui l'utente è autorizzato ad accedere.
RILEVATORI BYPASSATI	Mostra un elenco di tutti i rilevatori bloccati nelle sezioni cui l'utente è autorizzato ad accedere.
STATO SISTEMA	Mostra lo stato del sistema (elenco dei rilevatori innescati, contatti tamper innescati, batterie quasi scariche, bypass, ecc.).
IMPOSTAZIONI	Permette la modifica di utenti e dispositivi (solo quando l'USB è disconnesso).
IMPOSTAZIONE DEL DISPLAY	Permette la regolazione dell'intensità della retroilluminazione della tastiera e del contrasto del display.
MOD. MANUTENZIONE	Consente all'amministratore di commutare le sezioni assegnate in modalità Manutenzione.

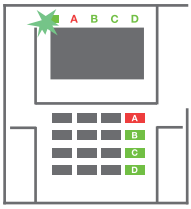
2.1.3.1. IMPOSTAZIONE ALLARMI



1. Autorizzazione per se stessi mediante tastiera. I pulsanti di funzione A, B, C, D delle sezioni per cui si ha l'autorizzazione si accenderanno e l'indicatore di sistema inizierà a lampeggiare con luce verde.



2. Premere il pulsante di funzione per impostare una sezione particolare. Si possono impostare anche più sezioni contemporaneamente. L'intervallo di tempo tra la selezione delle sezioni non può superare 2 secondi.



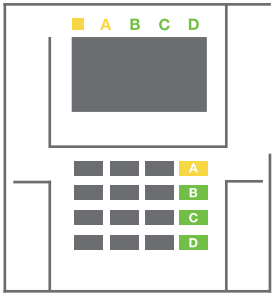
3. Il comando viene eseguito e la tastiera indica acusticamente il ritardo uscita. A questo punto la sezione è impostata. Solo i rilevatori con una «zona ritardata» forniscono il tempo necessario per uscire dalla zona protetta durante il tempo di ritardo uscita. L'indicatore di stato e il pulsante funzione della sezione inserita si accenderanno con luce rossa.

Durante l'impostazione di un allarme, se si innesca uno qualsiasi dei rilevatori (per esempio una finestra aperta), il sistema reagirà in una delle seguenti maniere (a seconda della configurazione del sistema):

:: La centrale si inserisce. I rilevatori innescati saranno automaticamente bloccati.*)
:: Il sistema indica otticamente i rilevatori innescati tramite mediante il lampeggio in rosso di un pulsante di funzione per 8 secondi; dopo di che la centrale si inserisce automaticamente allo scadere di questo intervallo di tempo (i rilevatori innescati sono bloccati). *)
:: È anche possibile impostare una sezione con rilevatori innescati, premendo il pulsante di funzione ripetutamente. L'utente conferma la propria intenzione di inserire la sezione con il rilevatore innescato (per esempio: finestra aperta). Altrimenti il sistema non si inserisce.
:: Un rilevatore innescato fa sì che la sezione non venga inserita. Questo stato è indicato otticamente da un pulsante di funzione lampeggiante in rosso. Il rilevatore che non permette l'inserimento è indicato nel menu del display LCD.

*) **AVVERTENZA**: Le opzioni a) e b) non sono supportate da EN 50131, grado 2 (profilo sistema centrale selezionato)

Se un rilevatore con reazione "Allarme zona istantaneo" viene ad innescarsi durante un ritardo uscita oppure se un rilevatore con reazione "Allarme zona ritardato" rimane innescato dopo l'estinzione del ritardo uscita, la centrale si disinserirà di nuovo. L'eventuale mancato inserimento viene indicato dalla luce gialla lampeggiante dell'indicatore di sistema, per poi essere trasmesso all'ARC e segnalato da una sirena esterna (per il grado di sicurezza 2).

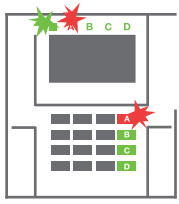


Se la centrale è configurata in modo tale da essere inserita senza autorizzazione, non sarà necessario autorizzare se stessi. Bisogna semplicemente premere un pulsante funzione di una sezione specifica. È anche possibile configurare la centrale in modo che l'inserimento avvenga mediante semplice autorizzazione.

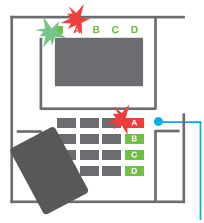
AVVERTENZA: L'inserimento senza autorizzazione abbassa automaticamente il livello di sicurezza massimo al grado 1. Considerare tutti i possibili rischi ineriti all'applicazione di tale funzione.

Consultare un consulente di progetto o un tecnico di assistenza per l'installazione, al fi ne di programmare il comportamento desiderato del sistema allarme.

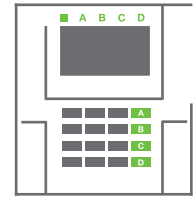
2.1.3.2. DISINSERIMENTO DELL'ALLARME



1. All'entrata nell'edificio (con innesco di un rilevatore con reazione «zona ritardata»), il sistema si avvia indicando il ritardo entrata, emettendo un suono fisso. Inoltre, l'indicatore di sistema e il pulsante di funzione lampeggiano entrambi con luce rossa (per la sezione in cui l'entrata ritardata è stata innescata).



2. Autorizzazione per se stessi mediante tastiera – l'indicatore di sistema inizierà a lampeggiare con luce verde.



3. Premere i pulsante di funzione delle sezioni che si desidera disinserire.

4. Il comando è eseguito. I pulsanti di funzione e l'indicatore di sistema diventano verdi, ad indicare le sezioni disinserite.

Nota: Se è abilitato il parametro «Disinserire sezione mediante autorizzazione solo durante ritardo entrata», la sola autorizzazione basterà a disinserire la sezione dove l'entrata ritardata è stata innescata. Quest'opzione va impiegata con cautela quando si usano sezioni multiple.

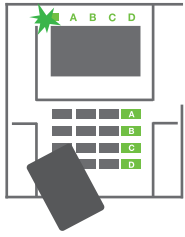
Consultare un tecnico di assistenza per l'installazione, al fi ne di programmare il comportamento desiderato del sistema.

2.1.3.3. IMPOSTAZIONE ALLARMI PARZIALE

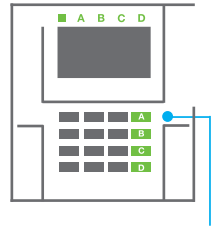
AVVERTENZA: Si tratta di una funzione aggiuntiva del sistema allarme.

Il sistema può anche essere configurato come parzialmente impostato (solo alcuni rilevatori nella sezione svolgeranno la propria funzione protettiva).

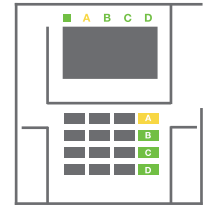
Esempio: Di notte è possibile impostare solo i rilevatori porta e finestra, mentre i rilevatori di movimento selezionati non faranno innescare l'allarme se qualcuno si muove all'interno della sezione.



1. Autorizzazione per se stessi con la tastiera (inserire un codice o utilizzare una scheda o targhetta RFID a contatto con l'apposito lettore). Il pulsante indicatore di sistema inizia a lampeggiare con luce verde.



2. Premere il pulsante di funzione della sezione selezionata.



3. Il comando viene eseguito e il pulsante di funzione diventa giallo fisso, ad indicare che la sezione è stata parzialmente inserita.

Per inserire le intere strutture in cui l'inserimento parziale è abilitato, tenere premuto il pulsante di inserimento della centrale per 2 secondi oppure premerlo per due volte. Una volta premuto il pulsante, verrà emessa luce gialla fissa. Dopo aver premuto il pulsante per una seconda volta, verrà emessa luce rossa fissa.

Se il sistema era già in inserimento parziale, il pulsante di funzione sarà caratterizzato da luce gialla fissa; l'intero sistema può essere completamente inserito mediante autorizzazione e premendo più a lungo il pulsante giallo. Una volta schiacciato il pulsante, il sistema sarà completamente inserito e il pulsante diventerà rosso.

L'inserimento parziale può essere configurato anche in modo tale da non rendere obbligatoria l'autorizzazione.

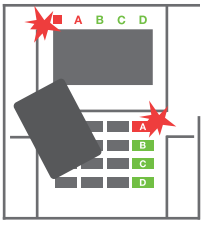
Per disinserire la centrale quando è parzialmente inserita, premere il pulsante giallo. La centrale si disinserisce e il pulsante torna ad essere verde.

2.1.3.4. CONTROLLO ACCESSO IN SITUAZIONI CRITICHE

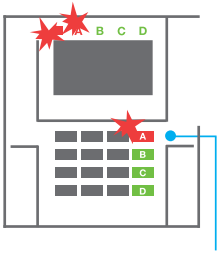
Consente di disinserire la centrale in modalità speciale. Il sistema apparentemente si disinserisce; in realtà però innesca un allarme panico silenzioso, che viene trasmesso agli utenti selezionati (compreso ARC). Il disinserimento in situazioni critiche viene eseguito aggiungendo un 1 all'ultimo numero, ad un codice valido. Per l'impiego di questa funzionalità contattare il tecnico dell'assistenza.

Esempio: Codice valido: 9999 Codice per disinserimento in situazioni critiche: 9990

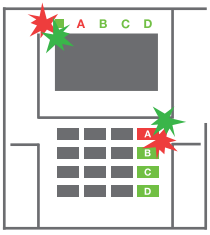
2.1.3.5. CESSAZIONE DI UN ALLARME INNESCATO



1. Autorizzazione per se stessi con la tastiera (inserire un codice o leggere una targhetta con l'apposito lettore).



2. Premere il pulsante di funzione della sezione in cui l'allarme è stato innescato.



3. Il disinserimento è completato e le sirene sono tacitate. I pulsanti di funzione lampeggiano con rapida intermittenza (verde/rosso) e gli indicatori di stato segnalano la memoria allarme.

L'allarme innescato in corso è indicato dall'indicatore di stato e dal rapido lampeggio rosso del pulsante di funzione. Per poter far cessare l'allarme bisogna dapprima autorizzare se stessi mediante tastiera. La sezione resta inserita; il lampeggio rapido in rosso del pulsante di funzione indica memoria allarmi. La spia continuerà a lampeggiare anche dopo il disinserimento del sistema.

AVVERTENZA: Se durante la vostra assenza si è attivata la spia memoria allarmi, sarà necessario sempre entrare con molta cautela nell'edificio e poi bisognerà ricercare la causa dell'allarme nella cronologia eventi. Prestare particolare attenzione nell'accedere e nel controllare le strutture oppure attendere l'arrivo dell'agenzia di sicurezza (se il vostro sistema è connesso ad un Centro Ricezione Allarmi).

La spia memoria allarmi resta accesa finché il sistema non viene reinserito. In alternativa, può anche essere cancellato dal menu tastiera. Menu principale – Cancella indicazione di avvertimento. L'indicazione di un allarme tamper innescato può essere cancellata soltanto da un tecnico dell'assistenza e amministratore.

Nota: Quando si impiega il profilo sistema «predefinito», è possibile selezionare una particolare azione premendo un pulsante di funzione e dandone conferma tramite autorizzazione con l'ausilio della tastiera.

La cessazione di un allarme mediante comando a distanza disinserirà anche la sezione corrispondente.

2.1.3.6. GESTIONE DEL SISTEMA MEDIANTE PORTACHIAVI

I portachiavi devono essere registrati nel sistema (installatore). Il portachiavi può essere collegato ad utenti specifici, per evitare la notifica di SMS ad utenti che interagiscono col sistema in quel dato istante (se i parametri di notifica sono così impostati). I portachiavi controllano ed indicano lo stato della batteria e sono muniti di indicazione ottica ed acustica.

PORTACHIAVI BIDIREZIONALE

Le funzioni pulsante sono differenziate mediante icone lucchetto. L'icona lucchetto chiuso inserisce le sezioni programmate; l'icona lucchetto aperto le disinserisce. La corretta esecuzione del comando è confermata da una luce LED; disinserimento – verde, inserimento – rossa. Eventuali errori di comunicazione (fuori dal range della centrale) sono segnalati da un singolo lampeggio del LED giallo. I pulsanti con i simboli di cerchi pieni e vuoti possono servire a controllare un'altra sezione. Anche i pulsanti del portachiavi possono essere con figurati per la gestione di uscite PG in diverse maniere: il primo pulsante serve per l'accensione; il secondo pulsante serve per lo spegnimento; ciascun pulsante può avere una funzione singola quando si impiegano le funzioni a impulsi o modifica. Per ulteriori funzioni è possibile premere due pulsanti contemporaneamente. In questa maniera un portachiavi a 4 pulsanti può avere fi no ad un massimo di 6 funzioni o un'unica uscita PG (per esempio spegnimento e accensione delle luci), o in alternativa due uscite PG (per esempio saracinesca e serratura della porta).

