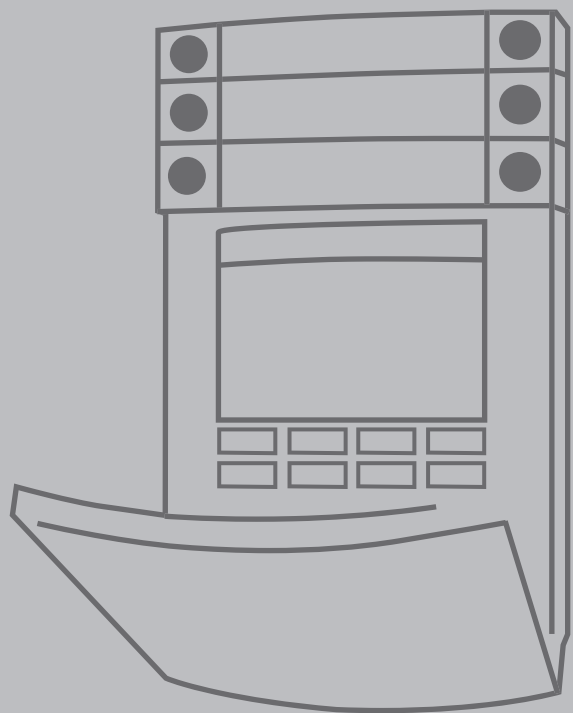


ekirja Használati Utasítás Gebruikershandleiding Bruke
de Utilizador Uživatelský návod Användarmanual Man
ti Utasítás Gebruikershandleiding Brukermanual Instru
vateľský návod Manuál Användarmanual Brugermanua
ruikershandleiding Brukermanual Instrukcja użytkownik
nvändarmanual Manuál Brugermanual Käyttöohjekirja
rukermanual Instrukcja użytkownika Manual de Utiliza
Brugermanual Käyttöohjekirja Használati Utasítás Ge
użytkownika Manual de Utilizador Uživatelský návod /
öohjekirja Használati Utasítás Gebruikershandleiding
de Utilizador Uživatelský návod Manuál Användarman



JABLOTRON 100+

SPIS TREŚCI

1. WPROWADZENIE	2
2. OBSŁUGA SYSTEMU JABLOTRON 100*	3
2.1. OBSŁUGA NA TERENIE OBIEKTU	5
2.1.1. KORZYSTANIE Z KŁAWIATURY SYSTEMU	6
2.1.2. UWIERZYTELNIANIE KODEM Z KŁAWIATURY	7
2.1.2.1. USTAWIENIE ALARMU	9
2.1.2.2. ROZBRAJANIE ALARMU	9
2.1.2.3. ROZBROJENIE POD PRZYMUSEM	10
2.1.2.4. CZĘŚCIOWE UZBRAJANIE ALARMU	10
2.1.2.5. ZAKOŃCZENIE URUCHOMIONEGO ALARMU	10
2.1.2.6. STEROWANIE STREFAMI Z MENU KŁAWIATURY Z WYŚWIELACZEM LCD	11
2.1.3. UŻYWANIE KŁAWIATUR SYSTEMU JA-110E I JA-150E	11
2.1.3.1. UZBROJENIE ALARMU	13
2.1.3.2. ROZBRAJANIE ALARMU	14
2.1.3.3. CZĘŚCIOWE UZBRAJANIE ALARMU	14
2.1.3.4. UZBRAJANIE SYSTEMU POD PRZYMUSEM	15
2.1.3.5. TERMINATING A TRIGGERED ALARM	15
2.1.4. OBSŁUGA SYSTEMU PILOTEM	16
2.2. OBSŁUGA ZDALNA	16
2.2.1. OBSŁUGA SYSTEMU ZA POMOCĄ APLIKACJI MOBILNEJ MyJABLOTRON	17
2.2.2. OBSŁUGA SYSTEMU ZA POMOCĄ INTERFEJSU SIECIOWEGO MyJABLOTRON	17
2.2.3. OBSŁUGA SYSTEMU ZA POMOCĄ MENU GŁOSOWEGO	17
2.2.4. OBSŁUGA SYSTEMU ZA POMOCĄ POLECEN SMS	17
2.2.5. ZDALNA OBSŁUGA SYSTEMU ZA POMOCĄ KOMPUTERA (J-LINK)	17
2.2.6. STEROWANIE WYJŚCIAMI PROGRAMOWALNYMI (PG)	17
2.2.6.1. SEGMENT KŁAWIATURY	17
2.2.6.2. UWIERZYTELNIANIE UŻYTKOWNIKA Z KŁAWIATURY	18
2.2.6.3. Z MENU KŁAWIATURY Z WYŚWIELACZEM LCD	18
2.2.6.4. ZDALNE STEROWANIE	18

2.2.6.5. APLIKACJA MOBILNA MyJABLOTRON	18
2.2.6.6. INTERFEJS SIECIOWY MyJABLOTRON	18
2.2.6.7. WYBÓR NUMERU	18
2.2.6.8. KOMUNIKAT SMS	18
3. BLOKOWANIE/DEZAKTYWACJA W SYSTEMIE	19
3.1. BLOKOWANIE UŻYTKOWNIKÓW	19
3.2. BLOKOWANIE CZUJEK	19
3.3. DEZAKTYWACJA ZEGARÓW	19
4. DOSTOSOWANIE SYSTEMU	19
4.1. ZMIANA KODU DOSTĘPU UŻYTKOWNIKA	19
4.2. ZMIANA, USUWANIE LUB DODAWANIE KARTY/BRELOKA RFID	20
4.3. ZMIANA NAZWY UŻYTKOWNIKA LUB NUMERU TELEFONU	20
4.4. DODAWANIE/USUWANIE UŻYTKOWNIKA	20
4.5. KONFIGURACJA ZDARZEŃ KALENDARZOWYCH	20
5. HISTORIA ZDARZEŃ	20
5.1. ZA POMOCĄ KŁAWIATURY LCD	21
5.2. Z OPROGRAMOWANIA UŻYTKOWNIKA J-LINK	21
5.3. LOGOWANIE DO APLIKACJI MyJABLOTRON (SIECIOWEJ/ MOBILNEJ)	21
6. SPECYFIKACJA TECHNICZNA	21



KONSERWACJA OKRESOWA

- :: Należy prowadzić regularne i terminowe przeglądy konserwacyjne pozwalające zapewnić niezawodne działanie systemu. Konserwacji dokonuje firma instalacyjna nie rzadziej niż raz w roku podczas okresowych przeglądów.
- :: Konserwacja realizowana przez użytkownika polega przede wszystkim na zapewnieniu czystości poszczególnych urządzeń. ADMINISTRATOR systemu może przełączyć system w tryb KONSERWACJA, aby umożliwić otwarcie czujek (wymianę baterii) lub usunięcie ich z instalacji. Żądanie ustawienia trybu KONSERWACJI należy skonsultować z firmą instalacyjną. W przypadku konfiguracji systemu na profil „EN 50131-1, klasa 2”, tryb KONSERWACJA nie jest dostępny.
- :: System można przełączyć w tryb konserwacji za pośrednictwem oprogramowania J-Link lub z menu klawiatury z wyświetlaczem LCD. Po uwierzytelnieniu tryb „konserwacja” można wybrać wraz z wyborem stref, gdzie konieczna jest konserwacja. W trybie konserwacji w wybranych strefach nie nastąpi uruchomienie alarmów, w tym podczas otwierania czujek lub usuwania ich z instalacji.
- :: Tryb konserwacji sygnalizuje przycisk migający na zielono (2 mignięcia co 2 sekundy) oraz wyłączenie dwóch przycisków segmentów dla danej strefy.
- :: Podczas kontaktu z urządzeniami należy zachować ostrożność, by nie dopuścić do uszkodzenia plastikowych części i mechanizmów czujek.
- :: Pokrywa jest zwykle zabezpieczona wypustką, którą małym narzędziem (np. śrubokrętem) należy lekko wepchnąć do korpusu czujki, a następnie można zdjąć pokrywę. W niektórych przypadkach wypustka jest zabezpieczona małą śrubą blokującą, którą najpierw należy odkręcić.
- :: Podczas wymiany baterii w czujce należy zawsze wymieniać jednocześnie wszystkie baterie (używać baterii tego samego typu i tego samego producenta).
- :: Niektóre urządzenia mogą wymagać testowania (np. czujki dymu). Aby uzyskać więcej informacji, należy się skontaktować z serwisantem.

1. WPROWADZENIE

System JABLOTRON 100* jest przeznaczony do użytku nawet przez 600 użytkowników i można go podzielić na 15 odrębnych stref. Można podłączyć do 230 urządzeń. System oferuje do 128 wielofunkcyjnych wyjść programowalnych (np. na potrzeby automatyki budynkowej).

2. OBSŁUGA SYSTEMU JABLOTRON 100+

Systemem bezpieczeństwa można sterować na różne sposoby. Do rozbrojenia alarmu zawsze konieczne jest uwierzytelnianie w formie identyfikacji użytkownika. System wykrywa tożsamość użytkowników i pozwala im obsługiwać części systemu, do których otrzymali dostęp. Można wybrać różne sposoby uzbrajania systemu z uwierzytelnianiem lub bez. W przypadku wykorzystania standardowego rodzaju uwierzytelniania nie jest ono konieczne, ponieważ system można uzbroić przez naciśnięcie prawego przycisku segmentu na klawiaturze. Przy każdym dostępie do systemu zarejestrowana i przechowywana w pamięci jest nazwa użytkownika, data i godzina. Informacje te są dostępne bez ograniczeń czasowych. Użytkownik może anulować uruchomiony alarm (wyłączyć syreny) na podstawie uwierzytelnienia w dowolnej części systemu (zależnie od posiadanych uprawnień dostępowych). Nie oznacza to jednak automatycznego rozbrojenia systemu (o ile nie zmieniono domyślnego ustawienia systemu).

