# Centrala alarmowa JA-100K do systemu zabezpieczeń

Centrala alarmowa stanowi podstawowy element systemu zabezpieczeń JABLOTRON 100. Jest to najmniejsza centrala alarmowa w serii JA-10xK, przeznaczona do ochrony małych i średnich obiektów. System zabezpieczeń oferuje wiele opcji konfiguracji, w tym profile systemu, umożliwiające bezproblemowe spełnienie wymogów klasy ochronności 2.

Centrali alarmowej można używać z urządzeniami podłączanymi do MAGISTRALI i/lub bezprzewodowymi (kiedy posiada ona moduł radiowy). W systemie zaleca się używanie wyłącznie urządzeń JABLOTRON 100. W przypadku korzystania z urządzeń innych producentów nie gwarantujemy poprawności działania.

**Przestroga:** System zabezpieczeń JABLOTRON 100 może być instalowany wyłącznie przez przeszkolony personel techniczny, posiadający ważny certyfikat wydany przez autoryzowanego dystrybutora.

***Niniejsza instrukcja przeznaczona jest dla przeszkolonego personelu technicznego i dotyczy oprogramowania firmware centrali alarmowej LJ60421 oraz oprogramowania do konfiguracji F-Link w wersji 1.6.0 lub wyższej.***

## Spis treści





JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

# 1 Podstawowy opis i definicje

**Architektura modułowa** — Umożliwia konfigurację systemu do potrzeb konkretnych instalacji, rozmiarów i potrzeb użytkownika.

**Aktualizacja oprogramowania firmware (FW)** — procedura aktualizacji do nowej wersji FW w systemie zawierającym nowe funkcje, ulepszenia i zmiany. Zalecamy, by podczas wszystkich instalacji oraz regularnych kontroli serwisowych sprawdzać aktualność FW. Oprócz FW centrali alarmowej należy w razie potrzeby aktualizować FW we wszystkich urządzeniach (klawiatury, moduły radiowe, czujki ruchu z kamerą itp.).

**Klawiatura sterująca** — moduł przeznaczony do uwierzytelniania użytkownika, sterowania systemem i sygnalizacji jego statusu. Składa się z czytnika breloka/karty RFID, klawiatury do wprowadzania cyfrowych kodów dostępu, czterech przycisków funkcji i wyświetlacza LCD. Klawiaturę dostarczamy zarówno w wersji do MAGISTRALI, jak i w wersji bezprzewodowej.

**Kontrolka systemu** — kwadratowa dioda w lewym górnym rogu klawiatury; sygnalizacja w 3 kolorach: zielony = wszystko w porządku, centrala alarmowa bez usterek; czerwony = alarm i pamięć alarmów; żółty = usterka systemu itp.

**Kontrolka stref** — diody oznaczone literami oznaczającymi strefy A, B, C i D, kolor (czerwony, żółty i zielony) sygnalizuje status wszystkich stref w systemie.

**Przycisk funkcji** — uniwersalny przycisk z możliwością programowania/sterowania/sygnalizacji na klawiaturze wewnętrznej. Istnieją 4 dostępne przyciski funkcji, oznaczone literami A, B, C i D. Każdy przycisk funkcji posiada intuicyjną sygnalizację w postaci podświetlenia w innym kolorze i umożliwia sterowanie systemem (wybranymi strefami).

**Rodzaje alarmów** — system jest w stanie zareagować na włamanie, napad, sabotaż, pożar, wyciek gazu i zalanie wodą. Wykorzystanie odpowiednich czujek pozwala także zgłaszać inne zagrożenia (osoba poruszająca się w ogrodzie, dotykająca strzeżonego obiektu itp.). Istnieją sposoby ograniczenia występowania fałszywych alarmów. Czujki umieszczone w środowisku trudnym pod względem strukturalnym lub operacyjnym można ustawić tak, by aktywacja wymagała potwierdzenia inną czujką.

**Weryfikacja wizualna alarmu** — Urządzenia do weryfikacji zdjęciowej (czujki z kamerą, kamery do weryfikacji zdjęć) są w stanie automatycznie robić i wysyłać zdjęcia sytuacji w monitorowanym obszarze.

**Ochrona osób** — w przypadku zatrzymania, problemów zdrowotnych lub pożaru użytkownik może wezwać pomoc (przez naciśnięcie przycisku na klawiaturze, wprowadzenie kodu panika, aktywację przycisku panika lub wykorzystanie bezprzewodowego pilota).

**Antynapadowa kontrola dostępu** — służy do aktywacji cichego alarmu wyłącznie w drodze uwierzytelnienia lub sterowania systemem (uzbrajanie, rozbrajanie, sterowanie PG itp.), kiedy użytkownik znajdzie się w obecności przestępcy. Alarm Panika aktywuje się podczas sterowania systemem przez wprowadzenie kodu, do którego ostatniej cyfry dodano 1.

**Opóźniona Panika** — funkcja służąca do aktywacji alarmu Panika z opóźnieniem, podczas którego alarmowi można zapobiec. Ta funkcja jest przeznaczona dla użytkowników, którzy obawiają się otworzyć drzwi nieznanej osobie, która może ich zaatakować. W takiej sytuacji użytkownik przed otwarciem drzwi aktywuje opóźniony alarm Panika, a kiedy ma pewność, że jest bezpieczny, musi anulować tę funkcję przed zakończeniem zadanego czasu opóźnienia. Czas opóźnionego alarmu panika można ustawić w odpowiednich ustawieniach wewnętrznych urządzenia, używanych do aktywacji alarmu panika.

**Raportowanie zdarzeń** — raportowanie wszystkich zdarzeń do centrum odbioru alarmów (SMA) może zapewnić terminową interwencję profesjonalistów. Informacje można wysłać także bezpośrednio do użytkowników za pomocą wbudowanego komunikatora LAN lub komunikatora GSM lub PSTN przy użyciu wiadomości SMS (dotyczy wyłącznie GSM) lub połączeń głosowych. Bezpośrednie raporty szczególnie przydają się do monitorowania awarii zasilania, wyjścia i przyjścia dzieci lub pracowników itp.

**Zdalne sterowanie** — za pomocą dodatkowych urządzeń do wybierania numerów upoważnieni użytkownicy mogą kontaktować się z systemem i za pomocą menu głosowego sterować statusem uzbrojenia lub go zmieniać. Statusem poszczególnych stref można sterować zdalnie za pomocą określonych poleceń SMS (tylko GSM). Polecenia SMS można wykorzystać także do włączania i wyłączania programowalnych wyjść PG. Można je aktywować także przez zadzwonienie (bez nawiązania rozmowy) z autoryzowanych numerów telefonu. Istnieje oprogramowanie F-Link przeznaczone dla serwisantów w celu przeprowadzenia zdalnego sterowania. Systemem można także zdalnie sterować za pośrednictwem aplikacji sieciowych lub mobilnych MyJABLOTRON lub MyCOMPANY.

**Prawa dostępowe użytkowników** — określają poziom dostępu dla uwierzytelnienia użytkowników. Można modyfikować prawa dostępowe użytkowników w zakresie części chronionego obiektu, którymi mogą sterować, w tym sterować za pomocą programowalnych wyjść PG. Użytkownicy dokumentują swoją tożsamość przez przyłożenie zbliżeniowego breloka lub wprowadzenie kodu za pomocą klawiatury.

**Administrator** — W systemie można określić (główną) żądaną liczbę administratorów, którzy będą mogli przypisać prawa dostępu zwykłym użytkownikom. Różne strefy budynku mogą posiadać różnych użytkowników.

Domyślnie istnieje jeden główny administrator systemu (pozycja 1), który zawsze ma prawo ustawiać prawa dostępu dla wszystkich użytkowników; kod domyślny 1234 lub 123456, zależnie od opcji długości Kodu (zakładka Konfiguracji początkowej) lub zadanego profilu systemu.

**Serwisant** — Specjalny kod serwisowy (ustawienie domyślne 1010 lub 101010, zależnie od wybranego profilu). Za pomocą tego kodu serwisant ma prawo dostosować wszystkie parametry systemu. W razie potrzeby liczba serwisantów może być większa. Dostęp serwisanta może zależeć od aprobaty administratora. Specjalnym przypadkiem uwierzytelnienia serwisowego jest serwisant Centrum Odbioru Alarmów (w tekście zwanego także „SMA"). Taki serwisant może wykorzystać własny kod (menu F-Link: Ustawienia / Użytkownicy / Uwierzytelnianie użytkownika = SMA) do blokowania dostępu do ustawień parametrów komunikacji z Centrum Odbioru Alarmów.

**F-Link (J-Link)** — Do programowania systemu niezbędny jest komputer z systemem operacyjnym Windows (WIN XP SP3 lub wyższy). Z centralą alarmową można się połączyć z komputera lokalnie za pomocą przewodu USB lub zdalnie z komputera połączonego z internetem. Wszystkie parametry ustawia się przy pomocy komputera i oprogramowania F-Link. To oprogramowanie jest przeznaczone wyłącznie dla przeszkolonego personelu technicznego. Dostępu do niego nie można umożliwić administratorowi ani użytkownikowi końcowemu systemu. Do tego służy uproszczona wersja tego oprogramowania (J-Link), która daje administratorom systemu dostęp do niektórych ustawień (zarządzanie użytkownikami, diagnostyka, ustawianie planowanych zdarzeń, odczyt historii zdarzeń).

**Tryb serwisowy** — to tryb, w którym można zmienić całą konfigurację systemu. W tryb serwisowy systemu może wejść wyłącznie serwisant (lub serwisant SMA). W tym celu należy użyć klawiatury z wyświetlaczem LCD, lokalnym połączeniem z centralą alarmową i komputerem (z przewodem USB) lub dostępem zdalnym za pośrednictwem internetu. W trybie SERWISOWYM system nie działa (nie monitoruje i nie realizuje innych funkcji użytkownika, np. sterowania programowalnymi wyjściami PG). Serwisant może dostosować znaczną część funkcji systemu podczas eksploatacji (tj. bez konieczności przełączenia systemu w tryb SERWISOWY).

**Sterowanie urządzeniami** — system posiada programowalne wyjścia PG, za których pomocą można włączać i wyłączać różne urządzenia. Odzwierciedla to logikę systemu i steruje żądaną liczbą modułów wyjściowych (urządzeń przypisanych do systemu). Wyjściem można sterować za pomocą przycisku funkcji na klawiaturze, przez aktywację czujek, za pomocą manipulatorów zdalnych, zdarzenia w systemie (np. uzbrajanie stref, aktywacja alarmu, itp.), działania kalendarzowego, przy użyciu polecenia SMS lub połączenie z autoryzowanym użytkownikiem. Aktywację wyjścia PG można także zablokować statusem strefy lub czujki bądź dowolnego innego wyjścia PG. Aktywacja wyjścia PG może posiadać sygnalizację świetlną oraz dźwiękową (syrena).

**Sterowanie blokadą drzwi** — elektryczną blokadę drzwi (połączoną z wyjściem PG) można otworzyć przez przyłożenie breloka lub wprowadzenie kodu z klawiatury. Każdemu użytkownikowi można przypisać drzwi, które ma prawo otworzyć. Wyjście można zablokować uzbrojeniem strefy, aby nie było ryzyka, że ktoś wejdzie do strzeżonej (uzbrojonej) strefy. Otwarcie drzwi w drodze uwierzytelnienia użytkownika można zarejestrować w historii zdarzeń systemu.

**Harmonogram zdarzeń automatycznych (Kalendarz)** — korzystając z automatycznej ochrony strefy w oparciu o harmonogram tygodniowy (uzbrojenie / uzbrojenie częściowe / rozbrojenie) i sterowania PG (aktywacja / dezaktywacja, blokowanie / odblokowanie), można programować wyjścia programowalne. W harmonogramie rocznym można ustanowić odstępstwa od harmonogramu tygodniowego (np. święta państwowe, wakacje/urlopy). Harmonogram roczny można ustawić na bieżący i przyszły rok.

**Urządzenia MAGISTRALI** — są podłączone do systemu za pomocą przewodu MAGISTRALI (4 przewodowej). MAGISTRALA zapewnia zasilanie oraz komunikację. Urządzenia MAGISTRALI (czujki, klawiatury, syreny itp.) wymagają przypisania do pozycji (adresu) w systemie, aby mogły działać. Istnieją także urządzenia, które jedynie podłącza się i które działają bez przypisywania do pozycji (niektóre moduły wyjść PG, kontrolki statusu, izolatory MAGISTRALI itp.).

**Urządzenia bezprzewodowe** — aby zapewnić komunikację, centrala alarmowa musi posiadać moduł radiowy, a w systemie muszą być urządzenia bezprzewodowe (czujki, klawiatury, syreny itp.) przypisane do pozycji (adresu). Jednakże w systemie mogą występować także urządzenia, które nie zajmują pozycji (służą wyłącznie do odbierania i nie raportują do centrali alarmowej), np. moduły wyjść PG. Aby objąć większy obszar, w systemie można zainstalować do 3 modułów radiowych (połączonych z przewodem MAGISTRALI). Centrala alarmowa regularnie sprawdza aktywność wybranych urządzeń bezprzewodowych (parametr Nadzór), a także aktualny stan baterii. W przypadku utraty komunikacji z urządzeniem bezprzewodowym centrala alarmowa wskaże błąd komunikacji. Moduły radiowe sprawdzają zagłuszanie/interferencje RF w paśmie komunikacji systemu JABLOTRON 100. W przypadku zagłuszania pasma system aktywuje błąd.

**Czujki włamania** — grupa czujek przeznaczonych do identyfikacji włamywacza. Obejmuje ona czujki ruchu, otwarcia, wybicia szkła, wychylenia lub wstrząsów. Jeśli posiadają zadane reakcje w celu aktywacji alarmu opóźnionego lub bezpośredniego i jego odmian (np. powtarzanego lub potwierdzonego), określa sposób, w jaki czujka zareaguje na aktywację. Czujki pożaru, gazu, zalania lub panika nie należą do grupy czujek włamania.

**Komunikator GSM** — zapewnia połączenie z siecią telefonii komórkowej i internetem. Dzięki temu system może przekazywać dane do centrum odbioru alarmów (SMA) kanałem głównym lub awaryjnym. Komunikator zapewnia dostęp zdalny do centrali alarmowej przy pomocy oprogramowania F-Link, raportując zdarzenia użytkownikom i zdalnie sterując systemem (za pośrednictwem menu głosowego i poleceń SMS).

**Komunikator LAN** — jeżeli wchodzi w skład centrali alarmowej, zapewnia szybki dostęp zdalny za pośrednictwem oprogramowania F-Link (J-Link), a także może przekazywać dane do usługi centrum odbioru alarmów (SMA), wyposażonego w technologię odbioru protokołu IP Jablotron. W ustawieniach centrali alarmowej można wybrać, który typ komunikacji będzie podstawowy, a który pomocniczy.

**PSTN — Komunikator telefoniczny** — można go zainstalować w centrali alarmowej jako moduł uzupełniający dla analogowych linii telefonicznych PSTN. Przekazuje dane do centrum odbioru alarmów (SMA) w standardowych formatach telefonicznych (CID, SIA DC-05 i SIA DC-03). Może także raportować zdarzenia do użytkowników (przez połączenie głosowe) i wspiera zdalne sterowanie systemem przy użyciu menu głosowego. Moduł telefoniczny zwykle stanowi element pomocniczy komunikacji LAN. Moduł może się także komunikować z linią telefoniczną symulowaną przez przekaźnik radiowy.