Se il sistema è configurato secondo la modalità «Inserimento dopo conferma», il rilevatore indicherà che l'inserimento non è andato a buon fi ne mediante l'accensione del LED verde, se un dispositivo è innescato. Bisogna confermare l'inserimento premendo di nuovo il pulsante di blocco. L'inserimento della sezione è confermato dall'accensione del LED rosso.

I pulsanti del portachiavi possono essere bloccati al fi ne di evitare che vengano premuto involontariamente. Quando un pulsante viene premuto ripetutamente, viene emesso un comando. L'eventuale batteria scarica è indicata da una segnalazione acustica (con 3 beep) ed anche otticamente mediante LED giallo lampeggiante, dopo la pressione di un pulsante. Per ulteriori informazioni consultare il proprio tecnico di assistenza per la configurazione del comando a distanza.

PORTACHIAVI UNILATERALI

I portachiavi unilaterali inviano un segnale ogni volta che un pulsante viene premuto senza ricevere alcun feedback dalla centrale. L'invio del segnale è confermato solo da un breve lampeggio del LED rosso e in alternativa con un beep.

2.2. OPERAZIONI A DISTANZA

Il massimo del comfort per la gestione delle operazioni a distanza del sistema è garantito dal servizio MyJABLOTRON. L'interfaccia web MyJABLOTRON è un servizio unico che consente l'accesso online ai dispositivi JABLOTRON. Permette agli utenti finali di monitorare e gestire il sistema. È disponibile sotto forma di applicazione per smartphone e come applicazione web. Il servizio MyJABLOTRON consente agli utenti di:

:: Visualizzare lo stato corrente del sistema,
:: In serire/disinserire l'intero sistema o parte di esso,
:: Gestire le uscite programmabili,
:: Visualizzare ia eventi,
:: Inviare report agli utenti selezionati mediante messaggi SMS, e-mail o notifiche PUSH,
:: Catturare immagini da dispositivi diverifica foto e sfogliarle nella Galleria fotografi ca o direttamente negli Eventi recenti,
:: Monitorare la temperatura attuale o il consumo di energia attuale, compresa panoramica della cronologia su grafici,
:: Ed altre funzionalità utili.

A seconda del paese e dell'area geografi ca è possibile impostare un account web su MyJABLOTRON da parte di un partner JABLOTRON autorizzato. Il nome login è l'indirizzo e-mail dell'utente. La password per il primo login sarà inviata a questo indirizzo. La password può essere modificata ogniqualvolta lo si vuole nelle impostazioni utente.

2.2.1. GESTIONE DEL SISTEMA MEDIANTE APPLICAZIONE SMART-PHONE MyJABLOTRON

Una volta creato un conto utente, l'utente potrà monitorare e gestire il sistema a distanza attraverso l'applicazione MyJABLOTRON per smartphone Android e iOS.

2.2.2. IMPIEGO DEL SISTEMA VIA INTERFACCIA WEB MyJABLOTRON

Il sistema JABLOTRON 100+ può essere gestito in maniera facile e conveniente mediante il vostro computer via internet tramite interfaccia web MyJABLOTRON, disponibile su www.myjablotron.com.

2.2.3. IMPIEGO DEL SISTEMA MEDIANTE MENU VOCALE

Il sistema può essere gestito da un telefono mediante un semplice menu vocale che guida l'utente nell'ambito di una serie di opzioni nella lingua preconfigurata. Per accedere al menu vocale basta chiamare il numero di telefono del sistema allarmi.

L'accesso al menu vocale può essere abilitato per tutti i numeri di telefono senza alcuna limitazione oppure soltanto ad determinati numeri autorizzati e archiviati presso la centrale. A seconda della configurazione, è possibile richiedere un'autorizzazione inserendo un codice valido mediante la tastiera del telefono. Quando l'utente accede al menu, il sistema fornisce un aggiornamento dello stato attuale di tutte le sezioni assegnate all'utente. La persona che chiama può quindi controllare queste sezioni, una per una oppure tutte insieme, servendosi della tastiera del telefono e delle opzioni menu disponibili.

Come impostazione predefinita il sistema risponde alle chiamate in arrivo dopo tre squilli (circa 15 secondi).

2.2.4. IMPIEGO DEL SISTEMA MEDIANTE COMANDI SMS

I comandi SMS sono in grado di gestire le sezioni singole e le uscite programmabili alla stessa stregua dei pulsanti segmento della tastiera. Il formato del messaggio di testo sarà il seguente: CODICE_COMANDO. I comandi del sistema sono predefiniti (INSERISCI/DISINSERISCI) con un parametro numerico aggiuntivo che identifica una sezione specifica. Un messaggio SMS è in grado di controllare più sezioni contemporaneamente. In questo caso i numeri aggiunti nel comando definiscono le sezioni.

Esempio di un comando SMS utilizzato per inserire le sezioni 2 e 4.
CODE_SET_2_4

I comandi per la gestione delle uscite programmabili possono essere programmati da un installatore di sistema. Per esempio, si può scegliere CHIUDERE LE TAPPARELLE come proprio comando per la chiusura delle tapparelle della finestra. È anche possibile configurare il sistema in maniera tale che non venga richiesto alcun codice prima di un comando. In questo caso il comando è semplicemente ed automaticamente identificato nel momento in cui il sistema riconosce il numero di telefono dell'utente da cui è stato inviato l'SMS. La configurazione è effettuata da un tecnico dell'assistenza.

2.2.5. GESTIONE DEL SISTEMA A DISTANZA MEDIANTE COMPUTER (J-LINK)

Il sistema JABLOTRON 100+ può essere gestito a distanza mediante un computer con software J-Link installato. Può essere scaricato dalla sezione «Download» sul sito **www.myjablotron.com**.

2.2.6. COMANDO DELLE USCITE PROGRAMMABILI (PG)

2.2.6.1. SEGMENTO TASTIERA

L'uscita PG si accende dopo la pressione del pulsante destro del segmento e si spegne premendo il pulsante sinistro. Se l'uscita è configurata come uscita ad impulsi, si spegnerà in base all'intervallo di tempo predefinito. Il comando PG può essere salvato (oppure non essere salvato) nella memoria eventi della centrale. La configurazione è effettuata da un tecnico dell'assistenza. A seconda della configurazione del sistema, è possibile stabilire se l'autorizzazione debba essere obbligatoriamente richiesta o meno.

2.2.6.2. AUTORIZZAZIONE TASTIERA UTENTE

È possibile attivare un'uscita PG semplicemente mediante autorizzazione utente (inserendo un codice oppure utilizzando un'etichetta RFID). L'uscita PG deve essere configurata in maniera tale da attivarsi da una tastiera definita.

2.2.6.3. DAL MENU DELLA TASTIERA CON DISPLAY LCD

Dopo l'autorizzazione utente, le uscite programmabili possono essere gestite dal menu della tastiera con display LCD. L'utente ha accesso alle uscite programmabili a seconda delle autorizzazioni utente.

Controllo mediante menu tastiera:

:: Autorizzazione tramite codice valido o chip RFID.
:: Accedere al menu premendo ENTER.
:: PG Control → ENTER.
:: Selezionare il gruppo PG desiderato mediante le frecce (1–32), (33–64), (65–96), (97–128) → ENTER.
:: Selezionare la PG desiderata con l'ausilio delle frecce → ENTER.
:: Premendo ripetutamente il tasto ENTER si cambiano gli stati delle PG (la PG attiva è mostrata da un numero PG in un rettangolo in nero .
:: Premere ESC per uscire dal menu.

2.2.6.4. COMANDO A DISTANZA

Premendo un pulsante associato del telecomando. I telecomandi bidirezionali confermano l'attivazione delle uscite PG con una spia LED.

2.2.6.5. APPLICAZIONE SMARTPHONE MyJABLOTRON

Toccando ON/OFF nella scheda Automazione (PG).

2.2.6.6. INTERFACCIA WEB B MyJABLOTRON

Facendo clic su ON/OFF nella scheda Automazione (PG).

2.2.6.7. COMPOSIZIONE NUMERI TRAMITE TELEFONO

Ciascun numero di telefono archiviato nel sistema (un unico numero di telefono per ciascun utente) è in grado di gestire un'unica PG semplicemente facendo il numero (ovvero senza realizzare una chiamata vera e propria). Basta comporre il numero di telefono della scheda SIM utilizzata nel sistema di sicurezza e riagganciare prima che il sistema risponda alla chiamata. Secondo le impostazioni predefinite il sistema risponde alla chiamata dopo il terzo squillo (circa 15 secondi).

2.2.6.8. MESSAGGIO SMS

L'invio di un SMS può accendere/spegnere una data PG. A seconda della configurazione del sistema, è possibile stabilire se l'autorizzazione debba essere obbligatoriamente richiesta o meno. Esempio: TESTO CODICE_CONFIGURATO

3. BLOCCO/DISABILITAZIONE DEL SISTEMA

3.1. BLOCCO DI UTENTI

Qualsiasi utente può essere temporaneamente bloccato (per esempio se ha perso la propria scheda/etichetta oppure il suo codice è stato svelato). Quando l'accesso dell'utente è bloccato, il suo codice o scheda/etichetta non sarà accettato dal sistema. L'utente bloccato non riceve più alcun SMS di avvertimento o report vocale sul proprio telefono.

Solo l'amministratore del sistema e il tecnico dell'assistenza possono bloccare un utente. Un metodo per rimuovere i diritti d'accesso è il seguente: scegliere Impostazioni / Utenti / Utente / Bypass e selezionare «Sì» sul tastierino LCD. Un'altra modalità consiste nel bloccare localmente o a distanza un utente attraverso il software J-Link, facendo clic sull'utente nella colonna Impostazioni / Utenti / Blocco utenti.

L'utente bloccato (disabilitato) è contrassegnato con un cerchio rosso finché il blocco non viene annullato.

3.2. BLOCCAGGIO DEI RILEVATORI

Un rilevatore può essere temporaneamente bloccato in maniera simile agli utenti. I rilevatori vengono bloccati quando la loro attivazione è temporaneamente indesiderata (per esempio, rilevatore di movimento in una stanza con presenza di animale domestico oppure disabilitazione del segnale acustico di una sirena). Il sistema continua ad eseguire diagnosi di contatti tamper ed invia informazioni su eventi di assistenza, anche se la funzione allarme è disattivata.

Solo l'amministratore del sistema e il tecnico dell'assistenza possono bloccare un rilevatore. Il rilevatore può essere bloccato scegliendo Impostazioni / Dispositivi / Bypass e selezionando Sì sulla tastiera LCD. Un'ulteriore modalità consiste nell'impiego del software J-Link facendo clic sul rilevatore nella colonna Impostazioni / Diagnosi / Disabilitato. I rilevatori bloccati sono contrassegnati da un cerchio giallo finché non vengono ripristinati mediante la medesima procedura. I dispositivi possono anche essere bloccati mediante applicazione smartphone MyJABLOTRON.

3.3. DISABILITAZIONE TIMER

Per disabilitare temporaneamente gli eventi programmati automatici nel sistema bisogna disabilitare il timer. Se si disabilita un evento programmato (per es. disinserimento della sorveglianza notturna in determinate fasce orarie), il dato evento non avrà luogo (per esempio, quando si è in vacanza).

Il timer può essere disabilitato localmente o a distanza attraverso il software J-Link facendo clic sulla rispettiva sezione nella colonna Impostazioni / Calendario / Bloccato. I timer disabilitati sono contrassegnati da un cerchio rosso finché non vengono ripristinati mediante la medesima procedura.