Uwaga: Zależnie od konfiguracji instalacji i ustawień systemu, niektóre z poniższych opcji mogą nie być dostępne. Konfigurację instalacji należy skonsultować z serwisantem.

Użytkownicy i ich uprawnienia dostępowe

UWIERZYTELNIANIE KODEM	OPIS TYPU
Kod SMA	<p>Ten kod posiada najwyższy poziom uwierzytelnienia na potrzeby konfiguracji zachowania systemu i jako jedyny służy do odblokowania systemu po aktywacji alarmu. Pozwala wejść w tryb serwisowy, daje dostęp do wszystkich zakładek z opcjami, w tym do komunikacji SMA, i może uniemożliwić dostęp do niej serwisantowi (kod serwisowy). Dopóki parametr „Usługa ograniczona do administratora / uprawnienia SMA” pozostaje niezaznaczony, kod SMA może sterować wszystkimi strefami i wyjściami PG w systemie. Ten kod pozwala dodawać nowych Administratorów oraz innych użytkowników o niższym poziomie autoryzacji, a także przypisywać im kody, breloki i karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych.</p> <p>Liczbę kodów SMA ogranicza wyłącznie wolne miejsce w centrali sterującej, nie ma kodu ustawionego fabrycznie.</p>
Kod serwisowy (serwis)	<p>Ten kod pozwala wejść w tryb serwisowy i konfigurować zachowanie systemu. Umożliwia dostęp do wszystkich zakładek z opcjami, w tym do komunikacji SMA, jeżeli technik SMA nie ograniczy dostępu. Dopóki parametr „Usługa ograniczona do administratora / uprawnienia SMA” pozostaje niezaznaczony, kod serwisowy może sterować wszystkimi strefami i wyjściami PG w systemie. Pozwala utworzyć użytkowników z pozwoleniem SMA, innych serwisantów, Administratorów oraz innych użytkowników o niższym poziomie autoryzacji, a także przypisać im kody dostępu, breloki i karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych. Liczbę kodów serwisowych ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Domyślny kod fabryczny to 1010. Użytkownik z kodem serwisowym znajduje się zawsze w pozycji 0 centrali sterującej i nie można go wykasować.</p>
Kod administratora (główny)	<p>Ten kod zawsze zapewnia pełny dostęp do wszystkich stref i umożliwia sterowanie wszystkimi wyjściami PG. Administrator może utworzyć innego Administratora oraz inne kody o niższym poziomie autoryzacji i przypisać im dostęp do stref i wyjść PG, kody dostępu, breloki i karty RFID. Ten kod ma możliwość kasowania pamięci alarmów. Może być tylko jeden główny kod administratora, którego nie można skasować. Kiedy opcja „Usługa ograniczona do administratora / prawo SMA” jest aktywna, kod administratora wymaga uwierzytelnienia, by potwierdzić dostęp dla techników SMA i serwisantów.</p> <p>Domyślny kod fabryczny to 1234. Użytkownik z głównym kodem Administratora zawsze znajduje się na pozycji 1 i nie można go wykasować.</p>
Kod administratora (inny)	<p>Posiada dostęp do stref zaznaczonych przez Administratora głównego, do których drugi Administrator może dodawać nowych użytkowników o tym samym lub niższym poziomie autoryzacji do sterowania strefami i wyjściami PG, przypisywać im kody dostępu, breloki i karty RFID. Posiada pozwolenie na kasowanie pamięci alarmów w przypisanych strefach. Kiedy opcja „Usługa ograniczona do administratora/uprawnienia SMA” jest aktywna, kod administratora wymaga uwierzytelnienia, by potwierdzić dostęp. Liczbę kodów Administratora (innego) ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>

UWIERZYTELNIANIE KODEM	OPIS TYPU
Kod użytkownika	<p>Ten kod umożliwia dostęp do sterowania strefami i PG przydzielonymi przez Administratora. Użytkownicy mogą dodać/usunąć własne breloki RFID i karty dostępu, a także zmienić własne numery telefonów. Użytkownicy mogą zmieniać własne kody pod warunkiem, że system używa kodów z prefiksami. Posiada pozwolenie na kasowanie pamięci alarmów w przypisanych strefach. Wybrani użytkownicy mogą mieć dostęp do stref ograniczonych harmonogramem. Liczbę kodów Użytkownika ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>
Uzbrojenie	<p>Ten kod może służyć jedynie do uzbrajania wyznaczonej strefy i do sterowania (WŁ./WYŁ.) wyjściami PG, wymagającymi uwierzytelnienia. Użytkownicy o tym poziomie autoryzacji nie mogą zmieniać własnego kodu ani kasować pamięci alarmów. Liczbę kodów Uzbrajania ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>
Sterowanie PG	<p>Ten kod pozwala użytkownikowi sterować wyjściami programowalnymi wyłącznie na podstawie uwierzytelnienia. Dotyczy to zarówno włączania, jak i wyłączania. Użytkownicy o tym poziomie autoryzacji nie mogą zmieniać własnego kodu ani kasować pamięci alarmów. Liczbę kodów Sterowanie PG ogranicza jedynie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>
Kod panika	<p>Ten kod służy jedynie do aktywacji alarmu panika. Użytkownik tego kodu nie może go zmieniać ani kasować pamięci alarmów. Liczbę kodów panika ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>
Kod strażnika	<p>Jest to kod przeznaczony dla agencji ochrony. Ten poziom uprawnień umożliwia uzbrajanie całego systemu. Kod strażnika może rozbroić cały system wyłącznie podczas alarmu lub po jego zakończeniu, jedynie kiedy pamięć alarmów pozostaje aktywna. Użytkownik tego kodu nie może go zmieniać ani kasować pamięci alarmów. Liczbę kodów strażnika ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>
Kod odblokowania	<p>Ten kod służy do odblokowania systemu po jego zablokowaniu przez alarm. Użytkownik tego kodu nie może go zmieniać ani kasować pamięci alarmów. Liczbę kodów odblokowania ogranicza wyłącznie wolne miejsce w centrali sterującej.</p> <p>Nie ma kodu ustawionego fabrycznie.</p>

Bezpieczeństwo kodów dostępu, urządzeń bezdotykowych RFID i pilotów:

Centrala sterująca pozwala każdemu użytkownikowi przypisać jeden kod 4, 6 lub 8 cyfrowy oraz do dwóch breloków RFID na potrzeby uwierzytelniania w systemie. Uwierzytelnianie użytkownika jest niezbędne podczas wszystkich czynności wykonywanych za pomocą klawiatury, menu głosowego, komputera, aplikacji sieciowych lub mobilnych. Długość kodu wpływa na możliwe kombinacje, a tym samym bezpieczeństwo kodu.

Liczba kombinacji kodu zależy od konfiguracji:

Parametry centrali sterującej	4 CYFRY	6 CYFR	8 CYFR
„Kod z prefiksem” aktywny	$= 10^4 = (10.000)$	$= 10^6 = (1.000.000)$	$= 10^8 = (100.000.000)$
„Kod z prefiksem” oraz „Antynapadowa kontrola dostępu” wyłączona	$= 10^4 - (\text{Liczba użytkowników} - 1)$	$= 10^6 - (\text{Liczba użytkowników} - 1)$	$= 10^8 - (\text{Liczba użytkowników} - 1)$
„Kod z prefiksem” wyłączony, „Antynapadowa kontrola dostępu” włączona	$\leq 10^4 - ((\text{Liczba użytkowników} - 1) * 3)$	$\leq 10^6 - ((\text{Liczba użytkowników} - 1) * 3)$	$\leq 10^8 - ((\text{Liczba użytkowników} - 1) * 3)$

Control panel parameters	4 DIGITS	6 DIGITS	8 DIGITS
Używanie wyłącznie karty RFID z najwyżej 14 znakami (6 stałych + 8 zmiennych)	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$	$= 10^8 = (100.000.000)$
„Kod z prefiksem” oraz „Potwierdzenie karty kodem” włączone	$= (10^8 * 10^4) = 10^{12} =$ (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
„Kod z prefiksem” wyłączone; „Potwierdzenie karty kodem” włączone	$= 10^8 * (10^4 - (\text{Liczba}$ użytkowników - 1))	$= 10^8 * (10^6 - (\text{Liczba}$ użytkowników - 1))	$= 10^8 * (10^8 - (\text{Liczba}$ użytkowników - 1))

Sposoby zwiększenia poziomu ochrony przed odgadnięciem prawidłowego kodu:

- :: używanie kodu z większą liczbą cyfr (kody 6- lub 8-cyfrowe),
- :: bardziej zaawansowane rodzaje uwierzytelniania (jak „Potwierdzenie karty kodem” lub „Podwójne uwierzytelnianie”).