**Strefa** — system można podzielić na części zwane „Strefami", które można niezależnie uzbrajać i rozbrajać. Strefą może być także odrębne mieszkanie w bloku, piętro w galerii handlowej lub dział w firmie lub budynku biurowym. Współzależność stref można ustawić w sposób przypominający użytkownikowi, że jest ona chroniona przez jego własną centralę alarmową (prawa dostępu, raporty, wyświetlanie na klawiaturze, sygnalizacja dźwiękowa itp.).

**Strefa wspólna** — to odrębna strefa stanowiąca podstrefę dla wybranej grupy stref. W przypadku uzbrajania strefy głównej jako ostatniej strefa wspólna uzbraja się automatycznie. W przypadku rozbrajania strefy głównej jako pierwszej, strefa wspólna również zostaje rozbrojona. Ma to na celu uzbrojenie takich obszarów jak korytarze, toalety, kuchnie w firmach itp.

**Uzbrojenie częściowe** — jest dostępne dla każdej strefy oddzielnie. Przy włączonym uzbrojeniu częściowym system nie reaguje na czujki włamania z parametrem „wewnętrzne" (tj. monitorujące przestrzeń wewnętrzną). Tym samym na przykład ruch jest dozwolony w mieszkalnej części domu, ale system uruchomi alarm lub czas na wejście w przypadku wejścia przez drzwi lub ruchu w garażu, piwnicy itp. Przy całkowitym uzbrojeniu strefa reaguje na aktywację wszystkich przypisanych do siebie czujek.

**Pominięcie** — aktywny status urządzeń lub usterkę obecną w systemie potwierdza się podczas uzbrajania systemu. Status aktywnych wejść ignoruje się po pominięciu do czasu przejścia w tryb czuwania (dezaktywacja). Kiedy wejścia przejdą w tryb czuwania (zostaną dezaktywowane), zostaną objęte ochroną. Przez pominięcie usterek systemu użytkownik potwierdza, że została ona rozpoznana, ale nie zmienia statusu (usterka jest w dalszym ciągu obecna w systemie). Funkcja zależy od opcji umożliwionej parametrem Sposoby uzbrajania.

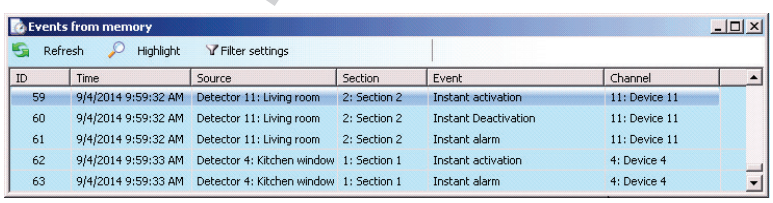
**Blokowanie** — blokuje aktywne wejście urządzenia w celu aktywacji wyjścia PG lub aktywacji dowolnej reakcji. Blokowanie można przeprowadzić ręcznie za pomocą klawiatury, oprogramowania F-Link lub J-Link lub aplikacji MyJABLOTRON. W ten sposób można zablokować wejście urządzenia w dowolnej chwili, nie tylko podczas uzbrajania. Funkcja zależy od opcji umożliwionej parametrem Sposoby uzbrajania.

**Auto-pominięcie** — automatyczne pominięcie reakcji systemu na urządzenie zależnie od opcji. Aktywacja wejścia po 3 aktywacjach lub 3 alarmach (opcjonalnie za pomocą oprogramowania F-Link, zakładka Parametry), usterki również po 3. aktywacji.

**Dezaktywacja** — ta opcja służy do czasowej, ręcznej dezaktywacji wybranych stref, urządzeń, użytkowników, wyjść programowalnych (PG) lub działań kalendarzowych. Strefy, do której przypisano centralę alarmową (zawsze strefa 1), nie można dezaktywować. Dotyczy to także kodu serwisowego w pozycji 0 i kodu administratora w pozycji 1. W przypadku urządzeń wyróżniamy Blokowanie (dotyczy tylko aktywacji wejścia) i Dezaktywację, patrz rozdział 9.13 Disabling and blocking options.

**Sposoby uzbrajania** — wybór poziomu procedury uzbrajania systemu. Opcje obejmują poziomy od najniższego, gdzie system nic nie sprawdza (zawsze uzbraja), do najwyższego, gdzie system nie pozwala na uzbrojenie w przypadku aktywacji jakiegokolwiek urządzenia (na przykład otwarte okno), patrz rozdział 9.9 Obstacles preventing setting the system.

**Historia zdarzeń** — system rejestruje w pamięci występujące zdarzenia. Zawartość pamięci można obejrzeć w oprogramowaniu F-Link przy pomocy klawisza „Event history" (Historia zdarzeń) lub za pomocą klawiatury. Początek zdarzenia zwykle rejestruje się jako Aktywacja (status urządzenia, usterka, sabotaż itp.), a koniec zdarzenia jako Dezaktywacja. Statusy stref rejestruje się jako Uzbrojone / Rozbrojone, statusy alarmów jako Alarm / Wygaśnięcie alarmu, Alarm wyciszony lub Anulowanie alarmu.




Aktywacja i dezaktywacja magnesu
Rozpoczęcie i zakończenie alarmu

Niektóre zdarzenia mogą posiadać jedynie rejestr aktywacji (np. Nowy obraz, Alarm panika, Zmiana konfiguracji).



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

**Karta pamięci MicroSD** — centrala alarmowa używa karty microSD w charakterze nośnika pamięci. Po podłączeniu centrali alarmowej do komputera przewodem USB, w Menedżerze plików wyświetlą się dwa dyski, tj. FLEXI_CFG i FLEXI_LOG. Dostarczona karta może mieć pojemność 4 GB (SD/SD-HC) lub wyższą. Przed rozpoczęciem użytkowania nowej karty SD należy zresetować centralę alarmową do ustawień domyślnych, patrz rozdział 12 Reset of the control panel. Następnie należy przeprowadzić aktualizację firmware, patrz rozdział 13 Firmware updates. Ta procedura zapisze wszystkie niezbędne pliki (teksty domyślne, nagrania głosowe itp.) na karcie SD.

**FLEXI_CFG** — z ukrytymi katalogami i plikami zawierającymi ustawienia systemu. Nie należy zmieniać zawartości dysku, istnieje ryzyko utraty funkcji systemu.

**FLEXI_LOG** — zawiera KOPIE ZAPASOWE, katalog ZDJĘĆ i plik FLEXILOG.TXT, gdzie zapisują się wszystkie zdarzenia w systemie. Wybrane dane z pliku można wyświetlać w programie F-Link / Historia zdarzeń. Katalog ZDJĘĆ służy do przechowywania plików IMGnnnnn.JPG, wysłanych do centrali alarmowej z kamer (np. z czujki ruchu JA-160PC z kamerą). Oba rodzaje plików (txt i jpg) przechowuje się w formie zaszyfrowanej, a ich zawartości zwykle nie można wyświetlać za pomocą programów do przeglądania tekstu i obrazów. Ich zawartość można wyświetlić jedynie, gdy na komputerze jednocześnie działa także program F-Link, a poziom uwierzytelnienia Serwis, Administrator lub SMA potwierdzi się wprowadzeniem odpowiedniego kodu. Zdarzenia rejestruje się w pliku FLEXILOG.TXT do wielkości 10 MB, później nazwa pliku zmienia się na FLEXILOG.OLD i powstaje nowy plik.

**SIMLock** — funkcja centrali alarmowej, którą może aktywować dane SMA w chwili rejestracji centrali alarmowej w aplikacji MyJABLOTRON. W przypadku aktywacji tej funkcji po wymianie karty SIM system automatycznie usunie ustawienie SMA (konieczne będzie odnowienie rejestracji systemu w aplikacji MyJABLOTRON). Ten etap zapobiega niepożądanej transmisji informacji do SMA z karty innej niż zarejestrowana do tego celu i z której dokonano konfiguracji.

## 1.1 Podstawowe wymogi dotyczące konfiguracji

Podczas projektowania systemu należy przestrzegać wymogów obowiązujących norm. Podstawowe instrukcje projektowania systemów zabezpieczeń, ich uruchamiania i serwisu opisano w specyfikacji technicznej CLC/TS 50131-7. Ten dokument należy zastosować do systemów instalowanych i klasyfikowanych zgodnie z normą EN 50131-1, Klasa ochronności 2.

Centralę alarmową JA-100K można ustawić tak, by zachowanie odpowiadające zadanemu **Profilowi systemu** oraz innym warunkom było zgodne z następującymi profilami:

1. **Domyślny** Profil zadany fabrycznie, wszystkie parametry systemu są opcjonalne.
2. **EN50131-1, Klasa 2** Profil zadaje niektóre szczególne parametry systemu (dotyczące centrali alarmowej, klawiatur, syren itp.) zgodnie z wymogami podanej normy dla klasy ochronności 2.
3. **INCERT T031, Klasa 2** Profil zadaje niektóre szczególne parametry systemu (dotyczące centrali alarmowej, klawiatur, syren itp.) zgodnie z wymogami podanej normy (dyrektywa belgijska T031) dla klasy ochronności 2. Profil opiera się na profilu EN 50131-1, Klasa 2 i jest ceniony ze względu na lepsze zabezpieczenie obiektów przed sabotażem i włamaniem.

W związku z raportowaniem alarmów i uznaniem wybranego profilu za zgodny z klasą ochronności 2 centralę alarmową należy instalować co najmniej zgodnie z jedną z poniższych konfiguracji:

| **Sposoby raportowania** | **Profil systemu i odpowiednia konfiguracja** | | |
|---|---|---|---|
| | **Domyślny** | **EN 50131-1, Klasa 2** | **INCERT T031, Klasa 2** |
| Lokalne raportowanie zdarzeń | **Zalecane:** JA-110A lub JA-163A lub JA-110A ustawione jako syrena zewnętrzna | **Wymagane:** JA-110A lub JA-163A lub JA-110A ustawione jako syrena zewnętrzna | **Wymagane:** JA-110A lub JA-163A lub JA-110A ustawione jako syrena zewnętrzna |
| Zdalne raportowanie alarmów — kanał główny (główna ścieżka komunikacji do SMA) | **Zalecane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID | **Zalecane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID | **Wymagane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID |
| Zdalne raportowanie alarmów — kanał pomocniczy (awaryjna ścieżka komunikacji z SMA) | **Zalecane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID | **Zalecane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID | **Zalecane:** LAN lub kanał GSM/GPRS z protokołem IP lub linia PSTN z protokołem Contact ID |

**UWAGA 1**: System alarmowy JABLOTRON 100 zaprojektowano zgodnie z normami wymienionymi w poszczególnych profilach systemu. Należy spełnić co najmniej podstawowe wymogi dotyczące dróg raportowania alarmów i sygnalizacji ostrzeżeń. Sposoby raportowania podane w niniejszej tabeli są zgodne z normą EN 50131-1 + A1+A2, punkt 8.6.4, tabela 10. Szczegółowe wymogi określające właściwości ścieżek komunikacji ze SMA podano w rozdziale dotyczącym ustawień komunikatora.

**UWAGA 2**: Termin „ścieżka komunikacji" oznacza fizyczne medium transmisyjne, np. przewody metalowe, światłowody lub transmisję radiową.

**UWAGA 3**: Awaryjną ścieżkę komunikacji należy zrealizować za pomocą odmiennego niż główne medium transmisyjnego. Nie można łączyć na przykład technologii GSM i LAN w oparciu o sieć WIFI. Oba te sposoby należą do transmisji radiowej i może dojść do ich jednoczesnego zagłuszania (sabotażu).

* ***Przestroga:***

*— Należy zapewnić zasilanie awaryjne dla wszystkich urządzeń sieci LAN zapewniających połączenie z internetem!*

*— Należy ograniczyć dostęp osób nieuprawnionych do urządzeń sieci LAN i innych paneli lub centrali komunikacyjnych!*

Podczas projektowania systemu należy uwzględnić podział na strefy i zadany czas na wejście, aby można było ustawić definicję stref alarmu opóźnionego. Mogą występować 2 rodzaje stref alarmu opóźnionego (Alarm opóźniony i Brama garażu), z których każda posiada własny zegar odliczający zadany czas na wejście i wyjście.

Należy wybrać jak najkrótszą drogę wejścia i wyjścia, tj. trasę od drzwi wejściowych do klawiatury sterującej. Klawiaturę (główny element sterowania systemem zabezpieczeń) należy umieścić w pobliżu drzwi wejściowych, ponieważ użytkownik powinien być w stanie rozbroić system w ciągu 30 sekund od chwili wejścia na teren chronionego obiektu. Ten wymóg wiąże się z koniecznością instalacji kilku klawiatur w chronionych obiektach o wielu drogach dostępu.

## 1.2 Kody dostępu i ich ustawienia domyślne

Aby można obsługiwać system (uzbrajanie, rozbrajanie lub sprawdzanie statusu wybranej strefy bądź urządzenia), konieczne jest uwierzytelnienie przez wprowadzenie poprawnego kodu lub przyłożenie karty bądź breloka RFID do modułu uwierzytelniania (klawiatury). System pokaże informacje i umożliwi sterowanie systemem zależnie od praw dostępu, związanych z poziomem uwierzytelniania danego użytkownika. Serwisant uzyskujący dostęp do systemu z programu F-Link (J-Link) zdalnie z aplikacji MyJABLOTRON lub z menu głosowego również musi dokonać uwierzytelnienia przez wprowadzenie prawidłowego kodu dostępu.

Kod dostępu może posiadać 4 lub 6 cyfr (zależnie od wybranego profilu systemu).

| Kody dla JA-100K | Profil domyślny (Kody 4-cyfrowe) | Profil EN50131-1, (Kody 6-cyfrowe) | INCERT T 0xx (Kody 6-cyfrowe) |
|---|---|---|---|
| **Format kodu:** | ***nnnn*** | ***nnnnnn*** | ***nnnnnn*** |
| **Serwis (domyślny):** | **1010** | **101010** | **101010** |
| **Administrator (domyślny):** | **1234** | **123456** | **123456** |

***Ostrzeżenie:*** *Zmiana ustawień profilu systemu kasuje wszystkie kody określone przez użytkownika i przywraca domyślne wartości dla kodów domyślnych (Serwis, Administrator). W systemie pozostają skonfigurowane wszystkie karty/breloki RFID.*

Domyślny kod serwisowy zostaje wprowadzony automatycznie przez program F-Link, dzięki czemu program nie żąda go od pierwszej aktywacji do zmiany kodu. Ze względów bezpieczeństwa bezpośrednio po zakończeniu instalacji należy zmienić wszystkie kody domyślne.

### 1.2.1 Zmiana kodów dostępu

Kody użytkownika lub breloki/karty RFID mogą zostać utworzone lub zmienione przez Administratora systemu lub serwisanta. Nowy kod lub brelok/kartę RFID można przypisać użytkownikowi o zadanych uprawnieniach. Wyłącznie serwisant posiada uprawnienia do utworzenia takiego użytkownika przy pomocy programu F-Link.

**Kody dostępu może dodawać i zmieniać:**

- administrator z klawiatury LCD (warunek: komputer wymaga odłączenia od centrali alarmowej, nie może być połączenia zdalnego lub lokalnego ani już zadanego użytkownika o żądanych uprawnieniach),
- serwisant za pomocą programu F-Link (warunek: aktywny parametr Serwis i SMA może sterować systemem),
- użytkownik bez prawa do zmiany własnego kodu.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Każdy kod użytkownika można ustawić na dowolną wartość z uwzględnieniem długości kodu podanej przez wybrany profil systemu, lecz centrala alarmowa ogranicza wykorzystanie tej samej wartości kodu, już używanej w systemie, dla innego użytkownika. Wyłącznie Administrator/Administratorzy systemu ponosi/ponoszą pełną odpowiedzialność za przypisywanie i edycję kodów użytkownika.