4. PERSONALIZZAZIONE DEL SISTEMA

4.1. MODIFICA DEL CODICE ACCESSO UTENTE

Se il sistema è impostato senza codici con prefisso, solo l'amministratore di sistema e il tecnico dell'assistenza saranno in grado di modificare i codici di sicurezza. L'amministratore di sistema può effettuare modifiche tramite menu tastiera LCD, software J-Link o applicazione smartphone MyJABLOTRON. Il codice può essere modificato dopo autorizzazione selezionando Impostazioni / Utenti / Utente / Codice. Per inserire un nuovo codice è necessario accedere alla modalità Modifica (il codice inizia a lampeggiare) premendo Enter; accedere poi a Nuovo codice e confermare premendo di nuovo Enter. Una volta completate le modifiche, è necessario darne conferma selezionando Salva quando il sistema vi chiederà «Salvare le impostazioni».

Se il sistema viene impostato con codici con prefisso, è possibile autorizzare utenti singoli a modificare i propri codici dal menu LCD sulla tastiera.

4.2. MODIFICA, ELIMINAZIONE O AGGIUNTA DI SCHEDE/ ETICHETTE RFID

Se il sistema è impostato senza codici con prefisso, solo l'amministratore di sistema e il tecnico dell'assistenza saranno in grado di modificare i codici di sicurezza. L'amministratore di sistema può effettuare modifiche tramite menu tastiera LCD, software J-Link o applicazione smartphone MyJABLOTRON. Il codice può essere modificato dopo autorizzazione selezionando Impostazioni / Utenti / Utente / Codice. Per inserire un nuovo codice è necessario accedere alla modalità Modifica (il codice inizia a lampeggiare) premendo Enter; accedere poi a Nuovo codice e confermare premendo di nuovo Enter. Una volta completate le modifiche, è necessario darne conferma selezionando Salva quando il sistema vi chiederà «Salvare le impostazioni».

Se il sistema viene impostato con codici con prefisso, è possibile autorizzare utenti singoli a modificare i propri codici dal menu LCD sulla tastiera.

4.3. MODIFICA DEL NOME UTENTE O NUMERO TELEFONICO

Se il sistema è impostato con uso di codici con prefisso, gli utenti saranno in grado di aggiungere, modificare o eliminare i propri numeri di telefono o cambiare il loro nome sul menu LCD tastiera. Tali operazioni si possono eseguire dopo rispettiva autorizzazione selezionando Impostazioni / Utenti / Utente / Telefono. Per effettuare le modifiche l'utente deve trovarsi in modalità Modifica. Per accedervi premere Enter. Le modifiche effettuate vanno confermate premendo di nuovo Enter. Per cancellare un numero di telefono premere «0» nel campo numeri di telefono. Una volta effettuate, le modifiche vanno salvate selezionando Salva, quando il sistema chiederà «Salvare le impostazioni?».

L'amministratore di sistema e il tecnico dell'assistenza possono aggiungere, modificare o eliminare il numero di telefono di un utente oppure cambiare il nome di un utente sia mediante tastiera LCD che mediante il software J-Link.

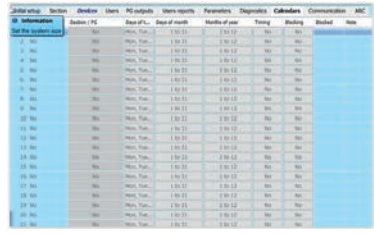
4.4. AGGIUNTA/ELIMINAZIONE DI UTENTI

Solo l'amministratore di sistema e il tecnico dell'assistenza hanno la possibilità di aggiungere nuovi utenti al sistema (o eliminarli). I nuovi utenti possono essere aggiunti o eliminati soltanto mediante il software J-Link (o F-Link per i tecnici).

Durante il processo di creazione di un nuovo utente, è necessario assegnargli i permessi per l'accesso (diritti), le sezioni che l'utente può gestire, le uscite programmabili da comandare ed anche il tipo di autorizzazione richiesto per il dato utente.

4.5. IMPOSTAZIONE CALENDARIO EVENTI

È possibile configurare eventi calendario (disinserimento/ inserimento/inserimento parziale, controllo o bloccaggio delle uscite PG). Gli eventi calendario possono essere impostati mediante il software J-Link nella scheda Calendario.



Per ciascun evento calendario, azione, sezione o uscita PG, viene impostato un orario e una data esatta. Il giorno può essere definito come un giorno della settimana, mese o anno. Per quanto riguarda il giorno selezionato, è possibile eseguire fi no a 4 impostazioni, per realizzare un'azione o per importare la ripetizione ad intervalli regolari.

Pertanto, gli eventi calendario possono essere personalizzati non solo per il comando delle sezioni, ma anche per controllare varie tecnologie nell'edificio mediante le uscite PG.

5. CRONOLOGIA EVENTI

Il sistema di sicurezza salva tutte le operazioni e gli eventi realizzati (inserimenti, disinserimenti, allarmi, guasti, messaggio inviati ad utenti e ARC) nella micro-scheda SD nella centrale del sistema. Ciascuna registrazione comprende la data, orario (inizio e fi ne) e la fonte (causa/origine) dell'evento.

Varie modalità di esplorazione attraverso la cronologia eventi del sistema:

5.1. MEDIANTE TASTIERA LCD

Per entrare nella cronologia eventi mediante la tastiera è necessaria l'autorizzazione utente. Una volta concessa l'autorizzazione, le opzioni disponibili (sulla base dei permessi utente) sono visualizzate selezionando Memoria eventi. Le registrazioni possono essere visualizzate mediante le frecce.

5.2. MEDIANTE SOFTWARE J-LINK E COMPUTER

La memoria del sistema può essere esplorata tramite il software J-Link. Gli eventi possono essere scaricati dalla centrale in piccoli batch (circa 1.200 eventi) o grandi batch (circa 4.000 eventi). Gli eventi possono essere filtrati nei dettagli, codificati cromaticamente per favorire la loro identificazione oppure salvati su un file in un computer.

5.3. ACCESSO A MyJABLOTRON (WEB/SMARTPHONE)

Tutti gli eventi del sistema possono essere visualizzati accedendo all'interfaccia web/smartphone MyJABLOTRON. L'account mostra la cronologia secondo un range corrispondente ai permessi dell'utente.

6. SPECIFICHE TECNICHE

<table>
<tr><th>PARAMETRO</th><th colspan="2">JA-103K</th><th colspan="2">JA-107K</th></tr>
<tr><td>Alimentazione della centrale</td><td colspan="2">~ 110–230 V / 50–60 Hz,
max. 0,28 A con fusibile F1.6 A/250 V
Classe protezione II</td><td colspan="2">~ 110–230 V / 50–60 Hz,
max. 0,85 A con fusibile F1.6 A/250 V
Classe protezione II</td></tr>
<tr><td>Batteria backup</td><td colspan="2">12 V; 2.6 Ah (piombo gel)</td><td colspan="2">12 V; 7 to 18 Ah (piombo gel)</td></tr>
<tr><td>Tempo di caricamento massimo della batteria</td><td colspan="2">72 h</td><td colspan="2"></td></tr>
<tr><td>Tensione BUS (rosso - nero)</td><td colspan="2">12,0 a 13,8V</td><td colspan="2"></td></tr>
<tr><td>Consumo continuo massimo di corrente da centrale</td><td colspan="2">1000 mA</td><td colspan="2">2000 mA permanente
3000 mA per 60 minuti
(max. 2000 mA per un unico BUS)</td></tr>
<tr><td rowspan="2">Consumo continuo massimo di corrente per back-up 12 ore</td><td>Senza comunicatore GSM</td><td>LAN – OFF
115 mA
LAN – ON
88 mA</td><td colspan="2">Valido per batteria backup 18 Ah</td></tr>
<tr><td>Con comunicatore GSM</td><td>LAN – OFF
80 mA
LAN – ON
53 mA</td><td>Senza comunicatore GSM</td><td>LAN – OFF
1135 mA
LAN – ON
1107 mA</td></tr>
<tr><td></td><td></td><td>Con comunicatore GSM</td><td>LAN – OFF
1100 mA
LAN – ON
1072 mA</td></tr>
<tr><td>Numero di dispositivi massimo</td><td colspan="2">50</td><td colspan="2">230</td></tr>
<tr><td>Comunicatore LAN</td><td colspan="2">ETHERNET INTERFACE, 10/100BASE-T</td><td colspan="2"></td></tr>
<tr><td>Dimensioni (mm)</td><td colspan="2">268 x 225 x 83 mm</td><td colspan="2">357 x 297 x 105 mm</td></tr>
<tr><td>Peso con/senza AKU</td><td colspan="2">1844 g/970 g</td><td colspan="2">7027 g/1809 g</td></tr>
<tr><td>Reazione a inserimento codice non valido</td><td colspan="2">Allarme dopo 10 inserimenti di codici errati</td><td colspan="2"></td></tr>
</table>

PARAMETRO	JA-103K	JA-107K
Memoria eventi	Circa 7 milioni di ultimi eventi, compresa data e orario	
Unità alimentazione	Tipo A (secondo EN 50131-6)	
Comunicatore GSM (2G)	850 / 900 / 1800 / 1900 MHz	
Classificazione	Livello di sicurezza 2 / Classe ambiente II (secondo EN 50131-1)	
Ambiente operativo	Interno generale	
Range di temperatura d'esercizio	da -10 °C a +40 °C	
Umidità d'esercizio media	75 % RH, senza condensa	
Conforme a	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	
Frequenza operativa radio (con modulo JA-11xR)	868.1 MHz, protocollo JABLOTRON	
Emissioni radio	ETSI EN 300 220-1,-2 (module R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7	
Conformità in termini di sicurezza	EN 62368-1+A11	
Condizioni operative	ERC REC 70-03	
Organismo di certificazione	Trezor Test s.r.o. (no. 3025)	
Identificazione chiamante (CLIP)	ETSI EN 300 089	

JABLOTRON ALARMS a.s. con la presente è a dichiarare che le centrali JA-103K a JA-107K sono conformi alle rispettive norme comunitarie armonizzate: Direttive n.: 2014/53/UE, 2014/35/UE, 2014/30/UE, 2011/65UE, se impiegato secondo le istruzioni. Per l'originale della valutazione della conformità si rimanda a www.jablotron.com – sezione Download.

Nota: Benché i prodotti non contengano materiali dannosi, al termine della loro vita utile consigliamo comunque di riconsegnarli al rivenditore o direttamente al produttore.

СОДЕРЖАНИЕ

ПЕРИОДИЧЕСКОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

:: Для обеспечения надежного функционирования системы необходимо своевременно проводить регулярные и своевременные проверки технического состояния системы. Большая часть работ по обслуживанию выполняется компанией-установщиком по меньшей мере раз в год во время периодических проверок технического состояния.

:: Обслуживание, выполняющееся пользователем, в основном заключается в чистке отдельных устройств. АДМИНИСТРАТОР системы может переключить систему в режим ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ, что позволить открыть датчики (для замены батарей) или снять их с места установки. С запросом включения режима ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ обратитесь в компанию, выполнявшую установку. Если система конфигурирована с профилем системы «EN 50131-1, класс 2», включить режим ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ невозможно.

:: Систему можно переключить в режим технического обслуживания в программе J-Link или из меню клавиатуры с ЖК-дисплеем. После авторизации можно выбрать «Режим технического обслуживания», а также разделы, где необходимо выполнить техническое обслуживание. В режиме технического обслуживания в выбранных разделах не будут подаваться сигналы тревоги, включая открытие датчиков или их снятие с места установки.

:: Индикация режима технического обслуживания – это мигание зеленым светом кнопки активации (мигает 2 раза через каждые 2 секунды) и выключение двух кнопок сегмента конкретного раздела.

:: При обращении с устройствами, во избежание повреждения пластмассовых деталей и механизмов датчиков, необходимо проявлять осторожность. а Крышка обычно крепится лепестком, который необходимо слегка вдавить в корпус датчика каким-либо инструментом (например, отверткой), а затем крышку можно будет снять. В некоторых случаях этот лепесток зафиксирован небольшим стопорным винтом, сначала необходимо вывинтить.

:: При замене батарей в датчике обязательно заменяйте одновременно все батареи в конкретном датчике (используйте батареи одного типа и одного изготовителя).

:: Некоторые устройства могут требовать проведения проверки (например, пожарные датчики). Для получения дополнительной информации свяжитесь со своим техником по обслуживанию.

1. ВВЕДЕНИЕ

Количество пользователей системы JABLOTRON 100+ может доходить до 600, а количество разделов внутри системы – до 15. Система рассчитана на подключение максимум 230 устройств и включает до 128 многоцелевых программируемых выходов (например для домашней автоматизации).