Sposoby obsługi systemu JABLOTRON 100+

Lokalnie:

- :: Z klawiatury systemu
- :: Z pilota
- :: Z komputera z przewodem USB i oprogramowaniem J-Link

Zdalnie:

- :: Poprzez aplikację MyJABLOTRON
- :: Z komputera za pośrednictwem interfejsu sieciowego MyJABLOTRON
- :: Z telefonu z menu głosowym
- :: Z telefonu za pośrednictwem SMS
- :: Z komputera za pośrednictwem internetu i oprogramowania J-Link
- :: Poprzez wdzwonienie się do systemu z autoryzowanego numeru telefonu (wyłącznie do obsługi wyjść programowalnych)



2.1. OBSŁUGA NA TERENIE OBIEKTU

2.1.1. KORZYSTANIE Z KLAWIATURY SYSTEMU

Systemem JABLOTRON 100+ można sterować za pośrednictwem różnych modułów dostępu, które umożliwiają nie tylko sterowanie, ale także wyświetlanie stanów poszczególnych segmentów. System można obsługiwać bezpośrednio (uzbrajanie lub rozbrajanie systemu i innych funkcji automatyki) za pomocą dwuprzyciskowych segmentów na klawiaturze. Przyciski segmentów są jasno opisane i oznaczone kolorem (zgodnie z logiką światła drogowych), w związku z czym wyraźnie widać status poszczególnych segmentów. Segment może służyć także do wskazania stanu (np. otwarte drzwi garażu) lub do sterowania różnymi urządzeniami zautomatyzowanymi (na przykład ogrzewaniem lub roletami na oknach). Maksymalna liczba segmentów w jednym module dostępowym wynosi 20. Segment można ustawić tak, by w nagłym wypadku dzwonił po pomoc (alarm medyczny lub panika).

CIĄGŁE ZIEŁONE ●
ROZBROJONY | WYL.
MIGA ZIEŁONE ★
CZAS NA WEJŚCIE

MIGA CZERWONE ★
ALARM |
PAMIĘĆ ALARMÓW
CIĄGŁE ZIEŁONE ●
WSZYSTKO OK
MIGA ZIEŁONE ★
STEROWANIE
MIGA NA ZIEŁONO ★
2X CO 2 s
KONSERWACJA
CIĄGŁE ŻÓŁTE ●
BŁĄD
MIGA NA ŻÓŁTO ★
NIEPOWODZENIE
UZBRAJANIA



CIĄGŁE CZERWONE ●
UZBROJONY | WŁ.
MIGA CZERWONE ★
ALARM |
PAMIĘĆ ALARMU

CIĄGŁE ŻÓŁTE ●
CZĘŚCIOWO UZBROJONY

**CZYTNIK KART |
KLAWIATURA**

Rodzaje modułów dostępny i ich kombinacji:

Czytnika kart RFID

umożliwia sterowanie systemem za pomocą segmentów i bezdotykowego uwierzytelniania użytkownika (karta/brelok RFID).



Klawiatura z czytnikiem kart

użytkownik może sterować systemem za pomocą segmentów i uwierzytelniania, wpisując kod lub metodą bezdotykową (karta/brelok RFID), bądź korzystając z połączenia obu sposobów, co zapewnia dodatkowe bezpieczeństwo.



Klawiatura z wyświetlaczem LCD i czytnikiem kart

użytkownik może sterować systemem za pomocą segmentów i uwierzytelniania, wpisując kod, metodą bezdotykową (karta/brelok RFID), co zwiększa bezpieczeństwo oraz korzystając zarówno z kodu, jak i karty/breloka, lub przez uwierzytelnianie i stosowanie opcji dostępnych na wyświetlaczu LCD klawiatury.



Podczas rozbrajania alarmu za pomocą przycisków segmentu

konieczne jest uwierzytelnianie użytkownika. Podczas uzbrajania alarmu i sterowania urządzeniami automatyki za pomocą przycisków segmentów uwierzytelnianie użytkownika dla każdego segmentu ma charakter opcjonalny.



Użytkownicy mogą dokonać własnego uwierzytelnienia,

wprowadzając przypisane sobie kody lub używając własnych kart/breloków RFID. Każdy użytkownik może posiadać jeden kod i najwyżej dwa breloki/karty RFID.

Zalecane karty/breloki bezstykowe: JABLOTRON 100+, Oasis lub inne producentów zewnętrznych, kompatybilne z UNIQUE 125 kHz EM. Jeżeli konieczne jest większe bezpieczeństwo, system alarmowy można skonfigurować tak, by korzystał z uwierzytelniania potwierdzonego przy użyciu kart/breloków RFID i kodów (opcjonalnie). Jeżeli użytkownicy pragną jednocześnie sterować kilkoma segmentami, muszą dokonać uwierzytelnienia i kolejno naciskać segmenty poszczególnych stref. W ten sposób użytkownicy mogą na przykład uzbroić dom i rozbroić garaż w ramach jednego uwierzytelniania.

Jeżeli aktywny jest parametr „Kod z prefiksem”, kod uwierzytelniania wpisywany na klawiaturze może się składać z najwyżej jedenastu cyfr: prefiks (jedna do trzech cyfr), gwiazdka * (która oddziela prefiks od kodu głównego) oraz kod 4-, 6- lub 8-cyfrowy zależnie od konfiguracji (na przykład: 123*12345678 lub 1*12345678). Wszyscy użytkownicy mogą zmieniać własne kody następujące po prefiksie. Kod można zmienić za pomocą klawiatury z wyświetlaczem LCD, oprogramowania J-Link lub aplikacji MyJABLOTRON.

Jeżeli aktywny jest parametr „Kod z prefiksem”, użytkownicy mogą mieć prawo do zmiany własnego kodu. Jeżeli parametr „Kod z prefiksem” jest nieaktywny, kody może zmienić jedynie Administrator.

2.1.2. UWIERZYTELNIANIE KODEM Z KAWIATURY

Uwierzytelnianie kodem użytkownika wymaga wpisania prawidłowego kodu na klawiaturze lub użycia breloka/karty RFID.

W systemie można zastosować kod 4-, 6- lub 8-cyfrowy.

Kody można skonfigurować z prefiksem lub bez. W przypadku systemów alarmowych z większą liczbą użytkowników prefiks może być aktywny. Aby zmienić tę opcję, należy skontaktować się z serwisantem systemu alarmowego.

Kod bez prefiksu: CCCC

cccc to kod 4-, 6- lub 8-cyfrowy, dozwolone są kody od 0000 do 99999999

Domyślny kod centrali sterującej

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

Kod z prefiksem: nnn*cccc

- nnn** to prefiks, będący numerem pozycji użytkownika (pozycja 0 do 600)
- *** to separator (klawisz *)
- cccc** to kod 4-, 6- lub 8-cyfrowy, dozwolone są kody od 0000 do 99999999

Domyślny kod centrali sterującej Administrator: **1*1234; 1*123456; 1*12345678;**

- OSTRZEŻENIE:** Kod głównego Administratora zaczyna się od prefiksu **1**
- Główny kod serwisowy zaczyna się od prefiksu **0**

Aby zmienić ten typ kodu, należy skontaktować się z serwisantem systemu alarmowego.

Struktura i opis wewnętrznego menu klawiatury na wyświetlaczu LCD:

Uwierzytelnianie
Administratora
lub Użytkownika
kodem lub
brelokiem / kartą
RFID

**SYGNALIZACJA
ANULOWANIA
OSTRZEŻENIA**

Umożliwia anulowanie alarmu / wskazania nieudanego uzbrajania we wszystkich strefach, do których użytkownik posiada uprawnienia dostępowe.

**STEROWANIE
STREFĄ**

Umożliwia sterowanie strefami systemu, do których użytkownik posiada uprawnienia dostępowe i które są aktywne w ustawieniach wewnętrznych.

STEROWANIE PG

Pozwala użytkownikowi sterować programowalnymi wyjściami PG zależnie od uprawnień użytkownika i zgodnie z ustawieniami wewnętrznymi.

**PAMIĘĆ
ZDARZEŃ**

Wyświetla szczegółowy wykaz pamięci zdarzeń.

**UZBRAJANIE
NIEMOŻLIWE**

Pokazuje listę aktywowanych czujek uniemożliwiających uzbrojenie systemu pod warunkiem, że tę opcję aktywowano w ustawieniach centrali sterującej.

**BŁĘDY
W SYSTEMIE**

Wyświetla listę wszystkich czujek wskazujących błędy w systemie ze stref, do których użytkownik posiada uprawnienia dostępowe.

**POMINIĘTE
CZUJKI**

Wyświetla listę wszystkich zablokowanych czujek w strefach, do których użytkownik posiada uprawnienia dostępowe.

**STATUS
SYSTEMU**

Pokazuje status systemu (lista aktywowanych czujek, sabotaży, niskiego poziomu baterii, pominięcia itp.).

USTAWIENIA

Umożliwia edycję użytkowników i urządzeń (wyłącznie po odłączeniu USB).

**USTAWIENIE
WYŚWIELACZA**

Umożliwia regulację natężenia podświetlenia klawiatury i kontrastu wyświetlacza.

**TRYB
KONSERWACJI**

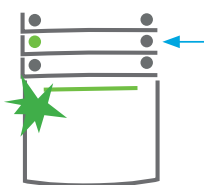
Pozwala Administratorowi zmieniać przypisane strefy na kod konserwacji.

2.1.2.1. USTAWIENIE ALARMU



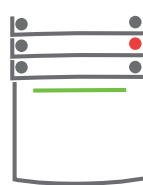
1. Dokonaj uwierzytelniania z klawiatury.

Strefy, którymi można sterować, podświetlają się, a podświetlany przycisk zaczyna migać na zielono.



2. Aby uzbroić konkretną strefę

należy nacisnąć przycisk z prawej strony (niepodświetlony). Kolejno można uzbroić większą liczbę stref. Opóźnienie między zaznaczeniem stref nie może przekraczać 2 sekund.



3. Polecenie zostanie zrealizowane

a klawiatura dźwiękiem powiadomi o czasie na wyjście. Strefa jest teraz uzbrojona, jedynie czujki z reakcją „Alarm opóźniony” zapewnią czas na opuszczenie chronionej strefy podczas czasu na wyjście. Przycisk segmentu uzbrojonej strefy zmienia kolor na czerwony.

Jeżeli podczas uzbrajania alarmu aktywuje się jakakolwiek czujka (np. otwarte okno), system zareaguje w jeden z poniższych sposobów (zgodnie z ustawieniami systemu):

:: System zostanie załączony (ustawienie domyślne).