### 1.2.2 Zabezpieczające kody dostępu i urządzenia RFID

Centrala alarmowa pozwala przypisać każdemu użytkownikowi jeden kod (zależnie od wybranego profilu) i jeden brelok/jedną kartę RFID na potrzeby uwierzytelniania. Uwierzytelnienie jest niezbędne w przypadku obsługi systemu za pomocą klawiatury. Poziom bezpieczeństwa jest do tego dostosowany i mogą go reprezentować liczby w poniższej tabeli.

**Obliczenie kombinacji kodu dla 1 użytkownika podano na poniższych przykładach:**

| Parametry centrali alarmowej | Kody 4-cyfrowe | Kody 6-cyfrowe |
|---|---|---|
| **Antynapadowa kontrola dostępu — WYŁ.**<br>**Uwierzytelnianie standardowe — WYŁ.** | **= $10^4$** – (Liczba użytkowników zapisanych w systemie – 1) | **= $10^6$** – (Liczba użytkowników zapisanych w systemie – 1) |
| **Antynapadowa kontrola dostępu — WŁ.**<br>**Uwierzytelnianie standardowe — WŁ.** | **≤ $10^4$** – ((Liczba użytkowników zapisanych w systemie – 1) * 3) | **≤ $10^6$** – ((Liczba użytkowników zapisanych w systemie – 1) * 3) |
| **Antynapadowa kontrola dostępu — WYŁ.**<br>**Uwierzytelnianie podwójne — WYŁ.** | **= $10^8$ * ($10^4$** – (Liczba użytkowników zapisanych w systemie – 1)) | **= $10^8$ * ($10^6$** – (Liczba użytkowników zapisanych w systemie – 1)) |
| **Antynapadowa kontrola dostępu — WŁ.**<br>**Uwierzytelnianie podwójne — WŁ.** | **≤ $10^8$ * ($10^4$** – ((Liczba użytkowników zapisanych w systemie – 1) * 3)) | **≤ $10^8$ * ($10^6$** – ((Liczba użytkowników zapisanych w systemie – 1) * 3)) |
| Używanie wyłącznie **karty RFID** bez kodu cyfrowego | **= $10^8$** = (100 000 000) | **= $10^8$** = (100 000 000) |

**Przykład:**

Wybrany profil: Domyślny ~ Kody 4-cyfrowe
Liczba użytkowników zapisanych w systemie: Maks. 33
Antynapadowa kontrola dostępu: Nieaktywna
Liczba kombinacji kodu: $10^4$ – 33 = 9 967 kombinacji / użytkowników (przy 33 użytkownikach)

**Zwiększanie poziomu bezpieczeństwa kodów:**

- Proszę wybrać kody 6-cyfrowe (profil systemu EN-50131-1, INCERT)
- Proszę wybrać poziom uwierzytelniania „Uwierzytelnianie podwójne", gdzie należy zastosować standardowy poprawny kod dostępu i brelok/kartę RFID.

**Ochrona przed próbą złamania kodu:**

Centrala alarmowa liczy próby wprowadzenia nieprawidłowego kodu, a po **10. próbie** system uruchomi zdarzenie sabotażu „Próba złamania kodu", włączy alarm i zgłosi zdarzenie pod zadane numery. Nie stosuje się dodatkowego blokowania wprowadzenia do systemu innych kodów. Po wprowadzeniu prawidłowego kodu licznik prób wprowadzenia błędnego kodu resetuje się, a uruchomiony alarm wyłącza. Licznik ustawiono na 10 prób i nie można tej liczby zmienić.

## 1.3 Regularna kontrola systemu (konserwacja)

Cały system zabezpieczeń wymaga okresowych testów sprawności, w tym sprawności wszystkich elementów, ale także czyszczenia, zewnętrznych kontroli wzrokowych (pył i zabrudzenia, zwykle prowadzonych przez użytkownika systemu) oraz wewnętrznych kontroli wzrokowych (pajęczyny, owady, stan baterii, itp., prowadzonych przez serwisanta). Niektóre elementy systemu są w stanie prowadzić auto-testy i zgłaszać możliwe usterki do centrali alarmowej, która powiadomi o takim statusie zgodnie z ustawieniami. Serwisant podczas corocznego przeglądu systemu zobowiązany jest przeprowadzić niemal wszystkie czynności konserwacji.

Centrala alarmowa podczas próby obciążenia sprawdza główną baterię awaryjną okresowo kilka razy na minutę. Baterie w urządzeniach bezprzewodowych (w czujkach, klawiaturach, syrenach, manipulatorach zdalnych) sprawdza się automatycznie przy każdej transmisji testowej łącza. System zgłasza niski poziom baterii z każdego przypisanego urządzenia od chwili jego pojawienia się do czasu wymiany za pomocą zadanego raportu SMS i równocześnie na klawiaturze LCD. Wymianę baterii może prowadzić jedynie serwisant.

Po wyjęciu baterii należy odczekać kilka chwil (20 sekund), by wewnętrzne kondensatory mogły się rozładować, i dopiero wówczas włożyć nową baterię.

**Przegląd zalecanej konserwacji / kontroli funkcji:**

| Typ urządzenia | Opis | Kto wykonuje czynność | Częstotliwość czynności |
|---|---|---|---|
| Czujki pożaru | Test funkcji; przed rozpoczęciem należy poinformować agencję SMA! | Administrator | Raz w miesiącu |
| | Usunąć zabrudzenia i pył. | Administrator | Dwa razy do roku |
| | Sprawdzenie baterii (urządzenia MAGISTRALI i bezprzewodowe) | Serwisant | Raz w roku |
| Przyciski panika | Test funkcji; przed rozpoczęciem należy poinformować agencję SMA! | Administrator | Raz w miesiącu |
| | Sprawdzenie baterii, pomiar napięcia, stan fizyczny. | Serwisant | Raz w roku |
| Czujki | Usunąć zabrudzenia i pył. | Administrator | Raz w roku |
| | Test funkcji; test zasięgu RF dla czujek bezprzewodowych. W przypadku czujek z wbudowaną kamerą sprawdzić przez zrobienie zdjęcia. | Serwisant | Raz w roku |
| | Sprawdzenie baterii, pomiar napięcia każdej baterii, stan fizyczny itp. | Serwisant | Raz w roku |
| Klawiatury | Usunąć zabrudzenia i pył. | Administrator | Dwa razy do roku |
| | Sprawdzić każdy przycisk, przyciski funkcji i czujnik RFID; sprawdzić zasięg RF dla klawiatur bezprzewodowych. | Serwisant | Raz w roku |
| | Kontrola stanu baterii i ich stanu fizycznego, pomiar napięcia każdej baterii itp. | Serwisant | Raz w roku |
| Syreny | Usunąć pył i zabrudzenia, owady, sprawdzić, czy do płytki drukowanej nie dostała się woda itp. | Serwisant | Raz w roku |
| | Test funkcji; test zasięgu RF dla syren bezprzewodowych. | Serwisant | Raz w roku |
| | Sprawdzenie baterii i baterii awaryjnych, pomiar, stan fizyczny, pomiar napięcia każdej baterii | Serwisant | Raz w roku |
| Manipulatory zdalne (RC) | Test funkcji; zasięg RF, kontrola sygnalizacji niskiego poziomu baterii. Czyszczenie lub wymiana plastikowej obudowy. | Administrator lub Serwisant | Raz w roku |
| Stan alarmowy | Test komunikacji z SMA, połączenia głosowe i raportowanie SMS. | Administrator lub Serwisant | Raz w roku |
| Bateria awaryjna w centrali alarmowej | Test podczas odłączenia od sieci (prądu zmiennego) i pomiar napięcia w baterii awaryjnej po upływie 5 minut od wyłączenia zasilania sieciowego. | Serwisant | Raz w roku |
| Wyjścia programowalne (PG) | Test funkcji; zasięg RF modułów bezprzewodowych | Serwisant | Raz w roku |

Wszystkie procedury zalecane przez producenta systemu nie posiadają priorytetu wyższego od miejscowych przepisów i rozporządzeń.

# 2 Rozmiar systemu

Rozmiar systemu zabezpieczeń można ustalić opcjonalnie zależnie od wielkości chronionego obiektu i wymogów użytkownika końcowego.

Centralę alarmową można podzielić na 4 strefy (obszary z możliwością niezależnej regulacji). Każde urządzenie posiada własny adres (klawiatury, czujki, syreny) i wymaga przypisania do jednej ze stref. Liczbę urządzeń, stref, użytkowników i wyjść programowalnych konfiguruje się za pomocą programu F-Link w zakładce Konfiguracja początkowa. Dzięki temu łatwiej programować instalację. Ich ilość można zwiększać lub zmniejszać (zmniejszenie jest możliwe wyłącznie, gdy nie ma zadanych łączy logicznych mogących je blokować).



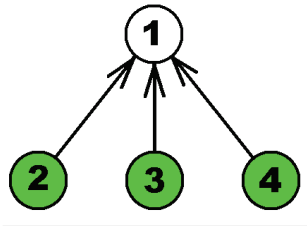
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

W ten sposób można utworzyć system dla niewielkiego mieszkania o jednej strefie i kilku urządzeniach lub dla dużego budynku, który wykorzysta cały potencjał centrali alarmowej JA-100K ze strefami z możliwością indywidualnego sterowania. Strefy można powiązać z innymi strefami (strefą wspólną), by sterować nimi wszystkimi i ich statusami.

## 2.1 Konfiguracja i podział

Centrala alarmowa systemu zabezpieczeń JA-100K, dzięki swemu zasięgowi, wymiarom i liczbie stref, przeznaczona jest do ochrony małych i średnich obiektów. Strefa jest elementem systemu, do którego przypisuje się urządzenia powiązane z chronionym obszarem. Małe obiekty mogą posiadać jedną podstawową strefę (mieszkanie, garaż, itp.), i w takim przypadku wszystkie urządzenia przypisuje się do tej strefy. Systemy średniej wielkości mogą posiadać kilka stref (na przykład dom rodzinny lub budynek biurowy), a także *strefę wspólną 2. poziomu* (wspólne korytarze, piwnice, garaże, toalety itp.) Dla eksploatacji takich systemów szczególnie ważna jest konfiguracja uwierzytelniania użytkownika na najniższy poziom sterowania podstawowymi strefami. Strefę wspólną uzbraja się automatycznie przy automatycznym uzbrajaniu każdej strefy wspólnej, a rozbraja automatycznie przy rozbrojeniu co najmniej jednej strefy podstawowej.

Strefy podzielone na dwa poziomy (1 — wspólny, 2, 3, 4 — sterowane niezależnie)




**2. poziom** (kontrolowany)

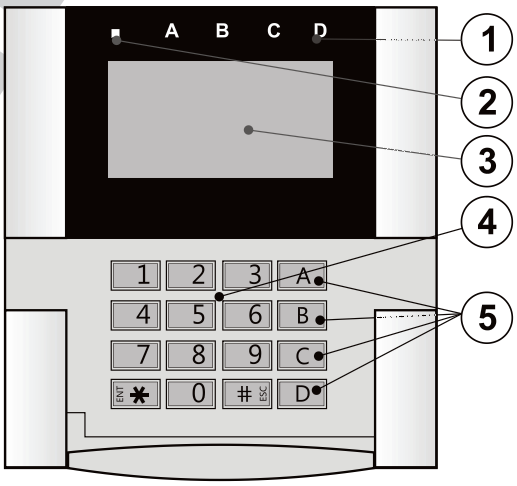
**1. poziom** (obsługiwa

Uwaga: *Użytkownik „sprzątaczka", posiadający jedynie dostęp do strefy wspólnej, może posiadać przypisaną strefę wirtualną (1. poziom), która nie musi obejmować żadnych czujek. Rozbrojenie tej strefy wirtualnej automatycznie rozbraja wszystkie strefy wspólne w obiekcie (2. poziom), do których ta osoba może przejść.*

## 2.2 Sterowanie systemem

Klawiatura systemu jest przeznaczona do podstawowego sterowania systemem. W systemie można używać kilku klawiatur, z których każda może działać inaczej, zgodnie z własnymi ustawieniami. Z każdej klawiatury można sterować dowolną strefą systemu.

Każda klawiatura posiada 4 **przyciski funkcji** zapewniające szybkie sterowanie. Każdy z nich można skonfigurować na potrzeby różnych funkcji, takich jak uzbrajanie/rozbrajanie, sterowanie urządzeniami lub przyzywanie awaryjne. Może także służyć do sygnalizacji statusu strefy lub wyjścia PG (może sygnalizować aktywny status standardową czerwoną lub zieloną diodą — funkcja „Odwrotna sygnalizacja PG"). Dlatego właśnie przycisk funkcji może służyć na przykład za sygnalizator styku magnetycznego umieszczonego na drzwiach, wskazując ich otwarcie lub zamknięcie. Może służyć także za „Wspólny przycisk funkcji", dzięki czemu można jednocześnie sterować kilkoma strefami. Konfigurację klawiatury opisano w rozdziale 10.3.1 Keypad configuration.




*1 — kontrolka statusu; 2 — kontrolka systemu; 3 — wyświetlacz LCD; 4 — klawiatura i czytnik RFID; 5 — przyciski funkcji*

# 3 Parametry użytkowe centrali alarmowej JA-100K

Centrala alarmowa JA-100K jest podstawowym elementem systemu JABLOTRON 100. Jej podstawowe parametry zebrano w poniższej tabeli:

*Tabela 1*

| Funkcja / Typ | JA-100K | Uwaga |
|---|---|---|
| Maksymalna liczba urządzeń | 32 | Suma elementów bezprzewodowych i MAGISTRALI |
| Maksymalna liczba użytkowników | 33 | |
| Maksymalna liczba niezależnych stref (części) | 4 | |
| Maksymalna liczba wyjść programowalnych | 4 | |
| Maksymalna liczba modułów radiowych | 3 | |
| Komunikator IP LAN (Ethernet) | Tak | |
| Komunikator GSM / GPRS | Nie | Opcjonalne wyposażenie dodatkowe |
| Komunikator telefoniczny PSTN | Nie | Opcjonalne wyposażenie dodatkowe |
| Zalecana bateria awaryjna 12 V | Maks. 2,6 Ah | Bateria kwasowo-ołowiowa |
| Maksymalne stałe zużycie energii dostępne dla urządzeń z centrali alarmowej | 85 mA (z LAN)<br>125 mA (bez LAN) | Dla zasilania awaryjnego 12 h z zalecanej baterii liczba uwzględnia wewnętrzne zużycie centrali alarmowej |
| Maksymalne możliwe zapotrzebowanie krótkoterminowe na energię | 1000 mA | Maks. 5 min |
| Zacisk końcowy MAGISTRALI | Złącze 1+RJ | Złącze RJ służy wyłącznie do podłączania modułu radiowego bezpośrednio w centrali alarmowej. |
| Maksymalna długość przewodu MAGISTRALI | 500 m | |