2. ЭКСПЛУАТАЦИЯ СИСТЕМЫ JABLOTRON 100+

Управление охранной системой осуществляется несколькими способами. Для снятия системы с охраны всегда необходима обязательная авторизация в форме идентификации пользователя. Система проверяет личность пользователей и позволяет им управлять теми частями системы, которыми им разрешено управлять. Можно выбирать различные способы постановки на охрану – как с авторизацией, так и без нее. При использовании авторизации стандартного типа авторизация пользователя не требуется, поскольку систему можно поставить на охрану простым нажатием правой кнопки сегмента на клавиатуре. При каждом доступе к системе в памяти системы записываются имя пользователя, дата и время. Эта информация доступна неограниченное время. Любой пользователь может также отменить сработавшую сигнализацию (выключить звук сирен) простой авторизацией в любой части системы (в зависимости от своих прав доступа). Тем не менее, это не означает автоматическое снятие системы с охраны (если только не изменены стандартные настройки системы).

Замечание: В зависимости от конфигурации установки и настроек системы некоторые из описанных ниже опций могут отсутствовать. По вопросу конфигурации установки проконсультируйтесь со своим техником по обслуживанию.

Пользователи и их права доступа

КОД АВТОРИЗАЦИИ	ОПИСАНИЕ ТИПА
Код ПЦН	Этот код имеет высший уровень авторизации для настройки характеристик системы и предоставляется исключительно для разблокирования системы после срабатывания сигнализации. С его помощью можно входить в сервисный режим, получать доступ ко всем вкладкам с опциями, включая связь с ПЦН, в доступе к которой технику по обслуживанию может быть отказано (Сервисный код). Пока не установлена отметка в параметре «Администратор-ограниченное право сервиса/связи с ПЦН», код ПЦН может контролировать все разделы и PG выходы, используемые в системе. Этот код позволяет добавлять администраторов и других пользователей с более низким уровнем авторизации и присваивать им коды, RFID метки и карты. Он также дает разрешение стирать память сигналов тревоги и тамперных сигналов. Количество кодов ПЦН в системе ограничивается только оставшимся объемом памяти панели управления, коды ПЦН отсутствуют в стандартных заводских настройках.
Сервисный код (Сервис)	Этот код может вводить сервисный режим и настраивать характеристики системы. Он предоставляет доступ ко всем вкладкам с опциями, включая связь с ПЦН, если этот доступ не ограничен техником ПЦН. Пока не установлена отметка в параметре «Ограниченные администратором права сервиса/ ПЦН», сервисный код может управлять всеми разделами и PG выходами, использующимися в системе. Он позволяет создавать пользователей с разрешением связи с ПЦН, других техников по обслуживанию, администраторов и других пользователей с более низким уровнем авторизации и присваивать им коды доступа, RFID метки и карты. Он также дает разрешение стирать память сигналов тревоги и тамперных сигналов. Количество сервисных кодов ограничено только оставшимся объемом памяти панели управления. Стандартная заводская настройка – это код 1010. Сервисный пользователь всегда находится в позиции 0 в панели управления, и стереть его невозможно.
Код администратора (Главный)	Этот код всегда предоставляет полный доступ ко всем разделам и дает авторизацию управлять всеми PG выходами. Администратор может создать другого администратора и другие коды с более низким уровнем авторизации и присвоить им доступ к разделам и PG выходам, коды доступа, RFID метки и карты. Этот код дает разрешение стирать память сигналов тревоги. Может быть только один код главного администратора, который нельзя стереть. Если включен выбран параметр «Ограниченные администратором права сервиса/ ПЦН», код администратора должен быть авторизован для подтверждения доступа для ПЦН и техников по обслуживанию. Стандартная заводская настройка – это код 1234. Пользователь «Главный администратор» всегда находится на позиции 1, и его невозможно стереть.
Код администратора (Другой)	Этот код предоставляет доступ к разделам, выбранным главным администратором, к которым другой администратор может добавить новых пользователей с таким же или более низким уровнем авторизации для управления разделами и PG выходами, присвоения им кодов доступа, RFID меток и карт. Этот код имеет разрешение стирать память сигналов тревоги в назначенных разделах.

КОД АВТОРИЗАЦИИ	ОПИСАНИЕ ТИПА
	Если включен выбран параметр «Ограниченные администратором права сервиса/ПЦН», код администратора должен быть авторизован для подтверждения доступа для ПЦН и техников по обслуживанию. Количество кодов администратора (другого) ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код пользователя	Этот код дает доступ к разделам и права управления PG выходами, назначаемые администратором. Пользователи могут добавлять/удалять свои RFID метки и карты доступа и изменять свои номера телефона. Пользователи могут изменять свои коды при условии, что в системе используются коды с префиксами. Он дает разрешение стирать память сигналов тревоги в назначенных разделах. Выбранные пользователи могут иметь доступ к разделам, ограниченный расписанием. Количество кодов пользователя ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код постановки на охрану	Этот код позволяет ставить на охрану только определенный раздел и управлять (Вкл./Выкл.) только PG выходами, которые требуют авторизации. Пользователям с этим уровнем авторизации не разрешено изменять свой код и стирать память сигналов тревоги. Количество кодов постановки на охрану ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код «только выходы PG»	Это код позволяет пользователю управлять программируемыми выходами только с авторизацией. Это относится как к включению, так и к выключению. Пользователям с этим уровнем авторизации не разрешено изменять свой код и стирать память сигналов тревоги. Количество кодов «только выходы PG» ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код паники	Этим кодом можно запускать только сигнал паники. Пользователю с этим кодом не разрешено изменять его или стирать память сигналов тревоги. Количество кодов паники ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код охраны	Это код для охранного агентства. Этот уровень авторизации позволяет ставить на охрану всю систему. Однако, снять систему с охраны кодом охраны можно только во время срабатывания сигнализации или после истечения ее времени, пока по-прежнему активна память сигналов тревоги. Пользователю с этим кодом не разрешено изменять его или стирать память сигналов тревоги. Количество кодов охраны ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.
Код разблокирования	Этот код предназначен для разблокирования системы после того, как она была блокирована срабатыванием сигнализации. Пользователю с этим кодом не разрешено изменять его или стирать память сигналов тревоги. Количество кодов разблокирования ограничено только оставшимся объемом памяти панели управления. Этот код не имеет стандартной заводской настройки.

Защита кодов доступа, бесконтактных RFID устройств и средств удаленного управления:

Панель управления позволяет назначать каждому пользователю один 4-х, 6-ти или 8-мизначный код и до двух RFID меток для авторизации в системе. Авторизация пользователя требуется во время каждого действия с клавиатурой, голосовым меню, компьютером, сетевыми или мобильными приложениями. Длина кода влияет на количество возможных комбинаций и, следовательно, на защиту кода.

Количество кодовых комбинаций зависит от конфигурации:

Параметры панели управления	4 ЦИФРЫ	6 ЦИФР	8 ЦИФР
«Код с префиксом» включен	$= 10^4 = (10.000)$	$= 10^6 = (1.000.000)$	$= 10^8 = (100.000.000)$

Параметры панели управления	4 ЦИФРЫ	6 ЦИФР	8 ЦИФР
«Код с префиксом» и «Управление доступом в ситуации принуждения» оба отключены	= 10^4 – (Количество пользователей – 1)	= 10^6 – (Количество пользователей – 1)	= 10^8 – (Количество пользователей – 1)
«Код с префиксом» выключен; «Управление доступом в ситуации принуждения» включен	≤ 10^4 – ((Количество пользователей – 1) * 3)	≤ 10^6 – ((Количество пользователей – 1) * 3)	≤ 10^8 – ((Количество пользователей – 1) * 3)
Использование только RFID карты с диапазон из 14 символов (6 постоянных + 8 переменных)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)
«Код с префиксом» и «Подтверждение карты кодом» оба включены	= (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)
«Код с префиксом» выключен; «Подтверждение карты кодом» включен	= 10^8 * (10^4 – (Количество пользователей – 1))	= 10^8 * (10^6 – (Количество пользователей – 1))	= 10^8 * (10^8 – (Количество пользователей – 1))

Способы усиления защиты от подбора действительного кода:

:: Использование кода с большим количеством цифр (6-ти или 8-мизначные коды),
:: Авторизация усложненного типа, например «Подтверждение карты кодом» или «Двойная авторизация»).

Способы управления системой JABLOTRON 100+

Локально:

:: Системная клавиатура
:: Системный брелок
:: Компьютер с USB кабелем и программным обеспечением J-Link

Удаленно:

:: MyJABLOTRON – приложение для смартфонов
:: Компьютер с веб-интерфейсом MyJABLOTRON
:: Использование телефона с голосовым меню
:: Телефон – через SMS сообщения
:: Компьютер – через Интернет, с помощью программного обеспечения J-Link
:: Вызов с авторизованного телефонного номера (только для управления программируемыми выходами)

Система JABLOTRON 100+ может управляться различными модулями доступа, которые позволяют не только простой контроль, но и отображение состояний отдельных сегментов. Система может управляться напрямую (постановка на охрану и снятие с охраны, а также другие автоматические функции) при помощи сегментов клавиатуры с двумя кнопками. Кнопки сегментов имеют четкую маркировку и отличаются по цвету (используется алгоритм светофора), благодаря чему обеспечивается отчетливая индикация состояния каждого сегмента. Сегмент также можно использовать для индикации состояния (например открыта гаражная дверь) или для управления различными автоматическими приборами (например отоплением или оконными жалюзи). Максимальное количество сегментов для одного модуля доступа составляет 20 сегментов. Сегмент также можно настроить таким образом, чтобы он мог в экстренных случаях отправлять просьбу о помощи (например в случае проблем со здоровьем или паники).

2.1. ЛОКАЛЬНАЯ ЭКСПЛУАТАЦИЯ

- Непрерывно горит зеленым светом
  СНЯТО С ОХРАНЫ / ВЫКЛ.
- Мигает зеленым светом
  ЗАДЕРЖКА НА ВХОД
- Мигает красным светом
  СИГНАЛ ТРЕВОГИ / ПАМЯТЬ СИГНАЛОВ ТРЕВОГИ
- Непрерывно горит зеленым светом
  ВСЕ В ПОРЯДКЕ
- Мигает зеленым светом
  УПРАВЛЕНИЕ
- Мигает зеленым светом 2x по 2 с
  ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ
- Непрерывно горит желтым светом
  СБОЙ
- Мигает желтым цветом
  НЕУДАВШАЯСЯ ПОСТАНОВКА НА ОХРАНУ

- Непрерывно горит красным светом
  ПОСТАВЛЕНО НА ОХРАНУ / ВКЛ.
- Мигает красным светом
  СИГНАЛ ТРЕВОГИ / ПАМЯТЬ СИГНАЛОВ ТРЕВОГИ
- Непрерывно горит желтым светом
  ЧАСТИЧНО ПОСТАВЛЕНО НА ОХРАНУ
- КАРТРИДЕР / КЛАВИАТУРА

Типы модулей доступа и их сочетания:

RFID картридер

позволяет управлять системой при помощи сегментов и бесконтактной авторизации пользователя (RFID карта/метка).

Клавиатура с картридером

пользователь может управлять системой при помощи сегментов и авторизации, либо вводом кода, либо бесконтактного метода (RFID карта/ метка) или же сочетания их обоих для повышенной безопасности.

Клавиатура с ЖК-дисплеем и картридером

пользователь может управлять системой при помощи сегментов и авторизации с помощью кода, бесконтактного метода (RFID карта/метка), сочетания кода и карты/метки для повышения безопасности или путем авторизации и использования одной из опций, доступных на ЖК-дисплее клавиатуры.

При снятии сигнализации с охраны с помощью кнопок сегмента авторизация пользователя всегда обязательна. При постановке сигнализации на охрану и управлении автоматическими процессами при помощи кнопок сегментов авторизация пользователя не обязательна.

Пользователи могут авторизоваться путем ввода своих назначаемых кодов или с помощью своей карты/метки RFID. У каждого пользователя может быть один код и до двух чипов RFID (карт/меток).