:: System optycznie wskaże aktywowane czujki. Segment będzie migał na czerwono przez 8 sekund, a po upływie tego czasu dojdzie do automatycznego uzbrojenia systemu.

:: Strefę z aktywowanymi czujkami można uzbroić także przez wielokrotne naciśnięcie przycisku segmentu z prawej strony. W ten sposób użytkownik potwierdzi zamiar uzbrajania strefy z aktywowaną czujką (np. otwarte okno). W przeciwnym razie nie nastąpi uzbrojenie strefy z aktywną czujką.

:: Aktywowana czujka uniemożliwi uzbrajanie strefy. Ten status wskaże migający na czerwono przycisk segmentu. Czujka uniemożliwiająca uzbrojenie zostanie zaznaczona w menu na wyświetlaczu LCD klawiatury.

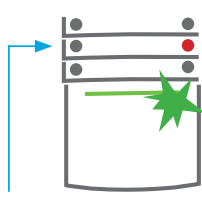
Nieudane uzbrojenie wskaże migający na żółto przycisk (parametr „Niepowodzenie uzbrojenia” musi być aktywny). Aby zaprogramować żądane zachowanie systemu, należy skonsultować instalację z serwisantem.

2.1.2.2. ROZBRAJANIE ALARMU



1. Po wejściu do budynku

(aktywacja czujki o reakcji „Alarm opóźniony”), system zacznie wskazywać czas na wyjście dźwiękiem ciągłym i migającym na zielono przyciskiem segmentu, w którym aktywowano czas na wyjście.

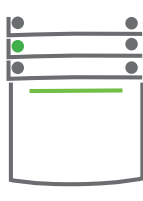


Należy dokonać uwierzytelnienia za pomocą klawiatury

zacznie migać zielona kontrolka pulpitu uwierzytelniania.

2. Nacisnąć lewy przycisk

segmentu dla strefy, która ma zostać rozbrojona.



3. Polecenie zostanie zrealizowane,

a przyciski segmentu będą świecić ciągłym światłem zielonym, wskazując strefy rozbrojone.

Uwaga: Przy aktywnym parametrze „Rozbroj strefę przez uwierzytelnianie tylko w czasie na wyjście” samo uwierzytelnianie pozwoli rozbroić strefę, w której aktywowano czas na wyjście.

2.1.2.3. ROZBROJENIE POD PRZYMUSEM

Ta funkcja umożliwia rozbrajanie systemu w trybie specjalnym. System pozornie się rozbraja, ale uruchamia cichy alarm napadowy, który zostaje następnie przekazany wybranym użytkownikom (w tym do SMA). Rozbrajanie w razie napadu realizuje się przez dodanie 1 do ostatniej cyfry obowiązującego kodu.

Przykładowy kod z prefiksem: Prawidłowy kod: 2*9999

Kod do rozbrajania w razie napadu: 2*9990

Przykładowy kod bez prefiksu: Prawidłowy kod: *9999

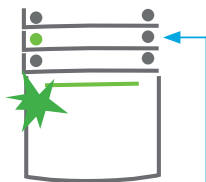
Kod do rozbrajania w razie napadu: 9990

2.1.2.4. CZĘŚCIOWE UZBRAJANIE ALARMU



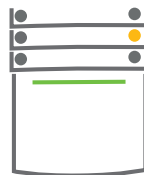
1. Należy uwierzytelnić się za pomocą klawiatury

(wpisać kod lub zbliżyć kartę / brelok do czytnika). Zacznie migać zielony przycisk.



2. Naciśnięć prawy przycisk segmentu

dla wybranej strefy.



3. Polecenie zostanie zrealizowane,

a przycisk segmentu zacznie świecić żółtym światłem, by wskazać częściowe uzbrojenie strefy.

System można również skonfigurować tak, by umożliwić jego częściowe uzbrojenie, zapewniające ochronę wyłącznie za pomocą wybranych czujek w strefie. **Przykład:** Nocą można uzbroić jedynie czujki drzwi i okien, przy czym czujki ruchu wewnątrz domu nie będą reagować.

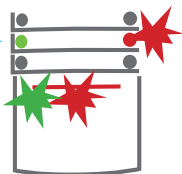
Aby całkowicie uzbroić obiekt, w którym aktywowano uzbrojenie częściowe, należy dwukrotnie naciśnąć przycisk do uzbrajania systemu. Po jednokrotnym naciśnięciu przycisk zacznie migać na żółto, zaś po kolejnym naciśnięciu na czerwono. Jeżeli system jest częściowo uzbrojony, co wskazuje ciągłe żółte światło, całość systemu można uzbroić całkowicie przez uwierzytelnienie i naciśnięcie żółtego przycisku. Po naciśnięciu przycisku system będzie całkowicie uzbrojony, a przycisk zmieni kolor na czerwony.

2.1.2.5. ZAKOŃCZENIE URUCHOMIONEGO ALARMU



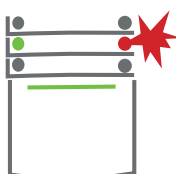
1. Uwierzytelnić

się za pomocą klawiatury (wpisać kod, zbliżyć brelok / kartę do czytnika).



2. Naciśnięć

lewy przycisk segmentu w strefie, w której aktywowano alarm.



3. Rozbrajanie

zostanie ukończone, a syreny ucichną. Przycisk migający na zielono wskazuje na rozbrojenie danej strefy. Czerwone, migające światło wskazuje pamięć alarmów.



4. Aby anulować

wskazanie pamięci alarmów, należy się uwierzytelnić i ponownie naciśnąć zielony przycisk.

5. Segment

wskazuje rozbrojoną strefę zielonym światłem ciągłym.

Szybko migający przycisk segmentu w kolorze czerwonym i podświetlony przycisk wskazania oznacza aktywowany, trwający alarm. Aby zakończyć alarm, należy dokonać uwierzytelnienia za pomocą klawiatury. Strefa pozostaje uzbrojona, przycisk segmentu migający z dużą częstotliwością na czerwono wskazuje pamięć alarmów. Kontrolka będzie migać również po rozbrojeniu systemu.

Jeżeli wskazanie pamięci alarmów uruchomiło się pod nieobecność użytkowników, należy przeszukać historię zdarzeń pod kątem przyczyny alarmu i zachować ostrożność, wchodząc do obiektu i sprawdzając go lub zaczekać na przyjazd agencji ochrony (pod warunkiem, że system jest połączony ze SMA).

Wskazanie pamięci alarmów segmentu pozostanie aktywne do czasu ponownego uzbrojenia systemu. Można je także anulować przez ponowne rozbrajanie systemu. Wskazanie alarmu można także anulować z menu głównego za pomocą klawiatury na wyświetlaczu LCD — Sygnalizacja anulowania ostrzeżenia.

Wskazanie aktywowanego alarmu sabotażu może wyłączyć jedynie Serwisant lub Administrator.

Uwaga: W przypadku użytkownika profilu systemu „EN 50131-1, klasa 2”, zawsze należy dokonać uwierzytelnienia, a potem przeprowadzić żądaną czynność.

Zakończenie alarmu pilotem również rozbroi daną strefę.

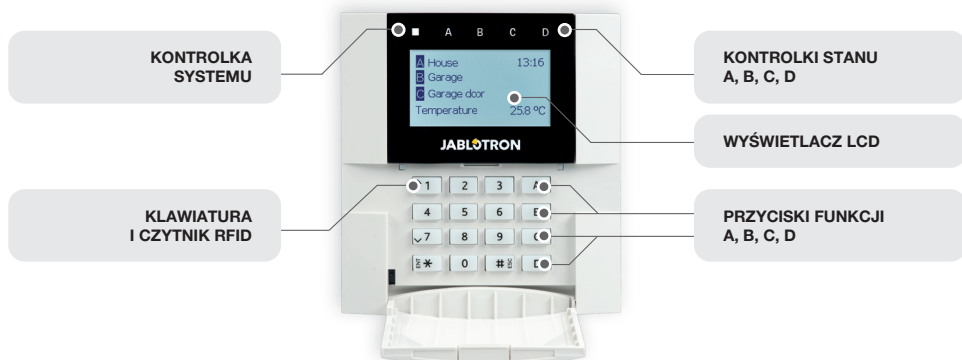
2.1.2.6. STEROWANIE STREFAMI Z MENU Klawiatury z Wyświetlaczem LCD

Stany stref wyświetlają się w lewym górnym rogu wyświetlacza LCD klawiatury. W pełni uzbrojoną strefę pokazuje liczba w prostokacie wypełnionym kolorem czarnym **2**, strefę uzbrojoną częściowo pokazuje liczba w ramce **4**.

Sterowanie z menu klawiatury:

- :: Uwierzytelnienie poprawnym kodem lub kartem / brelokiem RFID.
- :: Wejść do menu przez naciśnięcie **ENTER**.
- :: Sterowanie strefą → **ENTER**.
- :: Strzałkami wybrać żądaną strefę.
- :: Wielokrotne naciśnięcie klawisza **ENTER** umożliwi przejście pomiędzy stanami strefy: częściowo uzbrojona / uzbrojona / rozbrojona.
- :: Naciśnięcie ESC, aby opuścić menu.

2.1.3. UŻYWANIE Klawiatury SYSTEMU JA-110E I JA-150E



Stany poszczególnych stref wskazują kontrolki stanu A, B, C i D nad wyświetlaczem LCD oraz przyciski funkcji. Centralę sterującą można obsługiwać bezpośrednio (uzbrajanie lub rozbrajanie alarmu i innych funkcji automatyki) za pomocą przycisków funkcji na klawiaturze. Przyciski funkcji i kontrolki stanu podświetlają się na kolorowo, aby wyraźnie zasygnalizować stany stref.