## 3.1 Opis centrali alarmowej JA-100K

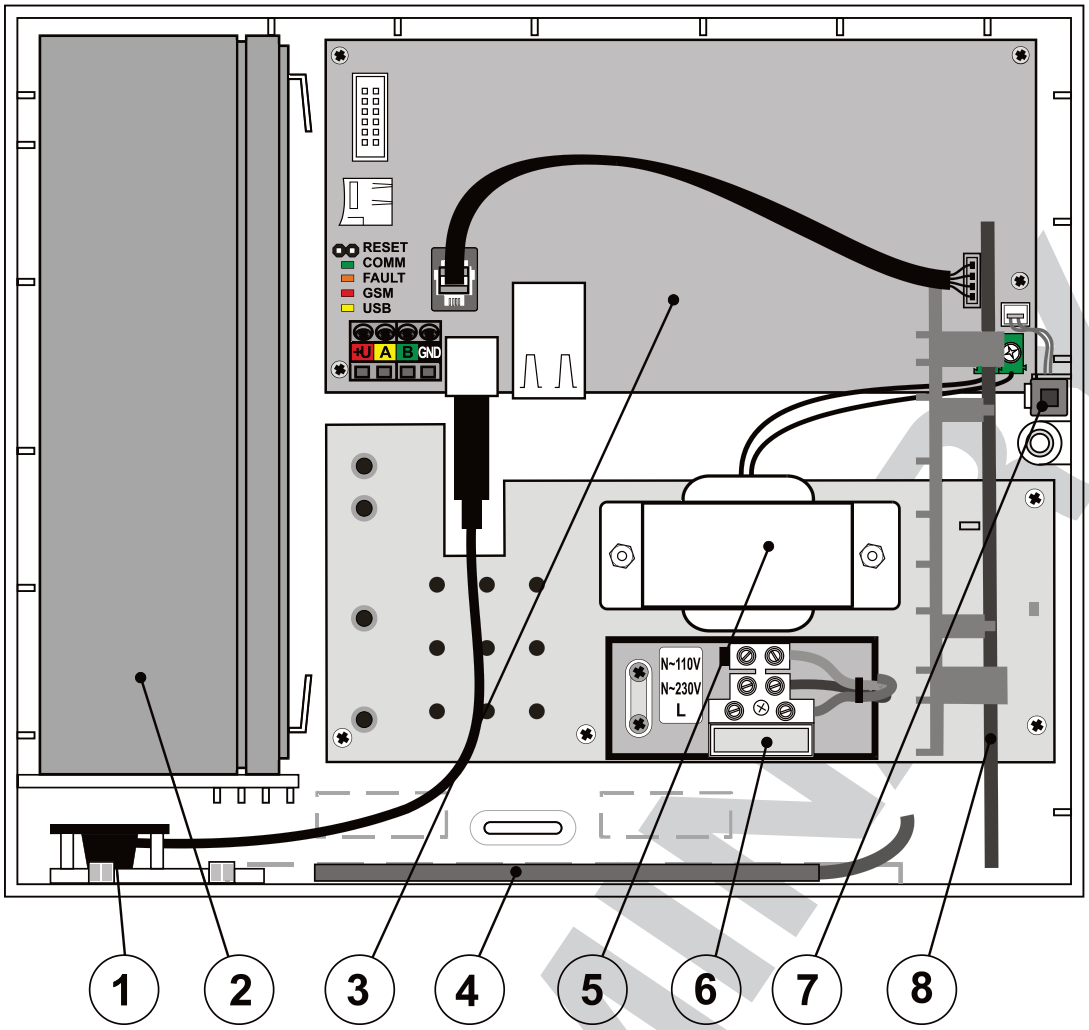
Centralę alarmową JA-100K można dostarczyć także z zainstalowanym modułem radiowym JA-111R w formie zestawu pod nazwą JA-100KR.

Centrala alarmowa JA-100K przeznaczona jest do **małych instalacji MAGISTRALI** oraz **średnich instalacji** z komunikacją bezprzewodową. Centralę alarmową JA-100K wyposażono w komunikator LAN, który można połączyć z internetem, i który umożliwia wysyłanie danych do zabezpieczenia obszarów pamięci masowej, tzw. chmury (zdjęcia wykonywane przez czujki PIR z kamerą lub kamery do weryfikacji zdjęciowej) lub do serwera agencji ochrony, po otrzymaniu wyposażenia technicznego na potrzeby takich danych. Połączenie z internetem pozwala także zapewnić dostęp zdalny za pomocą programu F-Link (J-Link).

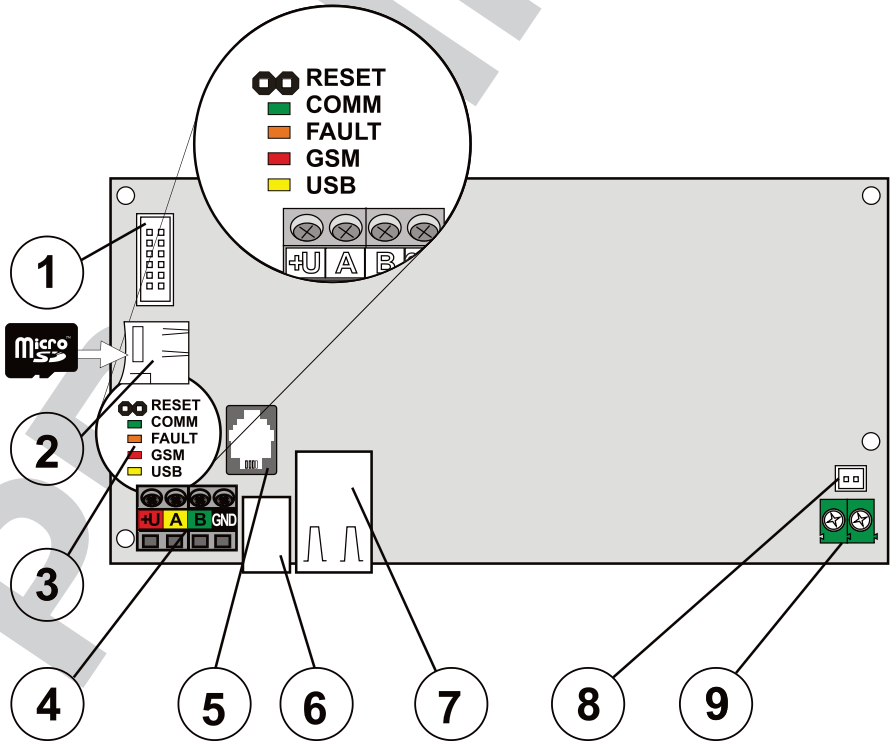
Centralę alarmową można także wyposażyć w moduł JA-190Y, przeznaczony do użytku z siecią dostawcy usług GSM lub w uzupełniający komunikator telefoniczny (PSTN) JA-190X, podłączony do analogowej linii stacjonarnej (np. PSTN) bądź symulowanych linii telefonicznych. Tych modułów nie można używać jednocześnie (na płytce drukowanej znajduje się tylko jedno złącze). Tych modułów uzupełniających można używać do raportowania zdarzeń w systemie, a także w charakterze komunikatora awaryjnego w przypadku, gdy wyżej wymieniony komunikator LAN wskaże błąd (awaria ścieżki komunikacji).



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com




*1 — złącze USB do podłączenia komputera; 2 — Bateria awaryjna 2,6 Ah; 3 — Płytka drukowana centrali alarmowej; 4— Antena GSM uzupełniającego urządzenia do automatycznego wybierania GSM; 5 — Transformator; 6 — Zaciski zasilania sieciowego, bezpiecznik 200 mA; 7 — Styk sabotażu obudowy; 8 — Moduł radiowy;*




*1 — Złącze do modułów uzupełniających (komunikator GSM lub PSTN); 2 — Uchwyt karty MicroSD; 3 — Kontrolki i kabel złączowy resetowania; 4 — Zacisk końcowy MAGISTRALI; 5 — Wewnętrzne złącze MAGISTRALI do modułu JA-11xR; 6 — Złącze kablowe USB; 7 — Złącze LAN, 8 — Wtyki sabotażu pokrywy centrali; 9 — Wejście zasilania z transformatora*

**Części centrali alarmowej JA-100K (wymienne):**

- Karta MicroSD 4 GB i więcej — służy do przechowywania zdarzeń, zdjęć z czujek PIR i kamer

**W celu poszerzenia opcji centrali alarmowej należy wykorzystać:**

- Moduł radiowy JA-111R (domyślnie zainstalowany w zestawie JA-100KR)
- Komunikator PSTN JA-190X
- Komunikator GSM JA-190Y
- Bateria awaryjna SA-214/2,6 Ah

**Do elementów wyposażenia dodatkowego centrali alarmowej należą:**

- 1 szt. Przedłużacz USB (20 cm) zainstalowany w centrali alarmowej
- 1 szt. Bezpiecznik T 0,2 A; 250 V (do ochrony obwodu 230 V)
- 1 szt. Bezpiecznik T 0,4 A; 250 V (do ochrony obwodu 110 V)
- 3 szt. Elementy mocujące 8 mm
- 3 szt. Wkręty 40 mm
- 2 szt. Opaski 100 mm
- Instrukcja instalacji

## 3.2 Kontrolki na płytce centrali alarmowej

Na płytce głównej znajdują się następujące kontrolki:

| Opis | Kolor | Znaczenie |
|---|---|---|
| **COMM** | zielony | Miganie podczas pracy MAGISTRALI komunikacji wskazuje poprawne działanie |
| **BŁĄD** | żółty | Nieprzerwane świecenie wskazuje ogólny błąd w systemie (więcej informacji znajduje się w programie F-Link lub na klawiaturze z wyświetlaczem) |
| **GSM** | czerwony | Wskazanie statusu komunikatora uzupełniającego (GSM lub PSTN) |
| **USB** | żółty | Wskazanie połączenia USB z komputerem |

## 3.3 Dodatkowe złącza na płytce drukowanej centrali

Dodatkowe złącza na płytce drukowanej centrali:

- **Kabel złączowy RESET** na płytce drukowanej, dzięki czemu system można ustawić na domyślne ustawienia fabryczne (jeżeli dopuszcza to parametr „Resetowanie aktywne"). Tę procedurę opisano w rozdziale 12 Reset of the control panel.
- **10-wtykowe złącze** do podłączenia komunikatora uzupełniającego.
- **Złącze RJ (RJ-44)** do podłączenia modułu radiowego JA-111R w przypadku instalacji wewnątrz obudowy centrali alarmowej. Zabrania się korzystania z tego złącza do łączenia urządzeń poza obudową centrali alarmowej.
- **Złącze LAN** do podłączania do internetu
- **2-wtykowe złącze** przeznaczone do łączenia styku sabotażu. Wskazuje wszelkie próby uszkodzenia pokrywy przedniej lub otwarcia centrali alarmowej. Do tej wersji centrali alarmowej nie dołączono tylnego styku sabotażu.

## 3.4 Zaciski łączące na płytce drukowanej centrali alarmowej

Centrala alarmowa systemu zabezpieczeń posiada wymóg stałego podłączenia do zasilania sieciowego (230 V / 50 Hz lub 110 V / 60 Hz). Więcej informacji podano w rozdziale 16 Technical specifications

Zasilanie sieciowe podłącza się za pomocą zacisków z wymiennym bezpiecznikiem. Centrala alarmowa jest urządzeniem o 2. klasie ochronności z podwójną izolacją. Dlatego właśnie wystarczy przewód 2-żyłowy (przewód pod napięciem i zerowy). W przypadku przewodu 3-żyłowego żyłę uziemiającą należy zostawić odłączoną i zaizolować.

**Przestroga:** Nie należy podłączać żyły uziemiającej do zacisków w centrali alarmowej!

Do zasilania centrali alarmowej niskim napięciem i izolacji MAGISTRALI od zasilania sieciowego używa się niewielkiego, ochronnego transformatora zapewniającego izolację. Transformator podłącza się do centrali alarmowej za pomocą małego, zielonego zacisku.

Komunikacja wewnętrzna między centralą alarmową a podłączonymi urządzeniami odbywa się za pośrednictwem MAGISTRALI 4-żyłowej. Do tego celu służy pojedynczy zacisk w czterech kolorach (czerwony, żółty, zielony i czarny).

Wbudowane złącze USB typu B umieszczono na płytkach drukowanych centrali alarmowej. Za pomocą krótkiego przedłużacza można ustanowić połączenie z komputerem przy użyciu przewodu USB bez otwierania centrali alarmowej.

# 4 Przed instalacją systemu

Należy wybrać odosobnione miejsce na centralę alarmową (w obrębie chronionego obszaru), z dostępem do zasilania sieciowego.

Zasilanie sieciowe centrali alarmowej może instalować jedynie osoba posiadająca wymagane kwalifikacje w zakresie elektryki.

Producent nie dopuszcza zasilania centrali alarmowej z alternatywnych źródeł, jak baterie o dużej pojemności ładowane energią słoneczną itp.

Central alarmowa JA-100K posiada zaciski zasilania, pozwalające wybrać jeden z 2 rodzajów sieci zasilających: ~230 V / 50 Hz i ~110 V / 60 Hz. Zależnie od rodzaju instalacji zasilającej należy wykorzystać odpowiedni zacisk przyłączeniowy oraz bezpiecznik, zgodnie z rozdziałem nr 16 Technical specifications.

Zasilanie centrali alarmowej posiada podwójne rozdzielenie obwodów ze względów bezpieczeństwa.
Nie podłącza się żadnego przewodu ochronnego.

Podczas instalacji i podłączania elementów MAGISTRALI należących do centrali alarmowej całe zasilanie centrali alarmowej musi być całkowicie odłączone.

**Producent nie ponosi odpowiedzialności za jakiekolwiek szkody w przypadku nieprawidłowej instalacji lub konfiguracji systemu.**

1. Rozmieszczenie i konfiguracja systemu musi odpowiadać dokumentacji projektowej systemu alarmowego zgodnie ze specyfikacją techniczną CLC/TS 50131-7, ustaleniami z klientem i obowiązującymi normami technicznymi dla instalacji elektrycznych.
2. Należy przygotować zasilanie centrali alarmowej, wykorzystując odpowiedni przewód z podwójną izolacją i przekrojem 0,75 do 1,5 mm². Zaleca się ochronę przepięciową na zasilaniu sieciowym centrali alarmowej. Zaleca się także wykorzystanie pojedynczego przewodu z wyłącznikiem automatycznym (2 A–6 A), pełniącym również funkcję wyłącznika głównego.

   Przestroga: Do tego obwodu nie należy podłączać innych urządzeń elektrycznych, w tym zasilania do zewnętrznych wyjść PG, instalacji grzewczej ani innych urządzeń związanych z funkcjami centrali alarmowej (np. sterowanie ogrzewaniem itp.). Na wyłączniku automatycznym na rozdzielnicy zasilania sieciowego należy umieścić naklejkę „Nie wyłączać”.
3. Zaleca się umieszczenie pewnej ochrony przepięciowej w obwodzie sieciowym na potrzeby centrali alarmowej.
4. Centralę alarmową należy przymocować bezpośrednio do ściany lub innej niepalnej powierzchni. Należy sprawdzić, czy nie ma metalowych przedmiotów, mogących niekorzystnie wpłynąć na przesyłanie i odbiór sygnałów radiowych (moduł radiowy i komunikator GSM). Do przygotowania otworów na elementy mocujące należy użyć dołączonego szablonu. Przełożyć wkręty przez górne otwory w plastikowej obudowie tak, by zachować odstęp 1 cm od ściany, a następnie powiesić na niej obudowę centrali alarmowej. Następnie przełożyć dodatkowy wkręt przez dolny otwór/otwory i wkręcić go w celu stabilizacji położenia centrali alarmowej. Dokręcić wszystkie wkręty.