Рекомендуемые бесконтактные чипы: JABLOTRON 100⁺, Oasis или другие чипы третьих изготовителей, совместимые со стандартом 125 кГц EM. Для повышения безопасности система сигнализации может быть настроена на использование авторизации с подтверждением с помощью RFID чипов и кодов (опция). При желании пользователя одновременно контролировать несколько сегментов он должен авторизоваться, а затем последовательно нажать сегменты конкретных разделов. Таким образом пользователь может, например, снимать с охраны дом или гараж посредством одной авторизации. Если включен параметр «Код с префиксом», то код авторизации с клавиатуры может состоять максимум из одиннадцати цифр: префикс (от одной до трех цифр), звездочка * (которая разделяет префикс и основной код) и 4-х, 6-ти или 8-мизначный код в соответствии с конфигурацией (например: 123*12345678 или 1*12345678). Все пользователи могут изменять свои собственные коды, которые следуют за префиксом. Код может быть изменен с клавиатуры с ЖК-дисплеем, посредством программы J-Link или приложения MyJABLOTRON.

Если параметр «Код с префиксом» включен, пользователям может разрешаться изменять свои коды.
Если параметр «Код с префиксом» выключен, коды могут изменяться только администратором.

2.1.2. АВТОРИЗАЦИЯ КОДА С КЛАВИАТУРЫ

Авторизация с кодом пользователя осуществляется набором действительного кода на клавиатуре или с помощью RFID метки.

В системе можно использовать 4-х, 6-ти или 8-мизначные коды.

Можно создать конфигурацию системы с использованием кодов с префиксом или без их использования (стандартная настройка). Для охранных систем с большим количеством пользователей префикс можно включить. Для изменения этой опции свяжитесь с техником по обслуживанию своей охранной системы.

Код без префикса: CCCC

cccc это код из 4, 6 или 8 цифр, допускаются коды от 0000 до 99999999

Код панели управления по умолчанию Администратор: 1234; 123456; 12345678;

Код без префикса: nnn*cccc

nnn — это префикс, который является номером позиции пользователя (от 0 до 600)

* — это разделитель (клавиша *)

cccc — это код из 4, 6 или 8 цифр, допускаются коды от 0000 до 99999999

Код панели управления по умолчанию — Администратор: 1*1234; 1*123456; 1*12345678;

ВНИМАНИЕ: Код главного администратора начинается с префикса 1

Главный Сервисный код начинается с префикса 0

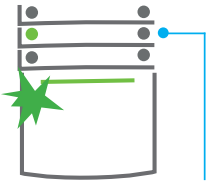
Для изменения типа кода свяжитесь с техником по обслуживанию своей охранной системы.

Структура и описание меню внутренней клавиатуры с ЖК-дисплеем.

2.1.2.1. ПОСТАНОВКА СИГНАЛИЗАЦИИ НА ОХРАНУ

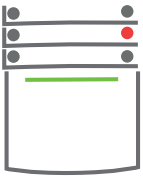
1. Авторизуйтесь с помощью клавиатуры. При этом загораются разделы, которыми можно управлять, а кнопка индикации с подсветкой начинает мигать зеленым светом.

2. Нажмите правую кнопку (одну из тех, которые не загорелись),



чтобы поставить на охрану конкретный раздел. На охрану можно последовательно поставить несколько разделов. Задержка между выбором разделов не должна быть дольше 2 секунд.

3. Команда будет выполнена, и клавиатура сообщит звуковым



сигналом о задержке для выхода. Теперь раздел поставлен на охрану, и только датчики с реагированием «Зона с задержкой» предоставляют время, за которое можно покинуть охраняемую зону во время задержки для выхода. Кнопка сегмента поставленного на охрану раздела загорается красным светом.

Если при постановке сигнализации на охрану срабатывает какой-либо датчик (например, открыто окно), система отреагирует одним из следующих способов (на основании от конфигурации системы):

:: После переключения датчиков режим ожидания они осуществляют охрану автоматически (стандартная настройка).

:: Система включает индикацию сработавших датчиков: сегмент мигает красным цветов в течение 8 секунд, и системы автоматически становится на охрану по истечении этого периода.

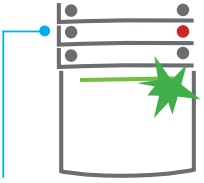
:: Раздел со сработавшими датчики можно также поставить на охрану повторным нажатием кнопки сегмента с правой стороны. Таким образом пользователь подтверждает намерение поставить на охрану раздел со сработавшим датчиком (например, открытое окно). В противном случае сработавший датчик будет препятствовать постановке раздела на охрану.

:: Сработавший датчик будет препятствовать постановке раздела на охрану. Это состояние указывается световой индикацией: кнопка сегмента мигает красным светом. Датчик, препятствующий постановке на охрану, будет показан в меню ЖК-дисплея клавиатуры.

Неудавшаяся постановка на охрану указывается индикацией кнопки, которая мигает желтым цветом (параметр «Неудавшаяся постановка на охрану» должен быть включен). По вопросу программирования необходимых характеристик установленной системы следует проконсультироваться с техником по обслуживанию.

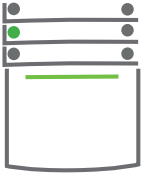
2.1.2.2. СНЯТИЕ СИГНАЛИЗАЦИИ С ОХРАНЫ

1. При входе в здание (сработает датчик с реагированием «Зона с задержкой»), система включает индикацию задержки для входа: непрерывный звуковой сигнал и мигание зеленым



светом кнопки сегмента раздела, в котором была сработала функция задержки для входа.

Авторизуйтесь с помощью клавиатуры, при этом начнет мигать зеленый индикатор панели авторизации.



2. Нажмите левую кнопку сегмента раздела, который необходимо снять с охраны.

3. Команда выполняется, и кнопки сегмента загораются зеленым светом, указывая на снятый с охраны раздел.

Обратите внимание: Если включен параметр «Снятие раздела с охраны только авторизацией во время задержки для входа», такой раздел, в котором задействована функция задержки для входа, будет сниматься с охраны простой авторизацией.

2.1.2.3. УПРАВЛЕНИЕ ДОСТУПОМ В СИТУАЦИИ ПРИНУЖДЕНИЯ

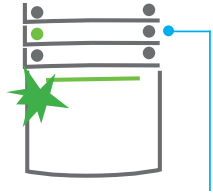
Эта функция обеспечивает снятие системы с охраны в специальном режиме. Создается впечатление, что система снимается с охраны, но включается беззвучный сигнал паники, который затем передается выбранным пользователям (включая ПЦН). Снятие с охраны в ситуации под принуждением выполняется добавлением 1 к последней цифре в действительном коде.

Пример кода с префиксом: Действительный код: 2*9999
Код для снятия с охраны под принуждением: 2*9990

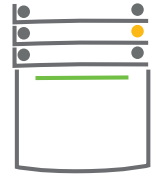
Пример кода без префикса: Действительный код: 9999
Код для снятия с охраны под принуждением: 9990

2.1.2.4. ЧАСТИЧНАЯ ПОСТАНОВКА СИГНАЛИЗАЦИИ НА ОХРАНУ

1. Авторизуйтесь с помощью клавиатуры (введите код или приложите карту или метку к считывающему устройству). Начнет мигать кнопка индикации с зеленой подсветкой.



2. Нажмите правую кнопку сегмента выбранного раздела.



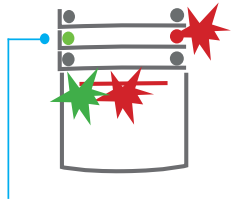
3. Команда выполняется, и кнопка сегмента начинает непрерывно гореть желтым светом, это индикация частичной постановки раздела на охрану.

Систему можно также сконфигурировать для частичной постановки на охрану, которая позволяет включать охрану только определенными датчикам в разделе. Пример: В ночное время можно поставить на охрану только датчики дверей и окон, а датчики движения внутри здания не будут реагировать на движение.

Чтобы поставить на охрану все помещения, в которых включена частичная постановка на охрану, необходимо дважды нажать кнопку постановки системы на охрану. При однократном нажатии кнопка мигает желтым светом, при повторном – мигает красным светом. Если система частично поставлена на охрану – непрерывно горит желтый свет, – то поставить на охрану всю систему можно авторизацией и нажатием желтой кнопки. После нажатия кнопки система будет полностью поставлена на охрану и кнопка загорится красным светом.

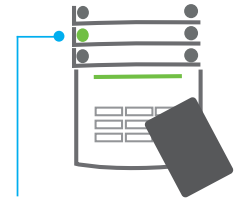
2.1.2.5. ОТМЕНА СРАБОТАВШЕЙ СИГНАЛИЗАЦИИ

1. Авторизуйтесь с помощью клавиатуры (введите код, приложите метку к считывающему устройству).



2. Нажмите левую кнопку сегмента раздела, в котором сработала сигнализация.

3. Завершается снятие с охраны, и сирены выключаются. Мигающая зеленым светом кнопка указывает на снятие с охраны конкретного раздела. Мигающий красный свет указывает на память сигналов тревоги.



4. Авторизуйтесь и снова нажмите зеленую кнопку для отмены индикации памяти сигналов тревоги.

5. Сегмент указывает на снятый с охраны раздел непрерывным горением зеленой кнопки.

На наличие активной сработавшей сигнализации указывает быстро мигающая красным светом кнопка сегмента и кнопка индикации с подсветкой. Для отмены сигнализации необходимо авторизоваться с помощью клавиатуры. Раздел остается под охраной, а быстро мигающая красным светом кнопка сегмента указывает на память сигналов тревоги. Индикация миганием будет продолжаться даже после снятия системы с охраны.

Если в ваше отсутствие была активирована индикация памяти сигналов тревоги, найдите причину срабатывания сигнализации в истории событий и будьте осторожны при входе и осмотре помещений или дождитесь прибытия сотрудников охранного агентства (при условии, что ваша система подключена к ПЦН).

Индикация памяти сигналов тревоги сегмента остается включенной до тех пор, пока система не будет снова поставлена на охрану. В качестве варианта эту индикацию можно отключить, еще раз сняв систему с охраны. Индикацию срабатывания сигнализации также можно отключить на клавиатуре с ЖК-дисплеем в главном меню – Отмена предупреждающей индикации.

Индикация сработавшей темперной сигнализации может быть отключена только техником по обслуживанию или администратором.

Обратите внимание: При использовании профиля системы «EN 50131-1, класс 2» всегда необходимо сначала авторизоваться, а затем выполнить необходимое действие.

При отключении сигнализации с помощью удаленного управления соответствующий раздел также будет снят с охраны.

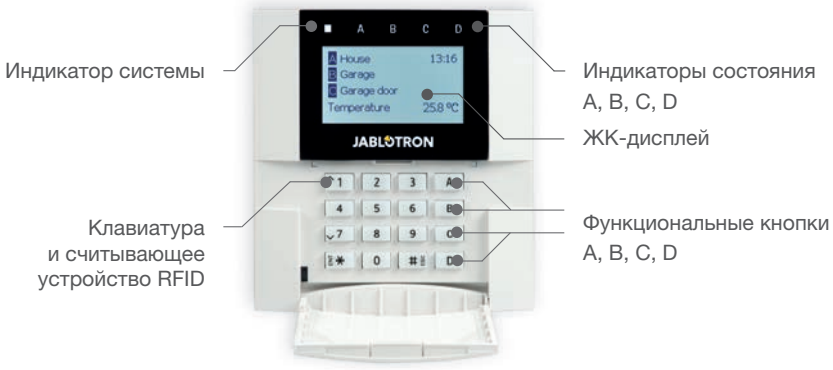
2.1.2.6. УПРАВЛЕНИЕ РАЗДЕЛАМИ ИЗ МЕНЮ КЛАВИАТУРЫ С ЖК-ДИСПЛЕЕМ

Состояние разделов отображаются в левой верхней части ЖК-дисплея клавиатуры. Полностью поставленный на охрану раздел обозначается номером в черном прямоугольнике 2, раздел с частичной постановкой на охрану обозначается номером в рамке 4.

Управление с помощью меню клавиатуры:

:: Авторизация с помощью действительного кода или RFID чипа.
:: Войдите в меню нажатием ENTER
:: Управление разделами → ENTER.
:: С помощью стрелок выберите необходимый раздел.
:: Повторными нажатиями клавиши ENTER изменяется состояние раздела: частичная постановка на охрану / постановка на охрану / снят с охраны.
:: Для выхода из меню нажмите клавишу ESC.

2.1.3. ИСПОЛЬЗОВАНИЕ СИСТЕМНЫХ КЛАВИАТУР JA-110E И JA-150E



Состояния отдельных разделов указываются индикаторами состояния A, B, C, D над ЖК-дисплеем и функциональными кнопками. Панель управления может управляться напрямую (постановка на охрану и снятие с охраны, а также другие автоматические функции) с помощью функциональных кнопок на клавиатуре. Функциональные кнопки и индикаторы состояния A, B, C, D имеют цветовую подсветку, чтобы четко различать состояние раздела.