:: **ZIELONY** – Rozbrojona :: **ŻÓŁTY** – Rozbrojona częściowo :: **CZERWONY** – Uzbrojona

W celu uwierzytelnienia można wpisać kod dostępu na klawiaturze lub skorzystać z karty/breloka RFID przypisanego do danego użytkownika. Każdy użytkownik może posiadać jeden kod i jedną kartę/brelok RFID. Jeżeli użytkownicy pragną jednocześnie sterować kilkoma strefami, muszą dokonać uwierzytelnienia i kolejno naciskać przyciski funkcji poszczególnych stref. W ten sposób użytkownicy mogą rozbroić wszystkie strefy (na przykład dom i garaż) w ramach jednego uwierzytelnienia.

Struktura i opis wewnętrznego menu klawiatury na wyświetlaczu LCD:

Uwierzytelnianie
Administratora
lub Użytkownika
kodem lub
brelokiem / kartą
RFID

SYGNALIZACJA ANULOWANIA OSTRZEŻENIA

Umożliwia anulowanie alarmu / wskazania nieudanego uzbrajania we wszystkich strefach, do których użytkownik posiada uprawnienia dostępowe.

STEROWANIE STREFĄ

Umożliwia sterowanie strefami systemu, do których użytkownik posiada uprawnienia dostępowe i które są aktywne w ustawieniach wewnętrznych.

STEROWANIE PG

Pozwala użytkownikowi sterować programowalnymi wyjściami PG zależnie od uprawnień użytkownika i zgodnie z ustawieniami wewnętrznymi.

PAMIĘĆ ZDARZEŃ

Wyświetla szczegółowy wykaz pamięci zdarzeń.

UZBRAJANIE NIEMOŻLIWE

Pokazuje listę aktywowanych czujek uniemożliwiających uzbrojenie systemu pod warunkiem, że tę opcję aktywowano w ustawieniach centrali sterującej.

BŁĘDY W SYSTEMIE

Wyświetla listę wszystkich czujek wskazujących błędy w systemie ze stref, do których użytkownik posiada uprawnienia dostępowe.

POMINIĘTE CZUJKI

Wyświetla listę wszystkich zablokowanych czujek w strefach, do których użytkownik posiada uprawnienia dostępowe.

STATUS SYSTEMU

Pokazuje status systemu (lista aktywowanych czujek, sabotaży, niskiego poziomu baterii, pominięcia itp.).

USTAWIENIA

Umożliwia edycję użytkowników i urządzeń (wyłącznie po odłączeniu USB).

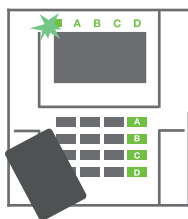
USTAWIENIE WYŚWIELACZA

Umożliwia regulację natężenia podświetlenia klawiatury i kontrastu wyświetlacza.

TRYB KONSERWACJI

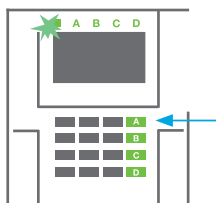
Pozwala Administratorowi zmienić przypisane strefy na kod konserwacji.

2.1.3.1. UZBROJENIE ALARMU



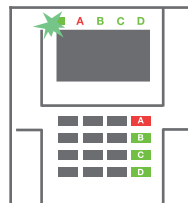
1. Należy dokonać uwierzytelnienia

za pomocą klawiatury. Zaświecą się przyciski funkcji A, B, C i D dla stref, którymi dany użytkownik może sterować, a kontrolka systemu zacznie migać na zielono.



2. Należy nacisnąć przycisk funkcji,

aby uzbroić daną sekcję. Kolejno można uzbroić większą liczbę stref. Opóźnienie między zaznaczeniem stref nie może przekraczać 2 sekund.



3. Polecenie zostanie zrealizowane,

a klawiatura dźwiękiem powiadomi o czasie na wyjście. Strefa jest teraz uzbrojona, jedynie czujki z reakcją „Alarm opóźniony” zapewnią czas na opuszczenie chronionej strefy podczas czasu na wyjście. Kontrolka stanu i przycisk funkcji dla uzbrojonej sekcji zmienia kolor na czerwony.

Jeżeli podczas uzbrajania alarmu aktywuje się jakakolwiek czujka (np. otwarte okno), system zareaguje (na podstawie konfiguracji systemu) w jeden z poniższych sposobów:

- :: Centrala sterująca uzbroi się samoczynnie. Uruchomione czujki zostaną automatycznie zablokowane. *)
- :: System zasygnalizuje uruchomione czujki miganiem przycisku funkcji na czerwono przez 8 sekund, a po zakończeniu tego czasu centrala sterująca zostanie uzbrojona automatycznie (uruchomione czujki zostaną zablokowane). *)
- :: Strefę z aktywowanymi czujkami można uzbroić także przez wielokrotne naciśnięcie przycisku funkcji. Użytkownik musi potwierdzić zamiar uzbrajania strefy z aktywną czujką (np. otwarte okno). W przeciwnym razie nie dojdzie do uzbrojenia systemu.
- :: Aktywowana czujka uniemożliwi uzbrajanie strefy. Ten stan wskaże migający na czerwono przycisk funkcji. Czujka uniemożliwiająca uzbrojenie zostanie pokazana na menu wyświetlacza LCD.

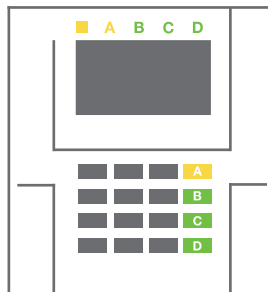
*** OSTRZEŻENIE:** EN 50131, klasa 2 (wybrany profil systemu centrali sterującej) nie obsługuje opcji a) i b).

Jeżeli w trakcie odliczania czasu na wyjście aktywuje się czujka z reakcją „Alarm natychmiastowy w strefie” lub po zakończeniu czasu na wyjście pozostanie aktywna czujka z reakcją „Alarm opóźniony w strefie”, dojdzie do ponownego rozbrojenia centrali sterującej. Nieudane uzbrojenie sygnalizuje kontrolka systemu migającą na żółto. Zostaje ono zgłoszone do SMA i sygnalizuje je syrena zewnętrzna (dotyczy klasy bezpieczeństwa 2).

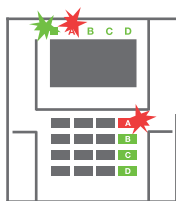
W przypadku konfiguracji centrali sterującej do uzbrajania bez uwierzytelnienia uwierzytelnianie nie jest konieczne. Należy jedynie nacisnąć przycisk funkcji konkretnej strefy. Można także skonfigurować centralę sterującą do uzbrajania po prostu przez uwierzytelnienie.

OSTRZEŻENIE: Uzbrajanie bez uwierzytelniania automatycznie obniża maksymalny poziom bezpieczeństwa do klasy 1. Należy rozważyć wszystkie ewentualne zagrożenia związane z używaniem tej funkcji.

Aby zaprogramować żądane zachowanie systemu alarmowego, należy skonsultować instalację z projektantem lub serwisantem.

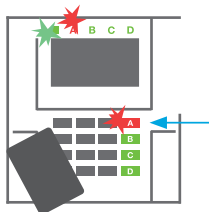


2.1.3.2. ROZBRAJANIE ALARMU



1. Po wejściu do budynku

(aktywacja czujki o reakcji „Alarm opóźniony w strefie”) system zacznie wskazywać czas na wejście dźwiękiem ciągłym i migającą na czerwono kontrolką systemu oraz migającym na czerwono przyciskiem funkcji dla strefy, gdzie aktywowano czas na wejście.

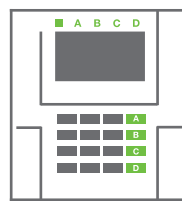


2. Należy dokonać uwierzytelnienia

za pomocą klawiatury — kontrolka systemu zacznie migać na zielono.

3. Należy nacisnąć przyciski

funkcji dla stref przewidzianych do rozbrojenia.



4. Trwa realizacja polecenia.

Przyciski funkcji i kontrolka systemu zmieniają kolor na zielony, wskazując strefy rozbrojone.

Uwaga! Przy aktywnym parametrze „Rozbrój strefę przez uwierzytelnianie tylko w czasie na wejście” samo uwierzytelnianie pozwoli rozbroić strefę, w której aktywowano czas na wejście. W przypadku wielu stref tej opcji należy używać z rozwagą.

Aby zaprogramować żądane zachowanie systemu, należy skonsultować instalację z serwisantem.

2.1.3.3. CZĘŚCIOWE UZBRAJANIE ALARMU

OSTRZEŻENIE: Jest to dodatkowa funkcja systemu alarmowego.

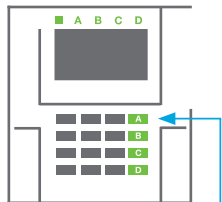
System można również skonfigurować tak, by umożliwić jego częściowe uzbrojenie, zapewniające ochronę wyłącznie za pomocą wybranych czujek w danej strefie.

Przykład: W godzinach nocnych można uzbroić wyłącznie czujki drzwi i okien, zaś wybrane czujki ruchu nie będą aktywować alarmu w przypadku stwierdzenia ruchu w obrębie strefy.

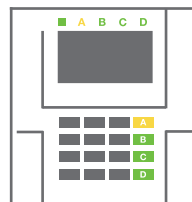


1. Należy dokonać uwierzytelnienia

za pomocą klawiatury (wpisać kod lub zbliżyć kartę/ brelok RFID do czytnika). Przycisk kontrolki systemu zacznie migać na zielono.



2. Nacisnąć przycisk funkcji dla wybranej strefy.



3. Polecenie zostanie zrealizowane,

a przycisk funkcji zacznie świecić żółtym światłem ciągłym, by wskazać częściowe uzbrojenie strefy.