# 5 Montaż urządzeń MAGISTRALI

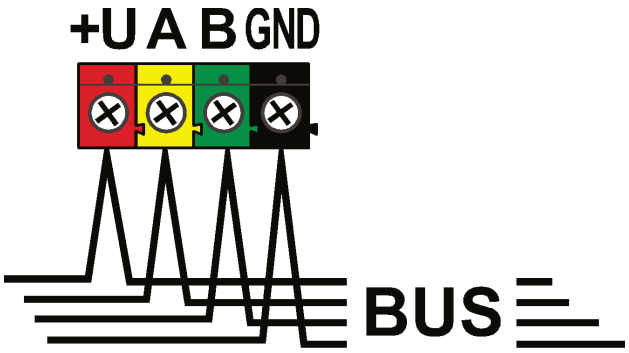
MAGISTRALA systemu JABLOTRON 100 jest przeznaczona do użytku z urządzeniami MAGISTRALI serii JA-1xx. Należy postępować w następujący sposób:

1. Podczas podłączania modułów MAGISTRALI zasilanie centrali alarmowej musi być całkowicie wyłączone (w tym także bateria awaryjna).
2. Należy przestrzegać instrukcji instalacji poszczególnych urządzeń.
3. Przewód MAGISTRALI należy zamontować wewnątrz obszaru chronionego przez system, tj. w ścianach, metalowych rurach, nad sufitem podwieszanym lub w miejscach, do których dostęp jest utrudniony.
4. Jeżeli przewód znajduje się poza obszarem chronionym, tę część należy oddzielić separatorem MAGISTRALI JA-110T. Ten separator należy umieścić w chronionym obiekcie. Przewody zainstalowane poza chronionym obszarem nie są przeznaczone do użytku w systemach zabezpieczeń.
5. Do rozgałęziania instalacji należy wykorzystać rozdzielacz JA-110Z BUS (i/lub JA-110Z-B, JA-110Z-C).
6. Podczas podłączania urządzeń MAGISTRALI należy zwracać uwagę na kolor żył (czerwona, żółta, zielona, czarna).

Urządzenia dostarczone przez innych producentów można podłączyć za pomocą odpowiedniego modułu, np. JA-111H, JA-116H, JA-118M, JA-114HN itp. Producent nie gwarantuje prawidłowego działania podłączonego urządzenia ani klasy jego ochronności.

## 5.1 MAGISTRALA JA-100 BUS

MAGISTRALA systemu JABLOTRON 100 posiada 4 żyły (4-żyłowa). MAGISTRALI nie można dzielić z innym systemem, nawet w celu zasilania różnych urządzeń.




*Listwa zaciskowa MAGISTRALI*

| zacisk | kolor | oznaczenie |
|---|---|---|
| +U | czerwony | dodatni zacisk zasilania; może służyć wyłącznie do zasilania urządzeń serii JABLOTRON 100 |
| A | żółty | dane A |
| B | zielony | dane B |
| GND | GND | zacisk wspólny (ujemny zacisk zasilania) |

## 5.2 Przewody MAGISTRALI

| Opór pary żył zasilających (tam i z powrotem) | | |
|---|---|---|
| **CC-01** | opór pary na 1 m | 0,0754 Ω |
| | opór pary na 10 m | 0,754 Ω |
| | opór pary na 100 m | 7,54 Ω |
| **CC-02** | opór pary na 1 m | 0,1932 Ω |
| | opór pary na 10 m | 1,932 Ω |
| | opór pary na 100 m | 19,32 Ω |
| **CC-11** | opór pary na 1 m | 0,0754 Ω |
| | opór pary na 10 m | 0,754 Ω |
| | opór pary na 100 m | 7,54 Ω |

Urządzenia MAGISTRALI należy podłączyć za pomocą przewodu CC-01, CC-02 lub CC-11 lub równoważnego.

**Przewód CC-01** jest przewidziany do głównej linii MAGISTRALI lub łączenia elementów o wysokim zużyciu (syrena) lub elementów zdalnych. Przewód posiada 4 żyły (kolory odpowiadające kolorowi MAGISTRALI). Żyły zasilające (czarna i czerwona) posiadają większy przekrój rdzenia (0,5 $mm^2$) w porównaniu z przewodami do komunikacji (0,2 $mm^2$). Kabel dostarczamy w opakowaniach (1 opakowanie — 300 m).

**Przewód CC-02** jest przeznaczony do odgałęzień głównej linii MAGISTRALI lub do podłączania elementów o niskim zużyciu (czujek), bądź na krótkie odległości. Przewód posiada 4 żyły (kolory odpowiadające kolorowi MAGISTRALI). Wszystkie żyły przewodu CC-02 posiadają ten sam przekrój rdzenia (0,2 $mm^2$). Kabel dostarczamy w opakowaniach po 300 m.

**Przewód CC-11** jest przewidziany do głównej linii MAGISTRALI lub łączenia elementów o wysokim zużyciu (syrena) lub elementów zdalnych. Przewód posiada 4 żyły (kolory odpowiadające kolorowi MAGISTRALI). Żyły zasilające (czarna i czerwona) posiadają większy przekrój rdzenia (0,5 $mm^2$) w porównaniu z przewodami do komunikacji (0,2 $mm^2$). Przewód dostarczamy w opakowaniach (1 opakowanie — 300 m) i posiada certyfikat bezpieczeństwa pożarowego.

**Układ MAGISTRALI:**

Przewodu MAGISTRALI **nie wolno** łączyć tak, by utworzyć **zamkniętą pętlę** jakiegokolwiek przewodu (końce poszczególnych odgałęzień nie mogą się łączyć; dotyczy to także wspólnego przewodu GND).

## 5.3 Długość MAGISTRALI i liczba podłączonych urządzeń

Maksymalna długość MAGISTRALI bez wzmacniania (separacji) wynosi 500 m. Długość oblicza się jako sumę długości wszystkich przewodów między wszystkimi podłączonymi urządzeniami. Liczbę podłączonych urządzeń MAGISTRALI ogranicza pojemność baterii awaryjnej centrali alarmowej. Aby spełnić warunki normy dotyczącej klasy ochronności 2, w przypadku awarii zasilania sieciowego 230 V system musi niezawodnie

pracować przez co najmniej 12 godzin z zasilaniem ze źródła awaryjnego. Tym samym całkowite zużycie dla wszystkich urządzeń MAGISTRALI nie może przekraczać maksymalnego ciągłego zużycia prądu z centrali alarmowej, patrz rozdział 5.4 Example of the calculation of BUS current consumption to back-up the system. Aby obliczyć całkowite ciągłe zużycie dla podłączonych elementów, należy zsumować ich **zużycie awaryjne** (jest podane w instrukcji lub tabeli zbiorczej, patrz 14.1 Overview table of the current consumption of BUS devices).

Innym parametrem ograniczającym maksymalną długość MAGISTRALI może być strata napięcia na linii (wyraźnie wskazana w Diagnostyce systemu w programie F-Link i J-Link).

## 5.4 Przykładowe obliczenie zużycia MAGISTRALI dla systemu awaryjnego

W tabeli podano przykład niewielkiej instalacji z 5 urządzeniami MAGISTRALI. Całkowite zużycie w trybie jałowym w trybie awaryjnym wynosi 78 mA. Tym samym można wykorzystać centralę alarmową JA-100K, która umożliwia maksymalne stałe obciążenie 125 mA i 85 mA przy aktywnym module LAN.

*Tabela 5*

| Urządzenie | Opis | Liczba sztuk | Zużycie w awaryjnym trybie zasilania |
|---|---|---|---|
| JA-111R | Moduł do komunikacji radiowej | 1 | 25 mA |
| JA-110E | Klawiatura sterująca | 1 | 18 mA |
| JA-110A | Syrena wewnętrzna | 1 | 5 mA |
| JA-111A RB | Zewnętrzna syrena z rozwiązaniem awaryjnym | 1 | 5 mA |
| JA-110N | Moduł wyjścia PG | 1 | 25 mA |
| | | **RAZEM** | **78 mA** |

| Parametr | JA-100K |
|---|---|
| Maksymalne stałe natężenie z MAGISTRALI | 400 mA stale<br>(1000 mA przez 5 min) |
| Maksymalne stałe natężenie dla zasilania awaryjnego na 12 h | 125 mA<br>(przy baterii awaryjnej 2,6 Ah) |

Obliczenie natężenia MAGISTRALI zależnie od konfiguracji sprzętowej centrali alarmowej:

| Bateria awaryjna **2,6 Ah** | **175 mA** maks. natężenie z baterii awaryjnej | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **JA-100K** | 50 | x | x | x | x | x | x | x | x | x | X | x | x |
| **JA-111R** | 30 | | x | x | x | x | | | | | | x | x |
| **LAN** | 40 | | | x | x | x | x | x | x | | | | |
| **JA-190Y** | 25 | | | | x | | | x | | x | | x | |
| **JA-190X** | 15 | | | | | x | | | x | | X | | x |
| Maks. natężenie pobrane z MAGISTRALI przez czas zasilania awaryjnego 12 h (mA) | | **125** | **95** | **55** | **30** | **40** | **85** | **60** | **70** | **100** | **110** | **70** | **80** |

## 5.5 Wymogi dotyczące zasilania

System zabezpieczeń musi posiadać klasę ochronności 2 i wymaga zasilania awaryjnego z baterii awaryjnej przez 12 h (zgodnie z normą EN 50131-1) i 24 h (zgodnie z INCERT T 031) podczas awarii zasilania sieciowego, przy czym pełne naładowanie baterii musi być możliwe w ciągu 72 h (zgodnie z EN 50131-1) i 48 h (zgodnie z INCERT T 031) po przywróceniu zasilania sieciowego.

Aby spełnić ten wymóg, należy zapewnić baterię awaryjną o odpowiedniej pojemności na wymagany czas, patrz poniższy przykład. Pojemność znamionową baterii należy sprawdzić, patrz specyfikacja techniczna CLC/TS 50131-7, testy systemu.

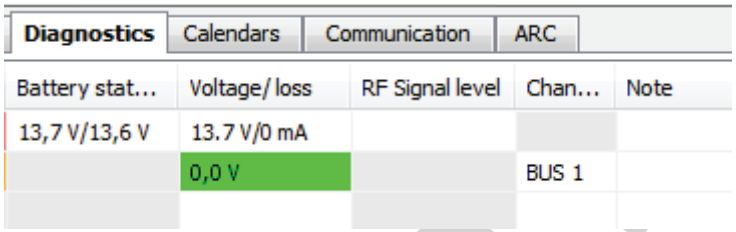
Obliczenie maksymalnego stałego natężenia pobieranego z MAGISTRALI systemu zgodnie z pojemnością baterii awaryjnej:

**Centrala alarmowa JA-100K**, dla baterii 2,6 Ah(obliczenie dotyczy 80% pojemności baterii)

**2,6 Ah** * 0,8 / 12 h = 0,17 A (zależnie od pojemności — maksymalne natężenie na 12 godzin)

Imax = 0,17 A – 0,05 A = **0,12 A** (odjąć natężenie własne centrali alarmowej 0,05 A)

Natężenie pobrane z każdego zacisku wyjściowego MAGISTRALI przedstawia program F-Link w zakładce Diagnostyka w wierszu 0, gdzie znajduje się centrala alarmowa. Pokazane natężenie należy uwzględnić przede wszystkim w przypadku wykorzystania modułu JA-111R (bezprzewodowa centrala alarmowa) połączonego ze specjalnym złączem RF, a tym samym należy dodać także natężenie tego modułu. To natężenie należy porównać z obliczonym natężeniem i wskazuje ono, czy pojemność baterii awaryjnej pozwoli spełnić normatywne wymogi dotyczące czasu zasilania awaryjnego systemu. Jeżeli zmierzone natężenie jest wyższe od obliczonego, bateria awaryjna powinna mieć większą pojemność.




# 6 Wykorzystanie urządzeń bezprzewodowych

W systemie JA-100 można używać urządzeń bezprzewodowych serii JA-1xx. Centralę alarmową należy wyposażyć w co najmniej jeden moduł radiowy JA-111R, przy czym w systemie można używać najwyżej 3 modułów radiowych.

Podczas instalacji poszczególnych urządzeń należy przestrzegać instrukcji podanych w odpowiadających im instrukcjach obsługi.

## 6.1 Instalacja modułu radiowego JA-111R

1. Zestaw JA-100KR posiada wbudowany moduł radiowy JA-111R w obudowie centrali alarmowej obok transformatora, w specjalnym uchwycie z tworzywa.
2. Jeżeli centralę alarmową zainstalowano w miejscu o słabym odbiorze sygnału GSM, moduł GSM zwiększy
   jego moc transmisji, co może niekorzystnie wpłynąć na zasięg komunikacji modułu radiowego. W takim przypadku zaleca się umieszczenie modułu radiowego poza centralą alarmową, co najmniej 2 m od niej, gdzie nie będzie dotknięty niekorzystnym wpływem i będzie posiadał wyższej jakości odbiór radiowy sygnałów z urządzeń, co umożliwi większy zasięg, a tym samym odległość między elementami. Moduł JA-111R należy umieścić poza obudową centrali alarmowej w obrębie skrzynki instalacyjnej PLV-111R (nie wchodzi w skład zestawu JA-100K, należy ją zamówić oddzielnie).

   **Złącze MAGISTRALI RJ na płytce centrali alarmowej przeznaczone jest wyłącznie do podłączania modułu radiowego zainstalowanego wewnątrz obudowy centrali alarmowej.**
3. Aby objąć większy obszar sygnałem radiowym, można zamontować najwyżej 3 moduły radiowe JA-11xR w ich własnej plastikowej obudowie w różnych miejscach (np. każdy na innym piętrze). Sygnały z urządzenia bezprzewodowego (tu za urządzeniem) może odbierać większa liczba modułów radiowych jednocześnie. Centrala alarmowa komunikuje się cyklicznie z poszczególnymi modułami radiowymi, dzięki czemu uzyskuje informacje wysłane przez urządzenie z modułu radiowego, który jako pierwszy otrzymał nieuszkodzony sygnał, i na niego reaguje. Następnie nie otrzyma tej samej informacji z innych modułów radiowych, nawet jeśli odebrały ją przy silnym sygnale. Tym samym może się zdarzyć, że sygnały z tego samego urządzenia jednokierunkowego mogą wskazywać całkiem różne dane w programie F-Link / Ustawienia systemu / Diagnostyka podczas kilku pomiarów, zależnie od tego, z którego modułu pochodzi dany sygnał. W odniesieniu do urządzeń jednokierunkowych centrala alarmowa „rezerwuje" raz użyty kanał (komunikacja z pierwszym modułem radiowym) i później komunikuje się z konkretnym urządzeniem wyłącznie przy pomocy tego modułu radiowego (jak pokazano w zakładce Diagnostyka, kolumna Kanał) dopóki urządzenie nie przestanie odpowiadać. Następnie szuka sygnału połączenia w innych modułach radiowych. W przypadku konieczności weryfikacji jakości połączenia poszczególnych urządzeń z poszczególnymi modułami radiowymi należy ją sprawdzić na podstawie wykresu sygnału RF w programie F-Link (przycisk na górnym pasku narzędziowym). Tam należy wybrać moduł radiowy, dla którego trzeba sprawdzić komunikację, i aktywować urządzenia do sprawdzenia. Wykres komunikacji radiowej wskazuje siłę sygnału RF mierzonego przez konkretny moduł radiowy. Można także otworzyć kilka okien sygnału RF, dzięki czemu można bez trudu monitorować zasięg radiowy w danym obiekcie.
4. Moduł radiowy należy zainstalować pionowo na ścianie. Nie należy go umieszczać w pobliżu obiektów, które przesłaniają lub zakłócają komunikację (metalowych, urządzeń elektronicznych, przewodów, rurociągów itp.).