:: ЗЕЛЕНЫЙ – Снят с охраны :: ЖЕЛТЫЙ – Частично снят с охраны :: КРАСНЫЙ – Поставлен на охрану

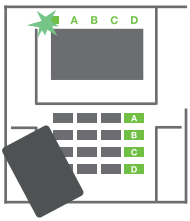
Авторизацию можно выполнить вводом кода доступа на клавиатуре или с помощью RFID карты/метки, назначенной конкретному пользователю. Каждый пользователь может иметь один код и один RFID чип (карту или метку). Если пользователям необходимо одновременно контролировать несколько разделов, они должны авторизоваться, а затем последовательно нажать функциональные кнопки конкретных разделов. Таким способом пользователи могут снимать с охраны все разделы (например дом и гараж) после одной авторизации.

Структура и описание меню внутренней клавиатуры с ЖК-дисплеем.

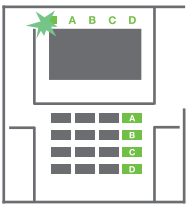
Авторизация администратора или авторизации пользователя по коду или с помощью RFID метки/карты

Отмена предупреждающей индикации	Позволяет отменять сигнал тревоги/индикацию неудавшейся постановки на охрану во всех разделах, в которые пользователь имеет право доступа.
Управление разделами	Позволяет пользователю управлять разделами системы, в которые у него есть право доступа и которые включены во внутренних настройках.
Управление PG	Позволяет пользователю управлять программируемыми выходами PG в зависимости от разрешений доступа пользователя и согласно внутренним настройкам.
Память событий	Отображает подробный перечень из памяти событий.
Постановка на охрану заблокирована	Показывает перечень сработавших датчиков, которые препятствуют постановке системы на охрану, при условии, что эта опция активирована в конфигурации панели управления.
Сбой в системе	Отображает перечень датчиков, указывающих на сбои системы из разделов, в которые у пользователя есть право доступа.
Обход датчиков	Отображает перечень блокированных датчиков в разделах, в которые у пользователя есть право доступа.
Состояние системы	Показывает состояние системы (перечень сработавших датчиков, сработавших тамперных контактов, низкий заряд батареи, обход датчиков и т.д.).
Настройки	Позволяет редактировать пользователей и устройства (только при отключенном USB выходе).
Настройки дисплея	Позволяет регулировать яркость подсветки и контрастность дисплея клавиатуры.
Режим обслуживания	Позволяет администратору переключать назначенные разделы в режим технического обслуживания

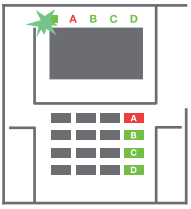
2.1.3.1. ПОСТАНОВКА СИГНАЛИЗАЦИИ НА ОХРАНУ



1. Авторизуйтесь с помощью клавиатуры. При этом загорятся функциональные кнопки A, B, C, D разделов, которыми вам разрешено управлять, а индикатор системы начнет мигать зеленым светом.
2. Нажмите функциональную кнопку, чтобы поставить на охрану конкретный



раздел. На охрану можно последовательно поставить несколько разделов. Задержка между выбором разделов не должна быть дольше 2 секунд.
3. Команда будет выполнена, и клавиатура сообщит звуковым сигналом о задержке для выхода. Теперь раздел поставлен



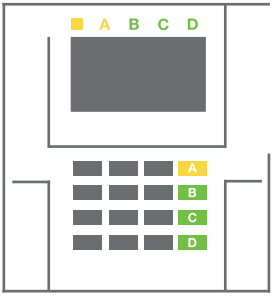
на охрану, и только датчики с реагированием «Зона с задержкой» предоставляют время для выхода из охраняемой зоны во время задержки для выхода. Индикатор состояния и функциональная кнопка поставленного на охрану раздела загорятся красным светом.

Если при постановке сигнализации на охрану срабатывает какой-либо датчик (например, открытое окно), система реагирует одним из следующих способов (на основании конфигурации системы):

:: Панель управления выполнит постановку на охрану самостоятельно. Сработавшие датчики будут автоматически заблокированы. *)
:: Система световой индикацией укажет сработавшие датчики: функциональная кнопка будет мигать красным светом 8 секунд, а по истечении этого периода панель управления автоматически выполнит постановку на охрану (сработавшие датчики будут заблокированы). *)
:: Раздел со сработавшими датчиками можно также поставить на охрану повторным нажатием функциональной кнопки. Пользователь должен подтвердить свое намерение поставить на охрану раздел со сработавшим датчиком (например, открытое окно). В противном случае постановка системы на охрану не осуществляется.
:: Сработавший датчик будет препятствовать постановке раздела на охрану. Это состояние указывается световой индикацией: мигающей красным светом функциональной кнопкой. Датчик, препятствующий постановке на охрану, будет показан в меню на ЖК-дисплее.

*) ВНИМАНИЕ: Варианты a) и b) не поддерживаются профилем EN 50131, класс 2 (выбранный профиль системы панели управления)

При срабатывании датчика в режиме «Мгновенная тревога в зоне» во время задержки для выхода или датчика в режиме «Тревога в зоне с задержкой» состояние реагирования не изменяется по истечении времени задержки для выхода, затем панель управления выполнит снятие с охраны. На неудавшуюся постановку на охрану будет указывать мигающий желтым светом индикатор системы, с отправлением сообщения на пульт ПЦН и звуковой индикацией внешней сирены (применяется к классу безопасности 2).

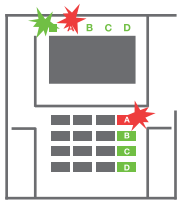


Если панель управления сконфигурирована для постановки на охрану без авторизации, то авторизоваться нет необходимости. Все, что необходимо сделать, – это нажать функциональную кнопку конкретного раздела. Панель управления также можно сконфигурировать для постановки на охрану просто авторизацией.

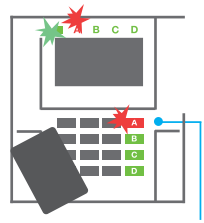
ВНИМАНИЕ: Постановка на охрану без авторизации автоматически снижает максимальный уровень безопасности до класса 1. Следует учесть все возможные риски, связанные с использованием этой функции.

Вопросы программирования необходимых характеристик системы сигнализации следует обсудить с консультантом проекта или техником по обслуживанию.

2.1.3.2. СНЯТИЕ СИГНАЛИЗАЦИИ С ОХРАНЫ

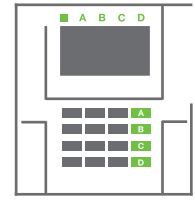


1. При входе в здание (срабатывает датчик с реагированием «Зона с задержкой») система включает индикацию задержки для входа непрерывным звуковым сигналом и миганием красным светом индикатора системы и функциональной



кнопки раздела, в котором задействована функция задержки для входа.

2. Авторизуйтесь с помощью клавиатуры, чтобы индикатор системы начал мигать зеленым светом.



3. Нажмите функциональные кнопки для разделов, которые необходимо снять с охраны.

4. Команда выполнена. Функциональные кнопки и индикатор системы начинают гореть зеленым светом, указывая на снятые с охраны разделы.

Обратите внимание: При включении параметра «Снятие раздела с охраны только авторизацией во время задержки для входа» раздел, в котором задействована функция задержки для входа, будет сниматься с охраны простой авторизацией. В случае нескольких разделов этой опцией следует пользоваться с осторожностью.

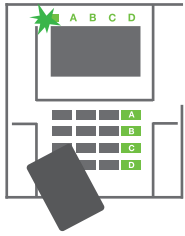
По вопросу программирования необходимых характеристик установленной системы следует проконсультироваться с техником по обслуживанию.

2.1.3.3. ЧАСТИЧНАЯ ПОСТАНОВКА СИГНАЛИЗАЦИИ НА ОХРАНУ

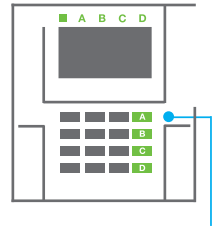
ВНИМАНИЕ: Это дополнительная функция системы сигнализации.

Систему можно также сконфигурировать для частичной постановки на охрану, которая позволяет включать охрану только определенными датчикам в разделе.

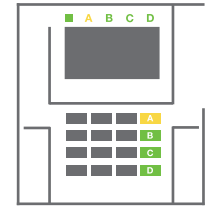
Пример: В ночное время на охрану можно поставить только датчики двери и окон, во время как выбранные датчики движения не будут включать сигнализацию, если кто-то двигается внутри раздела.



1. Авторизуйтесь с помощью клавиатуры (введите код или приложите RFID карту или метку к считывающему устройству). Кнопка индикатора системы начнет мигать зеленым светом.



2. Нажмите функциональную кнопку выбранного раздела.



3. Команда выполняется, и функциональная кнопка начинает непрерывно гореть желтым светом, указывая на частичную постановку раздела на охрану.

Чтобы целиком поставить на охрану помещения, в которых включена функция частичной постановки на охрану, в течение 2 секунд удерживайте нажатой кнопку постановки на охрану панели управления или дважды нажмите эту кнопку. После первого нажатия кнопки она начинает непрерывно гореть желтым светом, а после второго нажатия – непрерывно красным светом.

Если система уже частично поставлена на охрану, на что указывает непрерывное горение желтым светом функциональной кнопки, то авторизацией и более длительным нажатием желтой кнопки можно поставить на охрану всю систему. После нажатия кнопки система будет полностью поставлена на охрану и кнопка загорится красным светом.

Частичную постановку на охрану можно также сконфигурировать так, чтобы авторизация не требовалась.

Чтобы снять панель управления с охраны при ее частичной постановке на охрану, нажмите желтую кнопку. Панель управления будет снята с охраны, и кнопка загорится зеленым светом.

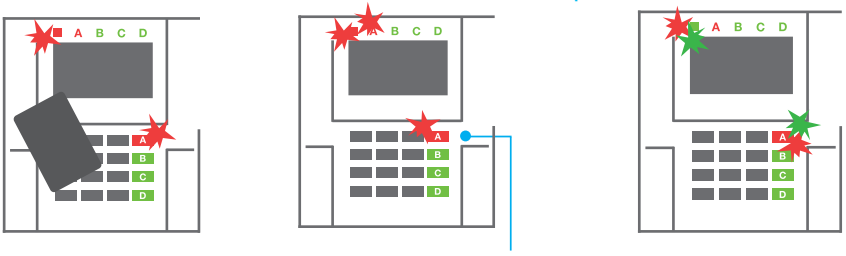
2.1.3.4. УПРАВЛЕНИЕ ДОСТУПОМ В СИТУАЦИИ ПРИНУЖДЕНИЯ

Обеспечивает снятие с охраны панели управления в специальном режиме. Создается впечатление, что система снимается с охраны, однако включается беззвучный сигнал паники, который затем передается выбранным пользователям (включая ПЦН).

Снятие с охраны в ситуации под принуждением выполняется добавлением 1 к последней цифре в действительном коде. Если вам необходимо использовать эту функцию, обратитесь к своему технику по обслуживанию.

Пример: Действительный код: 9999 Код для снятия с охраны под принуждением: 9990

2.1.3.5. ОТМЕНА СРАБОТАВШЕЙ СИГНАЛИЗАЦИИ



1. Авторизуйтесь с помощью клавиатуры (введите код или приложите метку к считывающему устройству).

2. Нажмите функциональную кнопку раздела, в котором сработала сигнализация.

3. Завершается снятие с охраны, и сирены выключаются. Быстро мигающие попеременным цветом (зеленым/красным) функциональные кнопки и индикаторы состояния – это индикация памяти сигналов тревоги.

Индикатор состояния и быстро мигающая красным светом функциональная кнопка – это индикация продолжающегося сигнала тревоги сработавшей сигнализации. Для отмены сигнализации необходимо авторизоваться с помощью клавиатуры. Раздел остается под охраной, а быстро мигающая красным светом функциональная кнопка указывает на память сигналов тревоги. Индикация миганием будет продолжаться даже после снятия системы с охраны.

ВНИМАНИЕ: Если индикация памяти сигналов тревоги была активирована в ваше отсутствие, обязательно входите в здание с осторожностью, найдите причину срабатывания сигнализации в истории событий и будьте очень осторожны при осмотре помещений или дождитесь прибытия сотрудников охранного агентства (если ваша система подключена к пульту централизованного наблюдения).