Aby uzbroić cały obiekt, w którym aktywowano uzbrojenie częściowe, należy przez 2 sekundy przytrzymać przycisk do uzbrajania centrali sterującej lub dwukrotnie go nacisnąć. Po jednokrotnym naciśnięciu przycisk świeci ciągłym żółtym światłem, po naciśnięciu po raz drugi świeci ciągłym czerwonym światłem.

Jeżeli system został już wcześniej częściowo uzbrojony, co wskazuje ciągle żółte światło przycisku funkcji, całość systemu można uzbroić całkowicie przez uwierzytelnienie i naciśnięcie żółtego przycisku przez dłuższy czas. Po naciśnięciu przycisku system będzie całkowicie uzbrojony, a przycisk zmieni kolor na czerwony.

Uzbrojenie częściowe można skonfigurować tak, by uwierzytelnianie nie było konieczne.

Aby rozbroić częściowo uzbrojoną centralę sterującą, należy nacisnąć żółty przycisk. Centrala sterująca zostanie rozbrojona, a przycisk zmieni kolor na zielony.

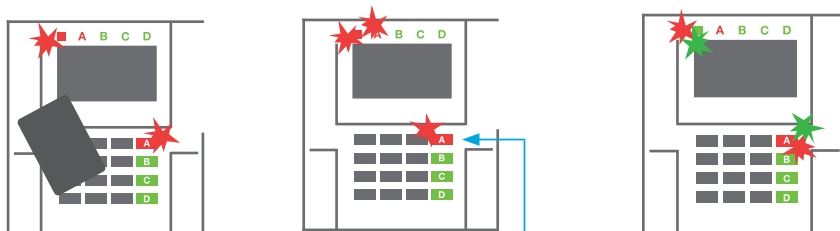
2.1.3.4. UZBRAJANIE SYSTEMU POD PRZYMUSEM

Umożliwia rozbrajanie centrali sterującej w specjalnym trybie. System pozornie się rozbraja, ale uruchamia cichy alarm panika, który zostaje przekazany wybranym użytkownikom (w tym do SMA).

Rozbrajanie w razie napadu realizuje się przez dodanie 1 do ostatniej cyfry obowiązującego kodu. Jeżeli chcą Państwo korzystać z tej funkcji, należy skontaktować się z serwisantem.

Przykład: Prawidłowy kod: 9999 Kod do rozbrajania w razie napadu: 9990

2.1.3.5. ZAKOŃCZENIE URUCHOMIONEGO ALARMU



1. Należy dokonać uwierzytelnienia

za pomocą klawiatury (wpisać kod lub zbliżyć brelok / kartę do

2. Nacisnąć przycisk funkcji

w strefie, w której aktywowano alarm.

3. Rozbrajanie zostanie ukończone

a syreny ucichną. Migające z dużą częstotliwością naprzemienne (zielone/czerwone) światło przycisków funkcji i kontrolki stanu sygnalizują pamięć alarmów.

Trwający aktywny alarm sygnalizuje kontrolka stanu i przycisk funkcji, które migają na czerwono z dużą częstotliwością. Aby zakończyć alarm, należy dokonać uwierzytelnienia za pomocą klawiatury. Strefa pozostaje uzbrojona, przycisk funkcji migający z dużą częstotliwością na czerwono wskazuje pamięć alarmów. Kontrolka będzie migać również po rozbrojeniu systemu.

OSTRZEŻENIE: Jeżeli sygnalizacja pamięci alarmów uruchomiła się pod Państwa nieobecność, należy ostrożnie wejść do budynku, przeszukać historię zdarzeń pod kątem przyczyny alarmu i zachować ostrożność podczas sprawdzania obiektu lub zaczekać na przyjazd agencji ochrony (pod warunkiem że system jest połączony z Stacją Monitorowania Alarmów).

Sygnalizacja pamięci alarmów segmentu pozostanie aktywna do czasu ponownego uzbrojenia systemu. Można ją ewentualnie anulować z menu klawiatury. Menu główne — Sygnalizacja anulowania ostrzeżenia. Wskazanie aktywowanego alarmu sabotażu może wyłączyć jedynie Serwisant i Administrator.

Uwaga: Korzystając z profilu systemu „Domyślny”, można najpierw wybrać konkretną czynność za pomocą przycisku funkcji, a następnie potwierdzić ją uwierzytelnieniem za pomocą klawiatury.

2.1.4. OBSŁUGA SYSTEMU PILOTEM

Piloty przypisuje w systemie instalator. Pilot może być powiązany z konkretnymi użytkownikami, co uniemożliwi powiadomienie przez wiadomość SMS użytkownika, zajmującego się w danej chwili systemem (jeżeli w taki sposób skonfigurowano parametry powiadomienia). Piloty kontrolują i wskazują stan baterii, posiadają sygnalizację świetlną i dźwiękową.

PILOT DWUKIERUNKOWY

Funkcje przycisków są oznaczone symbolem kłódki. Ikona zamkniętej kłódki uzbraja zaprogramowane strefy, otwartej zaś — rozbraja je. Poprawność realizacji polecenia potwierdza kontrolka; rozbrajanie — zielona, uzbrajanie — czerwona. Błąd komunikacji (poza zasięgiem centrali sterującej) wskazuje jedno mignięcie żółtej diody. Przyciski z symbolami pełnych kół i pustych okręgów mogą sterować inną strefą. Przyciski pilota można skonfigurować do sterowania wyjściami PG w różnych trybach: pierwszy przycisk włącza / drugi wyłącza, każdy przycisk może mieć indywidualną funkcję przy zastosowaniu funkcji impulsu lub zmiany. W przypadku większej liczby funkcji można jednocześnie nacisnąć oba przyciski. W ten sposób pilot z 4 przyciskami może posiadać do 6 indywidualnych funkcji lub jedno wyjście stanu PG (np. włączanie i wyłączanie światła), ewentualnie dwa wyjścia PG (np. blokada bramy garażu i drzwi).

Jeżeli system skonfigurowano na Uzbrój po potwierdzeniu, w przypadku aktywacji urządzenia czujka zieloną diodą wskaże nieudane uzbrajanie. Trzeba potwierdzić uzbrajanie, ponownie naciskając przycisk blokady. Uzbrojoną strefę potwierdzi czerwona kontrolka.

Aby nie dopuścić do przypadkowego naciśnięcia, przyciski na pilocie można zablokować. Polecenie zostanie wysłane po wielokrotnym naciśnięciu przycisku. Niski stan energii baterii wskaże po naciśnięciu przycisku sygnał dźwiękowy (trzy piknięcia) oraz migająca na żółto dioda.

Aby uzyskać więcej informacji, należy skonsultować konfigurację pilota z serwisantem.

PILOTY JEDNOKIERUNKOWY

Piloty jednokierunkowe wysyłają sygnał po każdym naciśnięciu przycisku bez otrzymania informacji zwrotnej z centrali sterującej. Wysłanie sygnału potwierdzi jedynie krótkie mignięcie czerwonej diody lub sygnał dźwiękowy.

2.2. OBSŁUGA ZDALNA

Najwyższą wygodę obsługi zdalnej i zarządzania systemem zapewnia usługa MyJABLOTRON. Interfejs sieciowy MyJABLOTRON jest unikalną usługą, umożliwiającą dostęp online do urządzeń firmy JABLOTRON. Umożliwia użytkownikom monitorowanie systemu i sterowanie nim. Jest dostępny w formie aplikacji mobilnej i sieciowej. Usługa MyJABLOTRON pozwala użytkownikowi:

- :: wyświetlać aktualny stan systemu;
- :: uzbrajać/rozbrajać cały system lub jego część;
- :: sterować wyjściami programowalnymi;
- :: przeglądać historię zdarzeń;
- :: wysyłać raporty do wybranych użytkowników za pośrednictwem SMS, poczty elektronicznej lub powiadomień PUSH;
- :: zrobić zdjęcia za pomocą urządzeń do weryfikacji fotograficznej i przeglądać je w zakładce Galeria zdjęć lub bezpośrednio w Ostatnich zdarzeniach;
- :: monitorować aktualną temperaturę lub zużycie energii, wraz z historią w postaci wykresów;
- :: zapewnia także inne przydatne funkcje.

Zależnie od kraju lub regionu konto sieciowe w aplikacji MyJABLOTRON może założyć autoryzowany partner JABLOTRON. Loginem jest adres e-mail użytkownika. Na ten adres zostanie wysłane hasło do pierwszego logowania. Hasło można zmienić w dowolnej chwili w ustawieniach użytkownika.

2.2.1. OBSŁUGA SYSTEMU ZA POMOCĄ APLIKACJI MOBILNEJ MyJABLOTRON

Po utworzeniu konta użytkownik może zdalnie monitorować system i nim sterować za pośrednictwem aplikacji MyJABLOTRON na smartfony z systemem Android i iOS.

2.2.2. OBSŁUGA SYSTEMU ZA POMOCĄ INTERFEJSU SIECIOWEGO MyJABLOTRON

System JABLOTRON 100+ można obsługiwać w sposób prosty i wygodny za pomocą komputera z dostępem do internetu oraz interfejsu sieciowego MyJABLOTRON dostępnego na stronie www.myjablotron.com.

2.2.3. OBSŁUGA SYSTEMU ZA POMOCĄ MENU GŁOSOWEGO

Systemem można sterować za pomocą telefonu komórkowego za pośrednictwem menu głosowego, które w wybranym języku prowadzi użytkownika przez różne opcje. Aby uzyskać dostęp do menu głosowego, należy wybrać numer telefonu systemu alarmowego.