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

5. Po włączeniu systemu **należy najpierw przypisać moduły radiowe.** Dopiero wówczas można przypisać urządzenia bezprzewodowe.
6. Zalecenie: Zaleca się przypisywanie urządzeń bezprzewodowych do systemu po ich umieszczeniu w położeniu docelowym. Procedura instalacji nie jest tak wygodna, ale pomaga uzyskać lepszy i niezawodny odbiór radiowy w module radiowym. Moduł radiowy posiada algorytm, który zapewnia „minimalny sygnał" z urządzenia, mierzony w trybie serwisowym. To zapewnia rezerwę na wypadek pogorszenia warunków radiowych w pełnym trybie pracy (np. w przypadku zmiany konfiguracji budynku, zakłóceń przemysłowych itp.). Więcej szczegółów znajduje się w normie EN 50131-5-3.

## 6.2 Instalacja urządzeń bezprzewodowych — tryb przypisywania

Urządzenia bezprzewodowe wymagają indywidualnego przypisywania do systemu. Procedurę przypisywania można przeprowadzić w trybie przypisywania za pomocą komputera z zainstalowanym programem F-Link. Patrz rozdział 8.4.1 Enrolling and erasing devices.

# 7 WŁĄCZANIE systemu

1. Sprawdzić połączenie przewodów MAGISTRALI.
2. Zweryfikować obecność karty microSD w uchwycie na płytce centrali alarmowej.
3. Sprawdzić poprawność podłączenia przewodu zasilania sieciowego do centrali alarmowej oraz stabilność podłączenia przewodu zasilającego.
4. Umieścić baterię w centrali alarmowej i zamocować ją w obudowie (za pomocą taśmy samoprzylepnej lub paska).
   **Przestroga — baterię awaryjną dostarczamy w stanie naładowanym, nie wolno dopuścić do zwarcia!**
5. Podłączyć przewody zasilające baterii. Zwrócić uwagę na prawidłowe podłączenie biegunów (czerwony +, czarny -).
6. Włączyć zasilanie sieciowe i sprawdzić kontrolki na centrali alarmowej:
   a. zielona dioda zaczyna migać (funkcja MAGISTRALI)
   b. czerwona dioda miga — logowanie do sieci GSM przez uzupełniający komunikator GSM
   c. czerwona dioda GSM gaśnie — komunikator GSM jest zalogowany do sieci GSM
   d. czerwona dioda świeci — centrala alarmowa nie zalogowała się do sieci GSM
7. Kiedy podłączone urządzenia MAGISTRALI zaczną migać na żółto, należy je podłączyć do systemu, patrz rozdział 8.4.1 Enrolling and erasing devices.
8. Należy przeprowadzić konfigurację klawiatur, patrz rozdział 10.3.1 Keypad configuration.
9. Skonfigurować niezbędne funkcje i sprawdzić system, patrz rozdział 10.7 Parameters tab.

# 8 Konfiguracja systemu

System zabezpieczeń (chroniony obiekt — budynek) można podzielić na niezależne części, czyli strefy. Każdą strefę można chronić w całości lub jedynie w części. Nazywa się to uzbrojeniem częściowym. Czujki z aktywnym parametrem „Wewnętrzny" nie zapewniają ochrony w takim trybie.

Podstawową część stanowi **ochrona terenu**. Dotyczy to ochrony głównego wejścia, bramy garażowej, okien, drzwi balkonowych, a także drzwi tylnych i wejść dachowych. Wśród urządzeń przewidzianych do ochrony terenu znajdują się czujki magnetyczne, czujki zbicia szyby, czujki wstrząsów / wychylenia, a także bariery na podczerwień. Należy pamiętać jedynie o tym, że główne drzwi wejściowe i brama garażowa zwykle posiadają opóźnienie na wejście, a pozostałe strefy definiuje się jako posiadające reakcję natychmiastową.

Poniższa część dotyczy **Czujek ruchu**. Czujki ruchu (PIR) lub ich połączenia z innymi czujkami śledzą ruch w chronionym obiekcie. Czujki umieszczone przy wejściu do obiektu zwykle posiadają zadaną reakcję z opóźnieniem lub następną reakcję z opóźnieniem. Pozostałe czujki ruchu zwykle ustawia się na reakcję natychmiastową. Do stworzenia ścieżek wejściowych (np. dłuższe opóźnienie w przypadku wejścia przez garaż) można wybrać najwyżej 2 zegary.

**Ochrona obiektu** zapewnia bezpieczeństwo sejfów i kosztowności, ale także wykrywanie włamanie z użyciem siły. Drzwi garażowe można zniszczyć bez otwarcia. W skład zabezpieczeń **obiektu** wchodzą czujki wstrząsów i wychylenia, ale można uwzględnić także czujki magnetyczne do wykrywania otwarcia drzwi, zwykle jest to czujka z reakcją opóźnioną.

Ochronę poszczególnych elementów zabezpieczeń realizują styki sabotażu wskazujące obsługę urządzenia przez osobę nieuprawnioną.

**Ochrona środowiska** to przede wszystkim czujki pożaru, czujki do wykrywania gazów palnych i trujących, oraz czujki zalania. Wszystkie wymienione czujki posiadają regulowaną reakcję, niezależną od statusu systemu lub po prostu reakcję 24 h.

## 8.1 Profile systemu

Gama profili systemu umożliwia globalną konfigurację następujących parametrów systemu (zakładka F-Link / Parametry) w celu modyfikacji zachowania systemu tak, by spełniało wymogi określonej normy i zapewniało wymaganą klasę ochronności. Te opcje można zablokować przy wyborze określonego profilu do zmiany.

***Przestroga**: ustawienie poszczególnych parametrów przez wybór profilu systemu nie gwarantuje, że zainstalowany system zapewni klasę ochronności 2. Klasę ochronności 2 może zapewnić jedynie prawidłowy projekt systemu (wykorzystanie odpowiednich urządzeń) oraz poprawny montaż zgodnie z wymogami CLC/TS 50131-7 oraz wdrożenie usługi SMA. Klasyfikacja centrali alarmowej JA-100K i poszczególnych urządzeń systemu JABLOTRON 100 do klasy ochronności 2 stanowi po prostu podstawowe dane wejściowe i zgodnie z tym można ustawić klasę ochronności chronionego obiektu.*



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

**Przegląd parametrów systemu z uwzględnieniem ustawienia profilu systemu:**

| Urządzenie | Profil / Parametr | DOMYŚLNY | | EN50131-1, Klasa 2 | | INCERT | |
|---|---|---|---|---|---|---|---|
| | | Opcja aktywna | Blokowanie | Opcja aktywna | Blokowanie | Opcja aktywna | Blokowanie |
| Centrala alarm. | Syrena przy uzbrojeniu częściowym (IW) | NIE | NIE | NIE | NIE | NIE | NIE |
| Centrala alarm. | Syreny aktywne | TAK | NIE | TAK | TAK | TAK | TAK |
| Centrala alarm. | Usługa ograniczona do Administratora/prawa SMA | NIE | NIE | TAK | TAK | TAK | TAK |
| Centrala alarm. | Serwis i SMA steruje systemem | TAK | NIE | NIE | TAK | NIE | TAK |
| Centrala alarm. | Antynapadowa kontrola dostępu | TAK | NIE | TAK | NIE | TAK | NIE |
| Centrala alarm. | Potwierdzenie alarmu w jednej strefie | NIE | NIE | NIE | NIE | NIE | NIE |
| Centrala alarm. | Syrena (wyjście IW) przy aktywacji sabotażu | NIE | NIE | TAK | TAK | TAK | TAK |
| Centrala alarm. | Reset aktywny | TAK | NIE | NIE | TAK | NIE | TAK |
| Centrala alarm. | Zgłoś nieuzbrojoną strefę | NIE | NIE | NIE | NIE | NIE | NIE |
| Centrala alarm. | Niepowodzenie uzbrojenia | NIE | NIE | TAK | TAK | TAK | TAK |
| Centrala alarm. | Sygnalizacja pamięci alarmów | TAK | NIE | NIE | TAK | NIE | TAK |
| Centrala alarm. | Opóźniony raport do SMA | NIE | NIE | TAK | NIE | TAK | NIE |
| Centrala alarm. | Sposoby uzbrajania | Zgodnie z profilem systemu | NIE | Zgodnie z profilem systemu | TAK | Zgodnie z profilem systemu | TAK |
| Centrala alarm. | Typ uwierzytelniania | Standardowy | NIE | Standardowy | NIE | Standardowy | NIE |
| Centrala alarm. | Utrata urządzenia MAGISTRALI | Błąd | NIE | Sabotaż zawsze | NIE | Sabotaż zawsze | NIE |
| Centrala alarm. | Długość alarmu | 240 | 90..1200 | 240 | 90…900 | 240 | 90…900 |
| Centrala alarm. | Opóźnienie na wejście | 30 | 5...120 s | 30 | 5…30 s | 30 | 5…30 s |
| Centrala alarm. | Opóźnienie na wyjście | 30 | 5...120 s | 30 | 5...60 s | 30 | 5...60 s |
| Centrala alarm. | Opóźnienie na wejście bramą garażową | 60 | 5...360 s | 30 | 5…30 s | 30 | 5…30 s |
| Centrala alarm. | Opóźnienie na wyjście bramą garażową | 60 | 5...360 s | 60 | 5...60 s | 60 | 5...60 s |
| Moduł radiowy | Wykrywanie zagłuszania RF | Nieaktywna | NIE | Niska | NIE | Niska | NIE |
| Klawiatura | Ustawienia sygnalizacji optycznej | 1.(MAGISTRALA) lub 4.(RF) | NIE | 2.(MAGISTRALA) lub 4.(RF) | TAK | 2.(MAGISTRALA) lub 4.(RF) | TAK |
| Klawiatura | Sygnalizuj status ROZBROJONY | TAK | NIE | NIE | NIE | NIE | NIE |
| Klawiatura | Sygnalizuj status UZBROJONY | TAK | NIE | NIE | NIE | NIE | NIE |
| Syrena | Ostrzeżenie (Sygnalizacja dźwiękowa) | NIE | NIE | TAK | TAK | TAK | TAK |
| Syrena | Utrata komunikacji | NIE | NIE | TAK | TAK | TAK | TAK |
| Syrena | Ostrzeżenie (Sygnalizacja optyczna) | NIE | NIE | TAK | TAK | TAK | TAK |

Ustawienie „Domyślny” profil systemu przywraca wszystkie powyższe parametry do zadanych ustawień fabrycznych
i wszystkie parametry można zmienić. System alarmowy nie spełnia wówczas wymogów klasy ochronności 2 i narusza również wymogi ustanowione przez firmę ubezpieczeniową lub przepisy lokalne. W przypadku jakiejkolwiek szkody firma ubezpieczeniowa nie musi wypłacać odszkodowania w związku z nieprawidłowym zaprogramowaniem systemu przez firmę instalacyjną.

**Globalny przegląd przyczyn uniemożliwiających konfigurację zgodnie z zadanym profilem systemu:**

| Zdarzenie / Profil | Domyślny | | EN50131-1, klasa 2 | | INCERT, klasa 2 | |
|---|---|---|---|---|---|---|
| | Dopuszczalne | Niedopuszczalne | Dopuszczalne | Niedopuszczalne | Dopuszczalne | Niedopuszczalne |
| Aktywny sabotaż | ☑ | | | ☑ | | ☑ |
| Aktywne wejście (dowolne wejście) | | | | | ☑ | |
| Aktywne wejście natychmiastowe | ☑ | | ☑ | | ☑ | |
| Aktywna sygnalizacja pamięci alarmów | | | | ☑ | | ☑ |
| Urządzenie RF nie reaguje przez 20 min | | | ☑ | | ☑ | |
| Błąd syreny | | | | ☑ | | ☑ |
| Błąd | ☑ | | ☑ | | | ☑ |
| Utrata urządzenia | ☑ | | ☑ | | | ☑ |
| Niski poziom baterii w urządzeniu | ☑ | | ☑ | | | ☑ |
| Niski poziom baterii w centrali alarmowej | ☑ | | ☑ | | | ☑ |
| Awaria baterii w centrali alarmowej | ☑ | | | ☑ | | ☑ |
| Awaria prądu stałego | | | ☑ | | ☑ | |
| Awaria prądu stałego przez 30 minut | ☑ | | ☑ | | | ☑ |
| System w trakcie konfiguracji | | | | ☑ | | ☑ |
| Błąd GSM | ☑ | | ☑ | | | ☑ |
| Błąd LAN | ☑ | | ☑ | | | ☑ |
| Błąd PSTN | ☑ | | ☑ | | | ☑ |
| Błąd we wszystkich SMA | | | | ☑ | | ☑ |

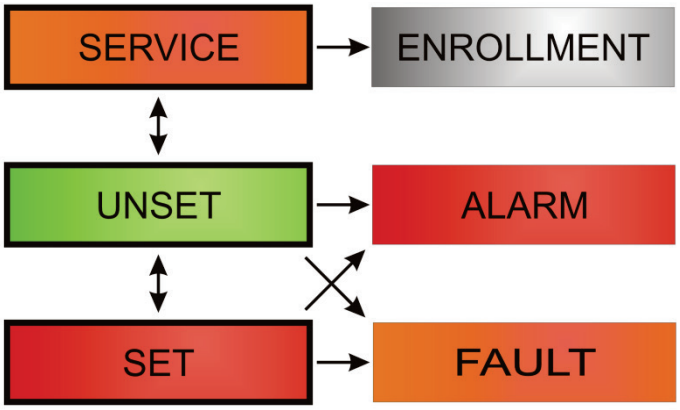


JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

## 8.2 Tryby pracy centrali alarmowej

System zabezpieczeń posiada kilka trybów pracy. Przełączanie między trybami zależy od poziomów autoryzacji użytkowników.

| TRYB | Opis |
|---|---|
| **SERWISOWY (+ Tryb przypisywania)** | Tryb, w którym nie można aktywować alarmu. Jest przeznaczony wyłącznie dla serwisanta lub serwisanta SMA, i służy do przypisywania nowych urządzeń oraz konfiguracji systemu. W tym trybie nie ma możliwości sterowania (lokalnie ani zdalnie). Przyciski funkcji na klawiaturach są wyłączone, a tryb sygnalizuje miganie żółtej diody w przycisku sygnalizacji systemu (2 mignięcia co 2 sekundy). Sygnały z pilotów i innych urządzeń są ignorowane. W tryb serwisowy można wejść, lub go opuścić, za pomocą klawiatury LCD lub komputera w programie F-Link. W przypadku komputera połączonego z internetem nie można wejść w tryb serwisowy ani go opuścić za pomocą klawiatury. |
| **ROZBROJONY** | Zwykły tryb, w którym czujki włamania nie zapewniają ochrony. Można się swobodnie poruszać po obiekcie, otwierać okna i drzwi. Czujki środowiskowe (dym / temperatura, czujki wycieku gazu lub zalania) oraz przyciski panika cały czas mogą uruchomić alarm. Również styki sabotażu wszystkich urządzeń zapewniają ochronę, a w przypadku ich aktywacji system uruchamia alarm sabotażu. Tryb rozbrojony sygnalizuje na klawiaturze zielone światło specjalnej kontrolki statusu (litery A–D) i przycisk sygnalizacji. |
| **UZBROJONY** (całkowicie lub częściowo) | Wszystkie czujki są aktywne i zapewniają ochronę (z wyjątkiem czujek wewnętrznych w przypadku uzbrojenia częściowego), a ich aktywacja powoduje uruchomienie alarmu (kolejny punkt) Tryb uzbrojony sygnalizuje na klawiaturze czerwone światło (żółte światło w przypadku uzbrojenia częściowego) na specjalnej kontrolce statusu (litery A–D) i przycisk sygnalizacji. |
| **ALARM** | Alarm to stan, kiedy przez zadany czas (długość alarmu) aktywują się wyjścia IW i EW i rozlega się dźwięk syren wewnętrznych i zewnętrznych. Stan alarmowy sygnalizuje na klawiaturze szybkie miganie czerwonej kontrolki systemu. Opis różnic między zachowaniem wyjścia EW i IW znajduje się w rozdziale 8.5 Types of alarms. |
| **BŁĄD** | Błąd to sygnał ostrzegawczy systemu, który wskazuje nieprawidłowy stan centrali alarmowej, komunikatorów lub urządzeń, oraz problemy z ich zasilaniem (zasilanie sieciowe lub z baterii) bądź z komunikacją. |