Индикация памяти сигналов тревоги остается включенной до тех пор, пока система не будет снова поставлена на охрану. Выборочно ее можно также отменить из меню клавиатуры. Главное меню - Отмена предупреждающей индикации. Индикация сработавшей тамперной сигнализации может быть отключена только техником по обслуживанию и администратором.

Обратите внимание: При использовании «Стандартного» профиля системы можно сначала выбрать конкретное действие нажатием функциональной кнопки, а затем подтвердить его авторизацией с помощью клавиатуры.

2.1.3.6. ЭКСПЛУАТАЦИЯ СИСТЕМЫ ПРИ ПОМОЩИ БРЕЛКА

Брелки должны быть зарегистрированы в системе установщиком. Брелок может быть связан с конкретными пользователями, благодаря чему пользователь, взаимодействующий с системой в данный момент, не будет получать текстовые уведомления в сообщениях SMS (если параметры уведомлений настроены подобным образом). Брелки контролируют и показывают уровень зарядки батареи и используют световую индикацию и звуковые сигналы.

БРЕЛОК ДВУХСТОРОННЕЙ СВЯЗИ

Функции кнопок поясняются значками с замком. Значок с запертым замком означает постановку запрограммированных разделов на охрану; значок с отпертым замком снимает их с охраны. Правильное выполнение команды подтверждается включением индикатора: снятие с охраны – зеленый; постановка на охрану – красный. Индикация сбоя связи (выход из зоны действия панель управления) – это однократное мигание желтого светодиода. Кнопками с символами закрашенного и незакрашенного кругов можно управлять другим разделом. Кнопки брелка могут быть также настроены на управление PG выходами в различных режимах: первая кнопка включает/ вторая – выключает, и каждая кнопка может иметь отдельную функцию, когда используются импульсные функции или функция изменения. Для выполнение большего количества функций можно одновременно нажимать две кнопки. Таким образом, 4-кнопочный брелок может иметь до 6 отдельных функций или один PG выход состояния (например включение и выключение освещения), или, как вариант, – два выхода PG (например гаражная дверь и дверной замок).

Если система настроена на постановку на охрану после подтверждения, то датчик будет указывать на неудавшуюся постановку на охрану горящим зеленым светодиодом, если устройство сработало. Постановку на охрану необходимо подтвердить, снова нажав кнопку с замком. Постановка раздела на охрану будет подтверждена включением красного светодиода.

Кнопки брелка можно заблокировать во избежание случайного нажатия. Команда будет отправлена при повторном нажатии кнопки. Низкий заряд батареи указывается звуковым сигналом (3 сигнала) и световой индикацией: миганием желтого светодиода после нажатия кнопки.

Более подробную информацию о конфигурации удаленного управления можно получить у техника по обслуживанию.

БРЕЛКИ С ОДНОСТОРОННЕЙ СВЯЗЬЮ

Брелки с односторонней связью передают сигнал при каждом нажатии кнопки без обратной связи с панелью управления. Передача сигнала подтверждается только кратковременным включением красного светодиода и, в качестве варианта, – звуковым сигналом.

2.2. ДИСТАНЦИОННОЕ ИСПОЛЬЗОВАНИЕ

Максимальный комфорт при удаленном использовании и управлении системой обеспечивается сервисом MyJABLOTRON. Веб-интерфейс MyJABLOTRON – это сервис, предоставляющий онлайн-доступ к устройствам системы JABLOTRON. Он дает конечным пользователям возможность контроля и управления системой. Он реализован в форме приложения для смартфона и Интернет-приложения. Сервис MyJABLOTRON позволяет пользователям выполнять следующие действия:

:: Просмотр текущего состояния системы,
:: Постановка на охрану/снятие с охраны всей системы или ее части,
:: Управление программируемыми выходами,
:: Просмотр памяти событий,
:: Отправка отчетов выбранным пользователям через SMS сообщения, электронную почту и PUSH-уведомления.
:: Захват изображений от устройств фотографического подтверждения и их просмотр на вкладке галереи фотографий или непосредственно в памяти последних событий,
:: Контроль текущей температуры и потребления электроэнергии, включая обзор истории по графическим диаграммам,
:: И другие полезные функции.

В зависимости от страны или региона учетная записи в веб-сервисе MyJABLOTRON может быть создана авторизованным партнером компании JABLOTRON. Именем для входа в систему при этом служит адрес электронной почты пользователя. Пароль для первого входа в систему будет отправлен по этому адресу. Пароль может быть изменен в настройках пользователя в любое время.

2.2.1. ИСПОЛЬЗОВАНИЕ СИСТЕМЫ С ПОМОЩЬЮ ПРИЛОЖЕНИЯ ДЛЯ СМАРТФОНОВ MyJABLOTRON

После создания учетной записи пользователя пользователь может удаленно осуществлять контроль и управление системой через приложение MyJABLOTRON для смартфонов Android и iOS.

2.2.2. УПРАВЛЕНИЕ СИСТЕМОЙ ПОСРЕДСТВОМ ВЕБ-ИНТЕРФЕЙСА MyJABLOTRON

Системой JABLOTRON 100+ можно легко и удобно управлять с помощью подключенного к Интернету компьютера и веб-интерфейса MyJABLOTRON, вход в который осуществляется на сайте www.myjablotron.com.

2.2.3. УПРАВЛЕНИЕ СИСТЕМОЙ С ПОМОЩЬЮ ГОЛОСОВОГО МЕНЮ

Системой также можно управлять с телефона с помощью голосового меню, которое проводит пользователя через последовательность вариантов опций на предварительно заданном языке. Для доступа к голосовому меню необходимо просто набрать номер телефона системы сигнализации.

Доступ к голосовому меню можно включить либо для всех телефонных номеров без ограничений, либо выбрать вариант, при котором только доступ имеют только авторизованные телефонные номера, хранящиеся в панели управления. В зависимости от конфигурации может быть необходимо пройти авторизацию путем ввода действительного кода на клавиатуре телефона. При входе пользователя в меню система обновляет текущее состояние всех разделов, назначенных пользователю. После этого звонящий может управлять этими разделами, либо по отдельности, либо совместно, с помощью клавиатуры своего телефона и доступных опций меню.

Стандартная настройка системы такова, что ответ на входящий вызов происходит трех гудков (что составляет примерно 15 секунд).

2.2.4. УПРАВЛЕНИЕ СИСТЕМОЙ С ПОМОЩЬЮ КОМАНД В SMS

SMS командами можно управлять отдельными разделами и программируемыми выходами, аналогично тому, как это делается кнопками сегментов клавиатуры. Форма текстового сообщения для управления системой следующая: CODE_КОМАНДА. Команды, выполняющие действие, заранее заданы в системе (SET – поставить на охрану/ UNSET – снять с охраны) и имеют дополнительным числовой параметр, который указывает конкретный раздел. Одним сообщением SMS можно одновременно управлять несколькими разделами. В этом случае цифры, добавленные к команде, определяют разделы.

Пример команды SMS, которая используется для постановки на охрану разделов 2 и 4:

CODE_SET_2_4

Команды для управления программируемыми выходами могут быть запрограммированы установщиком системы. Например, в качестве команды на опускание жалюзи на окнах можно задать команду BLINDS DOWN (опустить жалюзи). Систему можно также настроить так, чтобы она не требовала кода перед командой. В этом случае команда просто автоматически идентифицируется, когда система распознает номер телефона пользователя, с которого было отправлено сообщение SMS. Конфигурация выполняется техником по обслуживанию.

2.2.5. УДАЛЕННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ С ПОМОЩЬЮ КОМПЬЮТЕРА (ПРОГРАММА J-LINK)

Система JABLOTRON 100+ может использоваться удаленно, с помощью компьютера с установленным программным обеспечением J-Link.
Ее можно скачать из раздела «Загрузки» на сайте www.myjablotron.com.

2.2.6. УПРАВЛЕНИЕ ПРОГРАММИРУЕМЫМИ ВЫХОДАМИ (PG)

2.2.6.1. СЕГМЕНТ КЛАВИАТУРЫ

PG выход включается нажатием правой кнопки сегмента и выключается левой кнопки. Если выход имеет конфигурацию импульсного выхода, он выключается в соответствии с заданным временем. Управление PG выходами может сохраняться или не сохраняться в памяти событий панели управления. Конфигурация выполняется техником по обслуживанию.

На основании конфигурации системы авторизация требуется или не требуется.

2.2.6.2. АВТОРИЗАЦИЯ ПОЛЬЗОВАТЕЛЯ С КЛАВИАТУРЫ

Активировать PG выход можно простой авторизацией пользователя (вводом кода или с помощью RFID метки). PG выход должен быть конфигурирован на активацию с определенной клавиатуры.

2.2.6.3. ИЗ МЕНЮ КЛАВИАТУРЫ С ЖК-ДИСПЛЕЕМ

После авторизации пользователя программируемые выходы могут управляться из меню клавиатуры с ЖК-дисплеем. У пользователя имеется доступ к программируемым выходам в зависимости от разрешений доступа пользователя.

Управление с помощью меню клавиатуры:

:: Авторизация с помощью действительного кода или RFID чипа.
:: Войдите в меню нажатием ENTER
:: Управление PG → ENTER.
:: Выберите необходимую группу выходов PG с помощью стрелок (1–32), (33–64), (65–96), (97–128) → ENTER.
:: Выберите необходимый выход PG с помощью стрелок → ENTER.
:: При повторных нажатиях ENTER состояние выходов PG будет меняться (у активного выхода PG номер выхода PG выдается на дисплей в прямоугольнике черного цвета.
:: Для выхода из меню нажмите клавишу ESC.

2.2.6.4. УДАЛЕННОЕ УПРАВЛЕНИЕ

Нажатием назначенной кнопки на устройстве удаленного управления. Устройства удаленного управления с двухсторонней связью подтверждают активацию PG выходов светодиодным индикатором.

2.2.6.5. ПРИЛОЖЕНИЕ ДЛЯ СМАРТФОНОВ MyJABLOTRON

Касанием элемента ВКЛ/ВЫКЛ на вкладке «Автоматика (PG)».

2.2.6.6. ВЕБ-ИНТЕРФЕЙС MyJABLOTRON

Щелкнув на элементе ВКЛ/ВЫКЛ на вкладке «Автоматика (PG)».

2.2.6.7. ДОЗВОН

Система может управляться каждым хранящимся в ней телефонным номером (один пользователь может иметь один телефонный номер) простым дозвоном (т.е. без установления соединения). Дозвон предполагает, что телефонный номер набирается SIM-карты охранной системы, после чего трубка вешается до того, как система успеет ответить на звонок. По умолчанию система ответит на вызов после третьего звонка (примерно 15 секунд).

2.2.6.8. СООБЩЕНИЕ SMS

Конкретный PG выход можно включить/выключить отправкой SMS сообщения. На основании конфигурации системы авторизация требуется или не требуется.

Пример: CODE_CONFIGURED TEXT

3. БЛОКИРОВАНИЕ/ОТКЛЮЧЕНИЕ СИСТЕМЫ

3.1. БЛОКИРОВКА ПОЛЬЗОВАТЕЛЕЙ

Можно временно заблокировать любого пользователя (например, в случае утери им карты/метки или в случае разглашения его кода доступа). Если доступ пользователя заблокирован, система перестает распознавать его идентификационный код или карту/метку. Эти пользователи также не будут получать на свои телефоны предупредительных сигналов по SMS и голосовых оповещений.

Только системный администратор или техник по обслуживанию может блокировать пользователей. Один из способов отозвать права доступа состоит в выборе «Настройки» / «Пользователи» / «Пользователь» / «Обход» с последующим нажатием кнопки «Да» на клавиатуре с ЖК-дисплеем. Другой вариант состоит в локальной или удаленной блокировке пользователя с помощью программы J-Link, щелкнув на имени пользователя в столбце «Настройки» / «Пользователи» / «Блокировка пользователя».

Заблокированный (выключенный) пользователь отмечается красным кружком, пока блокировка не будет отменена.

3.2. БЛОКИРОВАНИЕ ДАТЧИКОВ

Временная блокировка датчика происходит аналогично выключению пользователя. Датчик блокируется, если его срабатывание временно нежелательно (например, выключить датчик движения в помещении, в котором находится животное, или сигнал сирены). Система по-прежнему выполняет диагностику темперных контактов и передает сообщения о сервисных событиях, но при функция сигнализации выключена.