Dostęp do menu głosowego można aktywować dla wszystkich numerów telefonu bez ograniczeń albo wyłącznie dla autoryzowanych numerów telefonu zapisanych w centrali sterującej. Zależnie od konfiguracji konieczne będzie uwierzytelnianie przez wpisanie prawidłowego kodu na klawiaturze telefonu. Kiedy użytkownik wejdzie do menu, system przekaże informacje o aktualnym stanie wszystkich stref przypisanych użytkownikowi. Osoba dzwoniąca może wówczas sterować tymi strefami indywidualnie lub zbiorowo za pomocą klawiatury i dostępnych opcji menu.

System domyślnie odbiera połączenia przychodzące po trzech tonach (około 15 sekund).

2.2.4. OBSŁUGA SYSTEMU ZA POMOCĄ POLECEŃ SMS

Polecenia SMS mogą sterować poszczególnymi strefami i wyjściami programowalnymi tak samo, jak przyciski segmentów na klawiaturze. Wiadomość tekstowa do obsługi systemu ma następującą postać: `CODE_COMMAND`. Faktyczne komendy są wstępnie zdefiniowane (UZBRÓJ/ROZBRÓJ) z dodatkowym parametrem numerycznym wskazującym konkretną strefę. Jedna wiadomość SMS może sterować jednocześnie wieloma strefami. W takim przypadku numery dodane do polecenia określają strefy.

Przykładowa komenda SMS do uzbrajania stref 2 i 4:

CODE_SET_2_4

Komendy do sterowania wyjściami programowalnymi może zaprogramować instalator systemu. Można na przykład ustawić ROLETY W DÓŁ jako polecenie do zamykania rolet na oknach. Można także skonfigurować system tak, by nie wymagał kodu przed poleceniem. W takim przypadku komenda zostaje zidentyfikowana automatycznie, kiedy system rozpozna numer telefonu użytkownika, z którego wysłano wiadomość SMS. Konfigurację wprowadza serwisant.

2.2.5. ZDALNA OBSŁUGA SYSTEMU ZA POMOCĄ KOMPUTERA (J-LINK)

System JABLOTRON 100+ można obsługiwać zdalnie przy pomocy komputera z zainstalowanym oprogramowaniem J-Link. Można je pobrać z sekcji „Do pobrania” na stronie www.myjablotron.com.

2.2.6. STEROWANIE WYJŚCIAMI PROGRAMOWALNYMI (PG)

2.2.6.1. SEGMENT KŁAWIATURY

Wyjście PG włącza się przez naciśnięcie przycisku z prawej strony segmentu, a wyłącza przez naciśnięcie przycisku z lewej strony. Jeżeli wyjście skonfigurowano jako wyjście impulsów, wyłącza się ono w zadanym czasie.

Sterowanie PG może, lecz nie musi, zapisywać się w pamięci zdarzeń centrali sterującej.

Konfigurację wprowadza serwisant.

Zależnie od konfiguracji systemu uwierzytelnianie jest / nie jest wymagane.

2.2.6.2. UWIERZYTELNIANIE UŻYTKOWNIKA Z KLAWIATURY

Wyjście PG można aktywować przez uwierzytelnienie użytkownika (wprowadzenie kodu lub zastosowanie breloka RIFD). Wyjście PG należy skonfigurować do aktywacji za pomocą wskazanej klawiatury.

2.2.6.3. MENU KLAWIATURY Z WYŚWIETLACZEM LCD

Po uwierzytelnieniu użytkownika wyjściami programowalnymi można sterować z menu klawiatury z wyświetlaczem LCD. Użytkownik posiada dostęp do wyjść programowalnych zależnie od praw użytkownika.

Sterowanie z menu klawiatury:

::Uwierzytelnienie poprawnym kodem lub kartą/brelokiem RFID.

::Wejść do menu przez naciśnięcie ENTER.

::Sterowanie PG → ENTER.

::Strzałkami wybrać żądaną grupę PG (1–32), (33–64), (65–96), (97–128) → ENTER.

::Strzałkami wybrać żądane PG → ENTER.

::Wielokrotne naciśnięcie ENTER zmieni stany PG (aktywne PG oznacza numer PG w prostokącie wypełnionym na czarno).

::Nacisnąć ESC, aby opuścić menu.

2.2.6.4. ZDALNE STEROWANIE

Przez naciśnięcie przypisanego przycisku na pilocie Piloty dwukierunkowe potwierdzają aktywację wyjść PG za pomocą kontrolki.

2.2.6.5. APLIKACJA MOBILNA MyJABLOTRON

Klikając WŁ/WYŁ w zakładce Automatyka (PG).

2.2.6.6. INTERFEJS SIECIOWY MyJABLOTRON

Klikając WŁ/WYŁ w zakładce Automatyka (PG).

2.2.6.7. WYBÓR NUMERU

Każdy numer telefonu zapisany w systemie (jeden użytkownik może mieć jeden numer telefonu) może sterować jednym wyjściem PG przez wybór numeru (tj. bez rozpoczynania rozmowy). Wybór numeru obejmuje wybór numeru telefonu karty SIM używanej w systemie bezpieczeństwa i rozłączenie się, zanim system odbierze połączenie. Domyślnie system odbierze połączenie po trzecim dźwięku (około 15 sekund).

2.2.6.8. KOMUNIKAT SMS

Wysłanie wiadomości SMS może włączyć/wyłączyć dane wyjście PG. Zależnie od konfiguracji systemu uwierzytelnianie jest / nie jest wymagane.

Przykład: KOD_SKONFIGUROWANY TEKST

3. BLOKOWANIE/DEZAKTYWACJA W SYSTEMIE

3.1. BLOKOWANIE UŻYTKOWNIKÓW

Każdego użytkownika można tymczasowo zablokować (np. jeśli zgubiono kartę/brelok lub dojdzie do ujawnienia jego kodu dostępu). Po zablokowaniu użytkownika system nie przyjmie jego kodu ID ani karty/breloka. Użytkownicy nie będą także otrzymywać na telefon powiadomień SMS ani raportów głosowych.

Użytkownika może zablokować jedynie administrator systemu lub serwisant. Jednym ze sposobów odebrania praw dostępu jest wybór opcji Ustawienia / Użytkownicy / Użytkownik / Pomiń i kliknięcie „Tak” na klawiaturze LCD. Użytkownika można zablokować lokalnie lub zdalnie za pomocą oprogramowania J-Link, klikając go w kolumnie Ustawienia / Użytkownicy / Blokowanie użytkownika.

Zablokowany (dezaktywowany) użytkownik zostanie oznaczony czerwonym kółkiem do chwili usunięcia blokady.

3.2. BLOKOWANIE CZUJEK

Czujkę można tymczasowo zablokować w sposób podobny do dezaktywacji użytkownika. Czujkę blokuje się, kiedy jego aktywacja jest niepożądana przez pewien czas (np. czujka ruchu w pomieszczeniu, gdzie znajduje się zwierzę, lub wyłączenie dźwięku syreny). System w dalszym ciągu prowadzi diagnostykę styków sabotażu i wysyła zdarzenia serwisowe, ale funkcja alarmu nie jest aktywna.

Czujkę może zablokować jedynie administrator systemu lub serwisant. W tym celu należy wybrać opcję Ustawienia / Urządzenia / Pomiń oraz „Tak” na klawiaturze LCD. Można także wykorzystać oprogramowanie J-Link, klikając czujkę w kolumnie Ustawienia / Diagnostyka / Nieaktywne. Zablokowana czujka pozostaje oznaczona żółtym kółkiem do chwili jej ponownego włączenia za pomocą tej samej procedury. Urządzenie można zablokować także za pomocą aplikacji mobilnej MyJABLOTRON.

3.3. DEZAKTYWACJA ZEGARÓW

Aby tymczasowo dezaktywować automatyczne, planowane zdarzenia w systemie, można dezaktywować zegar. Dezaktywacja planowanego zdarzenia (np. rozbrajanie systemu z ochrony nocnej o określonej godzinie) zapobiegnie jego realizacji (np. podczas urlopu).

Zegar można dezaktywować lokalnie lub zdalnie za pośrednictwem oprogramowania J-Link, klikając strefę w kolumnie Ustawienia / Kalendarz / Zablokowane. Nieaktywny zegar pozostaje oznaczony czerwonym kółkiem do chwili ponownego włączenia za pomocą tej samej procedury.

4. DOSTOSOWANIE SYSTEMU

4.1. ZMIANA KODU DOSTĘPU UŻYTKOWNIKA

W przypadku konfiguracji systemu bez kodów z prefiksem kody bezpieczeństwa może zmienić jedynie administrator systemu i serwisant. Administrator systemu może wprowadzać zmiany zarówno za pomocą menu klawiatury LCD w programie J-Link, jak i aplikacji mobilnej MyJABLOTRON. Kod można zmienić po uwierzytelnieniu, wybierając Ustawienia / Użytkownicy / Użytkownik / Kod. Aby wprowadzić nowy kod, należy wejść w tryb edycji (kod zacznie migać). W tym celu należy nacisnąć Enter, wprowadzić nowy kod i potwierdzić ponownym naciśnięciem Enter. Po zakończeniu wprowadzania zmiany należy potwierdzić, wybierając Zapisz, kiedy system zapyta „Zapisać ustawienia?”.

W przypadku konfiguracji systemu z kodem wymagającym prefiksu poszczególni użytkownicy mogą mieć możliwość zmiany kodu z menu LCD na klawiaturze.