## 8.3 Uwierzytelnianie użytkowników

Każda osoba, która może sterować systemem zabezpieczeń lub dokonywać jakichkolwiek ustawień, nazywana jest Użytkownikiem systemu. Pierwszy zadany użytkownik, z niemal najwyższymi uprawnieniami, którego nie można usunąć, nazywa się kodem serwisowym. Drugi zadany kod, którego nie można usunąć, nazywa się Administratorem głównym. Pozostałych użytkowników, których można dodawać, można po prostu usunąć, a ich uprawnienia można zmieniać zależnie od potrzeb.

| Uwierzytelnianie kodem | Opis typu |
|---|---|
| **Kod SMA** | 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 lub karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych. Liczbę kodów SMA ogranicza wyłącznie wolne miejsce w centrali alarmowej. Liczbę kodów SMA w systemie ogranicza wyłącznie pozostałe miejsce w centrali alarmowej, i żaden kod SMA nie jest domyślnie zadany. |
| **Kod serwisowy (serwis)** | 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 użytkownika z pozwoleniem SMA, innych serwisantów, Administratorów oraz innych użytkowników o niższym poziomie uprawnień, a także przypisać im kody dostępu, breloki lub karty RFID. Liczbę kodów serwisowych ogranicza wyłącznie wolne miejsce w centrali alarmowej. Otrzymuje pozycję 0 i nie można jej zmienić. Domyślny kod serwisowy to 1010, a przy włączonym profilu EN jest to 101010. Kodu nie można skasować. |
| **Administrator (Główny)** | 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, chipy lub karty RFID. Posiada pozwolenie na kasowanie 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. Otrzymuje pozycję 1 i nie można jej zmienić. Domyślny kod Administratora to 1234, a przy włączonym profilu EN jest to 123456. Kodu nie można skasować. |
| **Administrator (Inny)** | Posiada dostęp do stref zaznaczonych przez Administratora głównego, do których drugi Administrator może dodawać nowych użytkowników o tym samym lub niższym poziomie uprawnień do sterowania strefami i wyjściami PG, przypisywać im kody dostępu, breloki lub karty RFID. Posiada pozwolenie na kasowanie pamięci alarmów w przypisanych strefach. Kiedy opcja „Usługa ograniczona do administratora/prawo SMA" jest aktywna, kod administratora wymaga uwierzytelnienia, by potwierdzić dostęp. Liczbę kodów Administratora (innego) ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie. |
| **Użytkownik** | Ten kod umożliwia dostęp do praw sterowania strefami i PG przydzielonymi przez Administratora. Użytkownicy mogą dodać/usunąć własne breloki RFID i karty dostępu, a także zmienić numery telefonów. 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 alarmowej. Nie ma kodu ustawionego fabrycznie. Użytkownik nie może edytować ani kasować własnego kodu dostępu. |
| **Uzbrojona** | Ten kod umożliwia wyłącznie uzbrajanie wyznaczonej strefy. Użytkownicy o tym poziomie autoryzacji nie mogą zmieniać własnego kodu ani kasować pamięci alarmów. Liczbę kodów Uzbrajania ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie. |
| **Wyłącznie PG** | Pozwala użytkownikowi sterować wyjściami programowalnymi wyłącznie na podstawie uwierzytelniania. Dotyczy to zarówno włączania, jak i wyłączania. Użytkownicy o tym poziomie autoryzacji nie mogą zmieniać własnego kodu ani kasować pamięci alarmów. Liczbę kodów Wyłącznie PG ogranicza jedynie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie. |
| **Panika** | 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 alarmowej. Nie ma kodu ustawionego fabrycznie. |
| **Kod ochrony** | Jest to kod przeznaczony dla agencji ochrony. Poziom autoryzacji umożliwia uzbrajanie całego systemu. Jednakże kod ochrony 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 ochrony ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie. |
| **Kod odblokowania** | 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 alarmowej. Nie ma kodu ustawionego fabrycznie. |

Tworzenie nowych użytkowników i administrowanie ich poziomem uwierzytelnienia odbywa się w programie F-Link.

## 8.4 Opcjonalne parametry systemu (F-Link, zakładka Parametry).

**Syrena przy uzbrojeniu częściowym (IW)** — ta funkcja umożliwia aktywację syren wewnętrznych podczas alarmu włamania (nie jest związana z alarmem pożaru ani 24 h) przy częściowym uzbrojeniu systemu.

**Syreny aktywne** — aktywuje wszystkie syreny MAGISTRALI i bezprzewodowe w systemie. Przeznaczona do wyłączania alarmu dźwiękowego podczas testów systemu.

**Administrator — ograniczone prawa serwisowe / SMA** — uwierzytelnienie administratora (kod w pozycji 1) jest niezbędne, by serwisant SMA lub serwisant uzyskał dostęp do systemu. W przypadku dostępu zdalnego serwisanta do systemu za pośrednictwem programu F-Link administrator dokonać uwierzytelnienia przy użyciu klawiatury w budynku. W przypadku lokalnego połączenia przez serwisanta z centralą alarmową przy pomocy przewodu USB administrator może dokonać własnego uwierzytelnienia, korzystając z menu głosowego, pod warunkiem podłączenia komunikatora GSM.

**Serwis i SMA steruje systemem** — Ta funkcja pozwala serwisantom i serwisantom SMA sterować (Uzbrój / rozbrój) wszystkimi sekcjami oraz wyjściami PG (WŁ./WYŁ.) wymagającymi uwierzytelnienia.

**Antynapadowa kontrola dostępu** — Ta funkcja uruchamia cichy alarm panika wyłącznie przez uwierzytelnienie lub podczas sterowania systemem (uzbrajanie, rozbrajanie, PG), kiedy użytkownik odczuwa jakąkolwiek presję ze strony intruza. Alarm panika można uruchomić podczas sterowania systemem przez dodanie „1” do ostatniej cyfry kodu. Kiedy ostatnią cyfrą kodu użytkownika jest 9, podczas antynapadowej kontroli dostępu należy wpisać na ostatnim miejscu cyfrę 0.

**Potwierdzenie alarmu w jednej strefie** — W przypadku ustawienia dla czujki reakcji potwierdzającej ze strony innej czujki taką opcję potwierdzenia można wykorzystać do ograniczenia potwierdzenia **wyłącznie do jednej** strefy (w przeciwnym razie alarm może potwierdzić czujka z dowolnej innej strefy). Dotyczy to zarówno czujek włamania, jak i czujek pożaru.

**Syrena (wyjście IW) przy aktywacji sabotażu** — Syreny z reakcją IW sygnalizują dźwiękowo alarm sabotażu w przypadku strefy rozbrojonej lub częściowo uzbrojonej. Syreny zawsze sygnalizują przy całkowitym uzbrojeniu systemu (strefy).

**Reset aktywny** — Możliwość zablokowania resetowania centrali alarmowej za pomocą złącza na płytce. W przypadku utraty kodu serwisowego przy nieaktywnej opcji resetowania centralę alarmową może odblokować wyłącznie producent. Resetowanie centrali alarmowej opisano w rozdziale 12 Reset of the control panel.

**Zgłoś rozbrojoną strefę** — System zgłasza strefę rozbrojoną w przypadku braku wykrycia ruchu przez 16 godzin.

**Niepowodzenie uzbrojenia** —Funkcja przetwarzana podczas każdego uzbrajania. W przypadku uruchomienia alarmu natychmiastowego w ciągu czasu na wyjście lub otwarcia alarmu opóźnionego po upływie czasu na wyjście nie dojdzie do uzbrojenia systemu i uruchomi się zdarzenie „Niepowodzenie uzbrajania”, które zostanie zapisane w historii. W przypadku wykorzystania uzupełniającego komunikatora GSM to zdarzenie zostanie zgłoszone także za pomocą SMS na numer zadanego użytkownika, pod warunkiem aktywacji zdarzenia „SMS o niepowodzeniu uzbrojenia”. Wskazują je klawiatury oraz syrena zewnętrzna. Aby anulować sygnalizację niepowodzenia uzbrojenia, należy nacisnąć „Anuluj ostrzeżenie” w menu klawiatury LCD.

**Sygnalizacja pamięci alarmów** — Sygnalizacja alarmu przez wbudowaną diodę w czujce, która uruchomiła alarm. Dostępna w urządzeniach obsługujących tę funkcję.

**Sposoby uzbrajania** — Wybór sposobu, w jaki system realizuje uzbrajanie systemu z aktywnym urządzeniem lub błędem w systemie. Od najniższego poziomu system zawsze uzbraja się niezależnie od aktywnych urządzeń lub błędów do najwyższego poziomu, gdzie nie można go uzbroić przy aktywnym urządzeniu (alarm natychmiastowy).

**Typ uwierzytelniania** — Wybór sposobu, w jaki system przetwarza uwierzytelnienie użytkownika. Od Uwierzytelnienia standardowego (tylko kod lub karta) przez potwierdzenie karty RFID kodem (jeżeli użytkownikowi przypisano oba) do podwójnego uwierzytelnienia, co oznacza obowiązkowe stosowanie karty i kodu. Potwierdzenie kodu użytkownika kartą w celu ograniczenia ryzyka nieuprawnionego dostępu lub sterowania przez osoby trzecie.

**Utrata urządzenia MAGISTRALI** — Centrala alarmowa przetwarza utratę urządzenia lub zwarcie w MAGISTRALI systemu. Zależnie od wybranej opcji zareaguje, uruchamiając Błąd lub alarm sabotażu przy każdej utracie urządzenia lub uruchamiając alarm sabotażu po potwierdzeniu utraty innych urządzeń.

### 8.4.1 Przypisywanie i kasowanie urządzeń

Zainstalowane urządzenie (czujka, klawiatura, syrena, brelok itp.) będzie działać dopiero po przypisaniu go do pozycji (adresu) w systemie. Po przypisaniu niektóre urządzenia zajmują kilka pozycji (wejścia o wielu magnesach, multiplikatory wejść). Istnieją także urządzenia (moduły wyjść PG, kontrolki stanu, separatory MAGISTRALI i rozdzielacze), które nie wymagają przypisania do żadnej pozycji. Szczegółowe informacje znajdują się w instrukcji obsługi danego urządzenia.

1. Do przypisywania urządzenia służy program F-Link, zakładka Urządzenia, przycisk **Enroll** (przypisz). Przypisywanie
   **jest możliwe wyłącznie w trybie serwisowym.**
2. Urządzenie można przypisać na kilka sposobów:

a. **Przez naciśnięcie przycisku sabotażu urządzenia MAGISTRALI = zamknięcie pokrywy** (niektóre urządzenia można przypisać naciśnięciem klawisza — patrz instrukcja obsługi danego urządzenia).

b. **Przez podłączenie baterii do urządzenia bezprzewodowego** — najpierw należy jednak przypisać co najmniej jeden moduł radiowy. W przypadku pilotów typu JA-186J podłączenie baterii można zastąpić naciśnięciem i przytrzymaniem dwóch przycisków (tworzących parę). Piloty typu JA-154Jx przypisuje się naciśnięciem dowolnego przycisku.

c. **Przez wprowadzenie numeru seryjnego w polu kodu produktu SN** (znajduje się pod kodem paskowym na płytce wewnątrz urządzenia, np. 1400-00-0000-0123). Numer można odczytać także optycznym czytnikiem kodów paskowych. Następnie należy uruchomić czujkę, by sprawdzić, czy została przypisana.

d. **Przez selektywne ładowanie nieprzypisanych urządzeń MAGISTRALI** — w przypadku braku przypisania co najmniej jednego urządzenia, które jest jednak podłączone do MAGISTRALI, po naciśnięciu przycisku **Enroll** (Przypisz) w zakładce **Urządzenia** wyświetli się przycisk **Scan/add new BUS device** (Skanuj/dodaj nowe urządzenie magistrali), co umożliwi przypisywanie urządzenia MAGISTRALI. W celu przypisania urządzenia należy dwukrotnie kliknąć wybraną pozycję.

e. Przez łączne ładowanie **nieprzypisanych urządzeń MAGISTRALI** — w przypadku braku przypisania co najmniej jednego urządzenia, które jest jednak podłączone do MAGISTRALI, po naciśnięciu **Scan/add new BUS device** (Skanuj/dodaj nowe urządzenie magistrali) wszystkie urządzenia MAGISTRALI zostaną przypisane jednocześnie. Ta procedura nie pozwala określić kolejnych pozycji poszczególnych urządzeń.

3. Urządzenie można usunąć przez usunięcie jego kodu produkcji (zostanie usunięte wyłącznie urządzenie) lub przez wybranie odpowiedniego wiersza w zakładce Urządzenia oraz opcji Delete (Usuń) w menu lub prawym przyciskiem myszy lub po prostu przez naciśnięcie przycisku Delete, co usunie cały wiersz urządzenia (wraz z uzbrojeniem strefy, reakcją, sterowaniem wyjściem PG, uwagami i innymi opcjami). W ten sposób po zaznaczeniu większej liczby urządzeń (kliknięcie+Shift lub kliknięcie+Ctrl) można usunąć wszystkie te urządzenia lub po prostu zmienić wspólny parametr.

**Przestroga:**

*Zaleca się przypisanie urządzeń bezprzewodowych do systemu zgodnie z punktem B w faktycznych warunkach i w wymaganym miejscu w chronionym obiekcie. To pomoże uniknąć problemów związanych z niewystarczającym zasięgiem RF podczas przypisywania urządzeń „na stole".*

**Uwagi:**

- Nieprzypisane urządzenia MAGISTRALI migają na żółto. Jeżeli nieprzypisane urządzenie nie zacznie migać na żółto w ciągu około 180 sekund od włączenia zasilania centrali alarmowej (w trakcie uruchamiania), należy sprawdzić poprawność podłączenia urządzenia.
- Urządzenia bezprzewodowe o komunikacji jednokierunkowej nie posiadają możliwości sygnalizacji żądania przypisania.
- W przypadku przypisania urządzenia w systemie za pomocą powyższej procedury automatycznie zostanie zaproponowana kolejna pozycja. Nie trzeba wykonywać żadnych innych czynności. Należy tylko przypisać urządzenia w wybranym porządku. Automatyczne przejście do kolejnej pozycji można anulować w oknie przypisywania urządzenia.
- W przypadku przypisania już przypisanego urządzenia w innej pozycji przejście nastąpi automatycznie.
- Jeżeli urządzenie zajmuje więcej niż jedną pozycję, automatycznie zajmie odpowiednią liczbę pozycji w drodze jednego przypisywania (np. moduł JA-116H, który posiada szesnaście wejść alarmowych, zajmie szesnaście pozycji). Przestroga, może nastąpić przypadkowe usunięcie urządzenia przypisanego w innej pozycji!
- W przypadku przypisania urządzenia w najwyższej dostępnej pozycji dojdzie do zakończenia procesu stopniowego przypisywania.
- Wolne pozycje są domyślnie przypisywane do strefy 1. Przypisywanie sekcji można zmienić w późniejszym terminie.
- W przypadku urządzeń wielopozycyjnych, jak JA-116H, JA-118M, JA-114HN, JA-150M itp. można ograniczyć liczbę zajętych pozycji przez kasowanie konkretnych wierszy podczas przypisywanie modułu. W celu wykasowania należy kliknąć w konkretnym wierszu na żądaną pozycję (a nie przycisk w typie kolumny!) i nacisnąć przycisk Delete na klawiaturze komputera.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

### 8.4.2 Wykaz obowiązujących reakcji

W zakładce Urządzenia można ustawić reakcję aktywacji systemu dla przypisanego urządzenia. Dla poszczególnych urządzeń dostępne są wyłącznie rodzaje reakcji, które odpowiadają typowi danego produktu. W przypadku niektórych urządzeń nie można przypisać żadnej reakcji (np. syreny zewnętrznej).