Только системный администратор или техник по обслуживанию может блокировать датчик. Это можно сделать выбором «Настройки» / «Устройства» / «Обход» и нажатием «Да» на клавиатуре с ЖК-экраном. Другой вариант – использовать программу J-Link и щелкнуть на датчике в столбце «Настройки» / «Диагностика» / «Выключен». Блокированный датчик отмечается желтым кружком, пока он не будет включен с помощью такой же процедуры. Устройство можно также заблокировать из приложения для смартфонов MyJABLOTRON.

3.3. ВЫКЛЮЧЕНИЕ ТАЙМЕРОВ

Если необходимо временно выключить автоматическое осуществление запланированных событий системы, можно выключить таймер. Отмена запланированного события (например, снятие системы с охраны утром в заданное время) отменяет выполнение этого события (например, во время отпуска).

Таймер может быть выключен локально или удаленно с помощью программы J-Link щелчком на разделе в столбце «Настройки» / «Календарь» / «Блокировано». Выключенный таймер отмечается красным кружком, пока он не будет снова включен с помощью такой же процедуры.

4. НАСТРОЙКА СИСТЕМЫ

4.1. ИЗМЕНЕНИЕ КОДА ДОСТУПА ПОЛЬЗОВАТЕЛЯ

Если система настроена без использования кодов с префиксами, то только системный администратор и техник по обслуживанию могут изменить защитные коды. Системный администратор может вносить изменения в меню на ЖК-дисплее клавиатуры, в программе J-Link, а также приложении для смартфонов MyJABLOTRON. Код может быть изменен после авторизации выбором параметров «Настройки» / «Пользователи» / «Пользователь» / «Код». Для ввода нового кода необходимо нажатием кнопки ENTER войти в режим редактирования (код начнет мигать), ввести новый код и подтвердить его повторным нажатием кнопки ENTER. По завершении внесения изменений их необходимо подтвердить выбором опции «Сохранить» после запроса системы на сохранение настроек «Сохранить настройки?».

Если система настроена на использование кодов с префиксом, отдельным пользователям может быть разрешено изменять свои коды в меню на ЖК-дисплее клавиатуры.

4.2. ИЗМЕНЕНИЕ, УДАЛЕНИЕ ИЛИ ДОБАВЛЕНИЕ RFID КАРТЫ / МЕТКИ

Если система настроена без использования кодов с префиксами, то только системный администратор и техник по обслуживанию могут изменить защитные коды. Системный администратор может вносить изменения в меню на ЖК-дисплее клавиатуры, в программе J-Link, а также приложении для смартфонов MyJABLOTRON. Код может быть изменен после авторизации выбором параметров «Настройки» / «Пользователи» / «Пользователь» / «Код». Для ввода нового кода необходимо нажатием кнопки ENTER войти в режим редактирования (код начнет мигать), ввести новый код и подтвердить его повторным нажатием кнопки ENTER. По завершении внесения изменений их необходимо подтвердить выбором опции «Сохранить» после запроса системы на сохранение настроек «Сохранить настройки?».

Если система настроена на использование кодов с префиксом, отдельным пользователям может быть разрешено изменять свои коды в меню на ЖК-дисплее клавиатуры.

4.3. ИЗМЕНЕНИЕ ИМЕНИ ПОЛЬЗОВАТЕЛЯ ИЛИ ТЕЛЕФОННОГО НОМЕРА

Если система настроена на использование кодов с префиксом, пользователи могут добавлять, изменять или удалять свои телефонные номера или изменять свои имена в меню на ЖК--дисплее клавиатуры. Это можно сделать после авторизации выбором параметров «Настройки» / «Пользователи» / «Пользователь» / «Телефон». Для внесения изменений пользователь должен находиться в режиме редактирования. Для этого необходимо нажать ENTER. После внесения изменений их необходимо подтвердить повторным нажатием кнопки ENTER. Чтобы удалить телефонный номер, введите «0» в поле телефонного номера. По завершении изменений их необходимо сохранить, выбрав опцию «Сохранить», когда система выдает запрос на сохранение настроек «Сохранить настройки?».

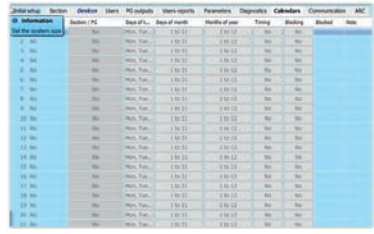
Системный администратор и техник по обслуживанию могут добавить, изменить или удалить телефонный номер пользователя или изменить имя пользователя как в меню на ЖК-дисплее клавиатуры, так и с помощью программы J-Link.

4.4. ДОБАВЛЕНИЕ / УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ

Только системный администратор или техник по обслуживанию могут добавлять в систему новых пользователей (или удалять их). Новые пользователи могут быть добавлены в систему (или удалены из нее) только с помощью программы J-Link или программы F-Link в случае техника по обслуживанию.

При создании нового пользователя ему необходимо присвоить разрешения (права) доступа, разделы, которыми он может использовать, программируемые выходы, которыми он может управлять, а также определить необходимый тип авторизации.

4.5. НАСТРОЙКА КАЛЕНДАРНЫХ СОБЫТИЙ



Имеется возможность конфигурировать календарные события (снятие с охраны / постановка на охрану / частичная постановка на охрану, управление или блокировка PG выходов). Календарные события могут задаваться с помощью программы J-Link на вкладке «Календарь».

Для каждого календарного события можно задать действия, раздел или PG выход и время события. День можно задать как день недели, месяца или года. Для выбранного дня можно задать действие, выполняющееся до 4 раз, или задать его повторение через равные промежутки времени.

Поэтому календарные события могут настраиваться не только для управления разделами, но также и для управления различными технологиями в объекте, использующем PG выходы.

5. ИСТОРИЯ СОБЫТИЙ

На специальной карте памяти формата micro SD, установленной в панели управления системы, охранная система сохраняет все выполненные действия и события (постановка на охрану, снятие с охраны,

сигналы тревоги, сбои, сообщения, отправленные пользователям и на ПЦН). Каждая запись включает дату, время (начало и окончание события), а также источник (причину / исходную точку) события.

Историю событий в системе можно просматривать разными способами:

5.1. ПОМОЩЬЮ КЛАВИАТУРЫ С ЖК-ДИСПЛЕЕМ

Для доступа к истории событий с помощью клавиатуры необходима авторизация пользователя. После авторизации отображаются доступные опции (на основе разрешений пользователя) при выборе параметра «Память событий». Записи можно просматривать с помощью стрелок.

5.2. С ПОМОЩЬЮ ПРОГРАММЫ J-LINK И КОМПЬЮТЕРА

Память системы можно просматривать с помощью программы J-Link. События можно загружать из панели управления небольшими (до 1 200 событий) или большими (около 4 000 событий) пакетами. События можно фильтровать по признакам, маркировать цветом для облегчения ориентации или сохранять в файлы на компьютере.

5.3. ВХОД В СИСТЕМУ MyJABLOTRON (ВЕБ-ИНТЕРФЕЙС/СМАРТФОН)

Все события в системе можно просматривать после входа в систему в веб-интерфейсе/в приложении для смартфонов MyJABLOTRON. Учетная запись показывает историю в диапазоне, соответствующем разрешениям пользователя.

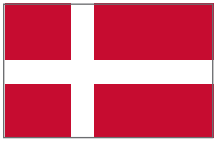
6. ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ

<table>
<tr><th>ПАРАМЕТР</th><th colspan="2">JA-103K</th><th colspan="2">JA-107K</th></tr>
<tr><td>Источник питания панели управления</td><td colspan="2">~ 110–230 вольт / 50–60 Гц, макс. 0.28 A с предохранителем F1,6 A/250 вольт Класс защиты II</td><td colspan="2">~ 110–230 вольт / 50–60 Гц, макс. 0.85 A с предохранителем F1,6 A/250 вольт Класс защиты II</td></tr>
<tr><td>Аккумулятор резервного питания</td><td colspan="2">12 В; 2,6 Ач (свинцово-кислотный, гелевый)</td><td colspan="2">12 В; от 7 до 18 Ач (свинцово-кислотный, гелевый)</td></tr>
<tr><td>Максимальное время заряда аккумулятора</td><td colspan="4">72 ч.</td></tr>
<tr><td>Напряжение на шине (красный - черный)</td><td colspan="4">от 12,0 до 13,8 вольт</td></tr>
<tr><td>Максимальный длительный потребляемый ток панели управления</td><td colspan="2">1000 мА</td><td colspan="2">2000 мА постоянный
3000 мА в течение 60 минут
(макс. 2000 мА на одну шину)</td></tr>
<tr><td rowspan="2">Макс. длительный потребляемый ток для резервного питания 12 часов</td><td rowspan="2">Без коммуникатора GSM</td><td rowspan="2">ЛОКАЛЬНАЯ СЕТЬ – ВЫКЛЮЧЕНА
115 мА
ЛОКАЛЬНАЯ СЕТЬ – ВКЛЮЧЕНА
88 мА</td><td colspan="2">Действительно для аккумуляторов резервного питания 18 Ач</td></tr>
<tr><td>Без коммуникатора GSM</td><td>ЛОКАЛЬНАЯ СЕТЬ – ВЫКЛЮЧЕНА
1135 мА
ЛОКАЛЬНАЯ СЕТЬ – ВКЛЮЧЕНА
1107 мА</td></tr>
</table>

ПАРАМЕТР	JA-103K		JA-107K	
	С коммуникатором GSM	ЛОКАЛЬНАЯ СЕТЬ – ВЫКЛЮЧЕНА 80 мА ЛОКАЛЬНАЯ СЕТЬ – ВКЛЮЧЕНА 53 мА	С коммуникатором GSM	ЛОКАЛЬНАЯ СЕТЬ – ВЫКЛЮЧЕНА 1100 мА ЛОКАЛЬНАЯ СЕТЬ – ВКЛЮЧЕНА 1072 мА
Максимальное количество устройств	50		230	
Устройство связи по локальной сети	ИНТЕРФЕЙС ETHERNET, 10/100BASE-T			
Габариты	268 x 225 x 83 мм		357 x 297 x 105 мм	
Управление с АКБ/без АКБ	1844 g/970 г		7027 g/1809 г	
Реагирование на ввод недействительного кода	Сигнал тревоги после 10 вводов неверного кода			
Память событий	Примерно 7 миллионов последних событий, включая дату и время			
Блок питания	Тип A (в соответствии с EN 50131-6)			
Коммуникатор GSM (2G)	850 / 900 / 1800 / 1900 МГц			
Классификация	Класс безопасности 2 / Категория размещения II (согласно EN 50131-1)			
Условия эксплуатации	Общие условия в помещении			
Диапазон рабочих температур	-от -10°C до +40°C			
Средняя рабочая влажность	75 % относительной влажности, без конденсации			
Соответствует	EN 50131-1 ред. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 ред. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN 50581			
Рабочая радиочастота (с модулем JA-11xR)	868,1 МГц, протокол JABLOTRON			
Радиоизлучение	ETSI EN 300 220-1,-2 (модуль R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)			
ЭМС	EN 50130-4 ред. 2+A1, EN 55032 ред. 2, ETSI EN 301 489-7			
Соответствие требованиям безопасности	EN 62368-1+A11			
Рабочие эксплуатации	ERC REC 70-03			
Орган сертификации	Trezor Test s.r.o. (no. 3025)			
Определение номера вызывающего абонента (CLIP)	ETSI EN 300 089			

JABLOTRON ALARMS a.s. настоящим заявляет, что панели управления JA-103K и JA-107K соответствуют следующим нормативным актам гармонизированного законодательства ЕС: Директивы №: 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU при целевом использовании. Оригинал оценки соответствия находится на сайте www.jablotron.com – Раздел «Загрузки».

Обратите внимание: Несмотря на то, что данные изделия не содержат никаких вредных материалов, после использования его рекомендуется правильно утилизировать.

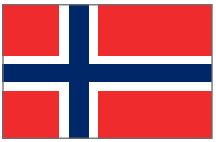


Brugermanual

Käyttöohjekirja

Használati Utasítás

Gebruikershandleiding



Brukermanual

Instrukcja użytkownika

Manual de Utilizador

Užívateľský návod

Användarmanual

www.jablotron.com
M-MULTI100+