4.2. ZMIANA, USUWANIE LUB DODAWANIE KARTY/BRELOKA RFID

W przypadku konfiguracji systemu bez kodów z prefiksem kody bezpieczeństwa może zmienić jedynie administrator systemu i serwisant. Administrator systemu może wprowadzać zmiany zarówno za pomocą menu klawiatury LCD w programie J-Link, jak i aplikacji mobilnej MyJABLOTRON. Kod można zmienić po uwierzytelnieniu, wybierając Ustawienia / Użytkownicy / Użytkownik / Kod. Aby wprowadzić nowy kod, należy wejść w tryb edycji (kod zacznie migać). W tym celu należy nacisnąć Enter, wprowadzić nowy kod i potwierdzić ponownym naciśnięciem Enter. Po zakończeniu wprowadzania zmiany należy potwierdzić, wybierając Zapisz, kiedy system zapyta „Zapisać ustawienia?”.

W przypadku konfiguracji systemu z kodem wymagającym prefiksu poszczególni użytkownicy mogą mieć możliwość zmiany kodu z menu LCD na klawiaturze.

4.3. ZMIANA NAZWY UŻYTKOWNIKA LUB NUMERU TELEFONU

Jeżeli system skonfigurowano z kodami zawierającymi prefiks, użytkownicy mogą dodawać, zmieniać lub usuwać własne numery telefonu lub zmieniać nazwę w menu LCD na klawiaturze. Można tego dokonać po uwierzytelnieniu, wybierając Ustawienia / Użytkownicy / Użytkownik / Nr telefonu. Aby wprowadzać zmiany, użytkownik musi być w trybie edycji. W tym celu należy nacisnąć klawisz Enter. Wprowadzone zmiany należy potwierdzić ponownym naciśnięciem przycisku Enter. Aby usunąć numer telefonu, wpisać „0” w pole numeru telefonu. Po zakończeniu zmianę należy zapisać, klikając Zapisz, kiedy system zapyta „Zapisać ustawienia?”

Administrator systemu oraz serwisant mogą dodawać, modyfikować lub usuwać numer telefonu użytkownika bądź zmieniać nazwę użytkownika zarówno z menu klawiatury LCD, jak i oprogramowania J-Link.

4.4. DODAWANIE/USUWANIE UŻYTKOWNIKA

Jedynie administrator systemu lub serwisant może dodawać nowych użytkowników do systemu lub ich usuwać. Nowych użytkowników można dodać do systemu (lub usunąć z niego) wyłącznie za pośrednictwem oprogramowania J-Link lub F-Link w przypadku serwisanta.

Podczas tworzenia nowego użytkownika należy mu przypisać pozwolenia na dostęp (uprawnienia), strefy, które może obsługiwać, wyjścia programowalne, którymi może sterować, oraz wymagany rodzaj uwierzytelniania.

4.5. KONFIGURACJA ZDARZEŃ KALENDARZOWYCH

Można skonfigurować zdarzenia kalendarzowe (rozbrajanie / uzbrajanie / częściowe uzbrajanie, sterowanie lub blokowanie wyjść PG).

Zdarzenia kalendarzowe można konfigurować za pośrednictwem oprogramowania J-Link w zakładce Kalendarz.

Dla każdego zdarzenia kalendarzowego, akcji, strefy lub wyjścia PG i zdarzenia można ustawić czas. Dzień można określić jako dzień tygodnia, miesiąca lub roku. Dla wybranego dnia można wybrać powyżej 4 godziny do realizacji akcji lub uzbrojenia powtarzającego się w regularnych odstępach czasu.

Dlatego też zdarzenia kalendarzowe można dostosować nie tylko do sterowania strefami, ale także do sterowania różnymi urządzeniami podłączonymi do wyjść PG.

5. HISTORIA ZDARZEŃ

System bezpieczeństwa przechowuje wszystkie zrealizowane operacje i zdarzenia (uzbrajanie, rozbrajanie, alarmy, błędy, wiadomości wysłane do użytkowników i SMA) na karcie micro SD w centrali sterującej systemem. Każdy wpis obejmuje datę, godzinę (początku i zakończenia) oraz źródło (przyczyna/pochodzenie) zdarzenia.

Różne sposoby przeszukiwania historii zdarzeń systemu:

5.1. ZA POMOCĄ KLAWIATURY LCD

Dostęp do historii zdarzeń za pomocą klawiatury wymaga uwierzytelniania użytkownika. Po uwierzytelnieniu dostępne opcje (zależnie od pozwoleń użytkownika) można wyświetlić, wybierając Pamięć zdarzeń. Rekordy można przeglądać za pomocą strzałek.

5.2. Z OPROGRAMOWANIA UŻYTKOWNIKA J-LINK

Pamięć systemu można przeszukiwać za pomocą oprogramowania J-Link. Zdarzenia można pobrać z centrali sterującej w małych (około 1200 zdarzeń) lub większych (około 4000 zdarzeń) partiach. Zdarzenia można szczegółowo filtrować, zaznaczać kolorami, by ułatwić orientację, lub zapisać w pliku w komputerze.

5.3. LOGOWANIE DO APLIKACJI MyJABLOTRON (SIECIOWEJ/ MOBILNEJ)

Wszystkie zdarzenia w systemie można wyświetlić po zalogowaniu do interfejsu sieciowego/ mobilnego MyJABLOTRON. Konto przedstawia historię w zakresie odpowiadającym uprawnieniom użytkownika.

6. SPECYFIKACJA TECHNICZNA

PARAMETR	JA-103K	JA-107K		
Zasilanie centrali sterującej	~ 110–230 V/50–60 Hz, maks. 0,28 A z bezpiecznikiem F1,6 A/250 V Klasa ochrony II	~ 110–230 V / 50–60 Hz, maks. 0,85 A z bezpiecznikiem F1,6 A/250 V Klasa ochrony II		
Akumulator	12 V; 2,6 Ah (ołowiowo-żelowy)	12 V; 7 do 18 Ah (ołowiowo-żelowy)		
Maksymalny czas ładowania akumulatora	48 h	48 h		
Napięcie magistrali BUS (czerwono–czarna)	od 12,0 V do 13,8 V	od 12,0 V do 13,8 V		
Maksymalne ciągłe zużycie energii elektrycznej przez centralę sterującą	1000 mA	2000 mA stałe 3000 mA przez 60 minut (maks. 2000 mA dla jednej MAGISTRALI)		
Maks. ciągłe zużycie energii elektrycznej do zasilania awaryjnego 12 godzin	JA-103K – akumulatora 2.6 Ah		JA-107K – akumulatora 18 Ah	
	Bez komunikatora GSM	sieć LAN wyl.: 115 mA sieć LAN wł.: 88 mA	Bez komunikatora GSM	sieć LAN wyl.: 1135 mA sieć LAN wł.: 1107 mA
	Z komunikatorem GSM	sieć LAN wyl.: 80 mA sieć LAN wł.: 53 mA	Z komunikatorem GSM	sieć LAN wyl.: 1100 mA sieć LAN wł.: 1072 mA
Maks. ciągłe zużycie energii elektrycznej do zasilania awaryjnego 24 godzin	Bez komunikatora GSM	sieć LAN wyl.: 21 mA	Bez komunikatora GSM	sieć LAN wyl.: 535 mA sieć LAN wł.: 499 mA
	Z komunikatorem GSM	sieć LAN wyl.: 17 mA	Z komunikatorem GSM	sieć LAN wyl.: 530 mA sieć LAN wł.: 494 mA

PARAMETR	JA-103K	JA-107K
Maksymalna liczba urządzeń	50	230
Komunikator LAN	Interfejs ethernetowy, 10/100BASE-T	Interfejs ethernetowy, 10/100BASE-T
Wymiary	268 x 225 x 83 mm	357 x 297 x 105 mm
Masa z/bez AKU	1844 g/970 g	7027 g/1809 g
Reakcja na wprowadzenie nieprawidłowego kodu	Alarm po 10 próbach wprowadzenia nieprawidłowego kodu	
Pamięć zdarzeń	Okolo 7 milionów najnowszych zdarzeń, z datą i godziną	
Zasilacz	Typ A (zgodnie z EN 50131-6) Informacja T 031: W przypadku awarii zasilania głównego system jest podtrzymywany przez 24 godziny a do ARC wysyłany jest raport z informacją o awarii.	
Komunikator GSM (2G)	850 / 900 / 1800 / 1900 MHz	
Klasyfikacja	Klasa ochronności 2 / klasa środowiskowa II (zgodnie z EN 50131-1)	
Środowisko pracy	Wewnętrzne, ogólne	
Zakres temperatur pracy	od -10°C do +40°C	
Średnia wilgotność pracy	75% (bez kondensacji)	
Spełnia wymogi	EN 50131-1 wyd. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 wyd. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN 50581	
Częstotliwość radiowa (z modulem JA-11xR)	868,1 MHz, protokół JABLOTRON	
Emisje radiowe	ETSI EN 300 220-1, -2 (moduł R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
Kompatybilność elektromagnetyczna	EN 50130-4 wyd. 2+A1, EN 55032 wyd. 2, ETSI EN 301 489-7	
Zgodność w zakresie bezpieczeństwa	EN 62368-1+A11	
Warunki pracy	ERC REC 70-03	
Organ certyfikujący	Trezor Test s.r.o. (nr 3025)	
Identyfikacja rozmówcy (CLIP)	ETSI EN 300 089	

Uwaga: Parametry mogą się różnić, jeśli używasz innego typu panelu sterowania.



Firma JABLOTRON ALARMS a.s. oświadcza, że centrale sterujące JA-103K oraz JA-107K są zgodne z wymaganiami Dyrektyw UE nr: 2014/53/UE, 2014/35/UE, 2014/30/UE, 2011/65/UE. Deklaracja zgodności znajduje się na stronie www.jablotron.com w sekcji Do pobrania.

Uwaga: Pomimo, że produkt nie zawiera żadnych niebezpiecznych materiałów, po zakończeniu użytkowania produktu, prosimy o jego zwrot do producenta lub dystrybutora.

www.jablotron.com

M-PLJA100*-USER