***Przestroga:*** *Zakres reakcji może być ograniczony profilem systemu.*

| | |
|---|---|
| **Opóźniona** | Alarm włamania z opóźnieniem na wejście / wyjście |
| **Natychmiastowa** | Alarm nagły, jeżeli został ustawiony. W przypadku ustawienia opóźnienia na wejście aktywuje się alarm IW. Alarm EW aktywuje się dopiero po upływie czasu opóźnienia na wejście (więcej informacji na temat EW i IW podano w rozdziale 8.5 Types of alarms). |
| **Brama garażowa** | Alarm włamania z opóźnieniem na wejście / wyjście, brama garażowa z zegarem.<br>W zakładce Parametry można dla tej reakcji wprowadzić takie ustawienia, by opóźnienie na wyjście zostało odroczone aktywną czujką statusu z reakcją Bramy garażowej (np. na czas otwarcia bramy garażu). |
| **Następna opóźniona** | Alarm włamania. Czujka zapewnia taki sam opóźnienia na wyjście, jak czujki z opóźnioną reakcją w tej samej strefie. Ta czujka zapewni opóźnienie na wejście jedynie w przypadku aktywacji po czujce, dla której ustawiono reakcję opóźnioną. Jeżeli aktywuje się jako pierwsza, bezzwłocznie uruchomi alarm. To ustawienie ma sens, gdy w tej samej strefie ustawiono czujkę z reakcją opóźnioną. |
| **Zawsze natychmiastowa** | Natychmiastowa reakcja strefy. W przypadku uzbrojenia na podstawie aktywacji czujki z reakcją natychmiastową, w tym ostrzeżenia alarmowe EW i IW uruchomią się także podczas czasu opóźnienia na wejście. |
| **Natychmiastowa / Opóźniona** | System reaguje na aktywację czujki (alarm, opóźnienie na wejście), jeżeli jest częściowo uzbrojony w strefie alarmu natychmiastowego oraz całkowicie uzbrojony w strefie Opóźniony A. |
| **Natychmiastowa potwierdzona** | Natychmiastowy alarm włamania — patrz rozdział **Reakcja na potwierdzone włamanie** poniżej. |
| **Opóźniona potwierdzona** | Alarm włamania z opóźnieniem na wejście i wyjście, zegar A — patrz rozdział Reakcja **na potwierdzone włamanie**. |
| **Sabotaż** | Alarm sabotażowy w dowolnym czasie (strefa nie wymaga uzbrojenia). |
| **24 godziny** | Natychmiastowy alarm włamania (strefa nie wymaga uzbrojenia). |
| **Cicha panika** | Alarm Cicha panika:<br>1) EW i IW nieaktywne (patrz rozdział 8.5 Types of alarms);<br>2) klawiatura nie wydaje sygnałów dźwiękowych, choć jest ustawiona w ten sposób;<br>3) jeżeli system potrafi rozpoznać, kto uruchomił Alarm panika (np. za pomocą breloka z przyjętą tożsamością użytkownika lub kodu wprowadzonego przez użytkownika), nie wysyła SMS Panika do tego użytkownika. |
| **Panika z sygnałem dźwiękowym** | Alarm panika z sygnałem dźwiękowym (zachowanie jest takie samo, jak w przypadku alarmu Cicha panika, jedyna różnica polega na sygnalizacji alarmu przez wykorzystywaną syrenę, jak wskazano w tabeli) w rozdziale 8.5 Types of alarms). |
| **Alarm pożarowy** | Alarm pożarowy niezależnie od statusu strefy (strefa nie wymaga uzbrojenia). |
| **Potwierdzenie pożaru** | Alarm pożarowy niezależnie od statusu strefy (strefa nie wymaga uzbrojenia), patrz rozdział **Potwierdzona reakcja na pożar** poniżej. |
| **Pożar, natychmiastowa** | Alarm pożarowy wyłącznie w przypadku uzbrojenia danej strefy. |
| **Gaz** | Alarm pożarowy aktywowany czujką wycieku gazu może zostać włączony zawsze, niezależnie od statusu strefy. |
| **Problemy zdrowotne** | Wysyła raport o problemach zdrowotnych. |
| **Zalanie** | Wysyła alarm zalania |
| **Uzbrojona / Częściowo uzbrojona** | Uzbrojenie (częściowe uzbrojenie) strefy. W przypadku strefy wspólnej dojdzie do jednoczesnego uzbrojenia wszystkich stref do niej należących. Ta reakcja posiada także funkcję Rozbrój. |
| **Wyciszony** | Wyciszenie syreny wewnętrznej z późniejszym raportem obecności osoby w budynku. |

| | |
|---|---|
| **Brak** | Bez wpływu na alarm włamania, urządzenie można wykorzystać do aktywacji wyjść PG. Zachowane zostaje wykrywanie sabotażu, nadzoru i błędów. |
| **Brak bez sabotażu** | System reaguje na aktywację czujki wyłącznie w drodze sterowania wyjściem PG. Nie uruchamia się żaden rodzaj alarmu (nawet alarmu sabotażu), zachowanie wykrywania awarii. |

### 8.4.3 Ograniczenie fałszywych alarmów

W instalacjach o zwiększonym ryzyku fałszywych alarmów można wykorzystać specjalne rodzaje reakcji:

**Potwierdzona reakcja na włamanie** — w przypadku aktywacji czujki z potwierdzoną reakcją w uzbrojonej strefie system raportuje do SMA wyłącznie niepotwierdzony alarm i czeka na potwierdzenie inną czujką. Alarm może zostać potwierdzony czujką włamania w uzbrojonej strefie. W zakładce Parametry można określić, czy potwierdzenie może pochodzić z dowolnej uzbrojonej strefy czy też musi pochodzić z tej samej strefy. W zakładce Parametry można także ustawić czas oczekiwania systemu na potwierdzenie inną czujką (do 60 min). Przy braku potwierdzenia alarmu w zadanym czasie alarm nie uruchomi się. W przypadku ustawienia potwierdzonej reakcji opóźnionej aktywacja czujki jedynie rozpoczyna wysłanie niepotwierdzonego alarmu po wygaśnięciu opóźnienia na wejście. Potwierdzoną reakcję można wykorzystać wyłącznie w przypadku instalacji większej liczby czujek włamania w budynku (by umożliwić potwierdzenie).

**Potwierdzona reakcja pożarowa** — w przypadku aktywacji czujki pożaru o tym rodzaju reakcji do SMA zostanie zgłoszony tylko niepotwierdzony alarm pożarowy, i system poczeka na potwierdzenie pożaru przez inną czujkę pożaru. W zakładce Parametry można określić, czy potwierdzenie może pochodzić z dowolnej strefy czy też musi pochodzić z tej samej strefy. Czas oczekiwania na potwierdzenie alarmu pożarowego ustawia się w zakładce Parametry. Przy braku potwierdzenia pożaru w zadanym czasie alarm pożarowy nie uruchomi się. Potwierdzoną reakcję można wykorzystać wyłącznie w przypadku instalacji większej liczby czujek pożaru w budynku (by umożliwić potwierdzenie).

**Ostrzeżenie:** Tę funkcję i jej zastosowanie potraktowano poważnie, zgodnie z miejscowymi przepisami i normami.

**Funkcja 3 aktywacji (3x i STOP!)** — wszystkie czujki z aktywną reakcją alarmową na włamanie i pożar posiadają tylko trzy możliwe aktywacje centrali alarmowej podczas jednego okresu monitorowania. Po trzeciej aktywacji (w przypadku czwartego włamania) uruchomi się pominięcie dla danego wejścia alarmu, a odpowiadający mu czujnik zostanie wyłączony. Jeżeli te trzy aktywacje wystąpią podczas alarmu, zostaną wygenerowane łączne trzy alarmowe wiadomości SMS i nastąpi wyłączenie czujki. W przypadku trzech aktywacji w odstępach czasu dłuższych od czasu trwania alarmu dojdzie do wygenerowania trzech alarmowych wiadomości SMS, uruchomienia trzech alarmów, a następnie do wyłączenia czujki.

Pominięcie można anulować w drodze rozbrojenia i ponownego uzbrojenia strefy. Wówczas czujka powróci w tryb strzeżenia. Pominięcie dla reakcji na pożar i zalanie zostanie anulowane automatycznie o godzinie 12:00 następnego dnia. Ten mechanizm pominięcia na zasadzie 3x i stop nie ma zastosowania w przypadku ustawienia reakcji Panika.

**Opóźniony raport do SMA** — Zgodnie z wymogami normy EN50131-1, w celu ograniczenia liczby fałszywych alarmów spowodowanych nieprawidłową obsługą systemu przez użytkownika końcowego oraz interwencji firmy ochroniarskiej. W przypadku aktywacji dojdzie do uruchomienia alarmu wewnętrznego (syreny, sygnalizacja klawiatury) po wygaśnięciu czasu na wejście, ale system odczeka 15 sekund przed wysłaniem raportu o alarmie do SMA. Użytkownik posiada kolejne 15 sekund na rozbrojenie systemu bez aktywacji alarmu zgłaszanego do SMA. Jeżeli zdąży, raport nie zostanie wysłany. To opóźnienie dotyczy wyłącznie alarmów uruchomionych przez strefę z opóźnieniem. Pozostałe rodzaje alarmów (natychmiastowy, pożarowy, sabotażu itp.) zostają zgłoszone natychmiast bez opóźnienia, niezależnie od tej funkcji.

## 8.5 Rodzaje alarmów

Główne zadanie systemu zabezpieczeń polega na raportowaniu zdarzeń do właściciela i użytkowników bądź do specjalistycznej agencji ochrony, by powiadomić o zagrożeniach. Może to być włamanie lub zdarzenie środowiskowe, jak dym, pożar, wyciek gazu czy zalanie w strzeżonym obiekcie. Każdy rodzaj alarmu można sygnalizować odmiennie, zależnie od jego przyczyny. W przypadku syren alarmy dzieli się na wewnętrzne (IW) i zewnętrzne (EW).

Wszystkie rodzaje syren w systemie emitują przerywany sygnał dźwiękowy (opcjonalnie ciągły lub przerywany), a syrena na zewnątrz miga na czerwono lub niebiesko. Długość sygnalizacji ustala się parametrem czasu trwania alarmu w centrali alarmowej. Każda syrena posiada własne ustawienia, jak ograniczenie długości alarmu, dzięki czemu można ustawić krótszy czas sygnalizacji alarmu przez syrenę zewnętrzną niż przez wewnętrzną. Każdy alarm (z wyjątkiem cichego alarmu panika) posiada początek i koniec (wygaśnięcie lub anulowanie przez użytkownika), a przyczynę zdarzeń rejestruje się z datą.

Na wszystkich klawiaturach systemu wszystkie alarmy (z wyjątkiem cichego alarmu panika) sygnalizuje migająca na czerwono kontrolka systemu oraz ciągła sygnalizacja dźwiękowa.

**W poniższej tabeli podano przegląd wyjść IW i EW zależnie od typu alarmu i statusu strefy:**

| | Typ alarmu | | | | | Ustawienia systemu — Parametry | | Aktywuje | |
|---|---|---|---|---|---|---|---|---|---|
| **Status sekcji** | **Włamanie** | **Sabotaż** | **sygnałem dźwiękowy** | **Pożar** | **24 h/ Zalanie** | **Syrena IW przy uzbrojeniu częściowym** | **Syrena IW podczas sabotażu** | **EW** | **IW** |
| **Rozbrojona** | | **X** | | | | *nd* | NIE | | |
| | | **X** | | | | *nd* | TAK | | **X** |
| | | | **X** | | | *nd* | *nd* | **X** | **X** |
| | | | | **X** | **X** | *nd* | *nd* | | **X** |
| **Częściowo uzbrojona** | | **X** | | | | *nd* | NIE | | |
| | | **X** | | | | *nd* | TAK | | **X** |
| | **X** | | | | | TAK | *nd* | | **X** |
| | **X** | | | | | NIE | *nd* | | |
| | | | **X** | | | *nd* | *nd* | **X** | **X** |
| | | | | **X** | **X** | *nd* | *nd* | | **X** |
| **Uzbrojona** | **X** | **X** | **X** | **X** | **X** | *nd* | *nd* | **X** | **X** |

### 8.5.1 Alarm włamania

To stan alarmowy centrali alarmowej, który mogą uruchomić czujki o reakcji opóźnionej lub natychmiastowej (i ich odmianach), i który dotyczy wyłącznie systemu całkowicie lub częściowo uzbrojonego. Sygnalizują go syreny wewnętrzne i zewnętrzne, jak wynika z powyższej tabeli. Długość alarmu wskazują ustawienia w parametrach systemu centrali alarmowej. Po wygaśnięciu alarmu ustaje sygnalizacja na klawiaturze i za pomocą syren. Uwierzytelnienie użytkownika wycisza sygnalizację dźwiękową wszystkich syren i klawiatur, ale nie anuluje stanu alarmowego systemu i nie rozbraja. W tym celu należy wykonać poniższą czynność przy użyciu przycisku funkcji i opcji menu klawiatury „Sterowanie strefą".

### 8.5.2 Alarm sabotażowy

Centrala alarmowa nadzoruje wszystkie urządzenia przypisane w systemie niezależnie od statusu systemu (uzbrojony / rozbrojony). Większość urządzeń posiada wbudowany styk sabotażu do wykrywania otwarcia ich pokrywy i oderwania od ściany. Aktywacja uruchamia alarm sabotażu, a do jego sygnalizacji służy syrena wewnętrzna (zgodnie z parametrem Syrena IW po aktywacji sabotażu) w systemie rozbrojonym, zaś w uzbrojonym obie syreny (wewnętrzna oraz zewnętrzna), patrz powyższa tabela. Alarm sabotażowy może oznaczać także utratę urządzeń MAGISTRALI (np. w wyniku zwarcia) lub próbę złamania kodu (10x) na klawiaturze.

### 8.5.3 Alarm pożarowy

Alarm pożarowy uruchamia się przez aktywację czujek z zadaną reakcją Pożar. Za czujki pożarowe uznaje się wszystkie następujące czujki: dymu, wysokiej temperatury, gazów łatwopalnych lub trującego CO. Alarm pożarowy sygnalizują syreny wewnętrzne przy systemie rozbrojonym lub częściowo uzbrojonym, zaś przy systemie całkowicie uzbrojonym robią to syreny wewnętrzne i zewnętrzne.

Istnieją różne rodzaje alarmów, na przykład:

1. **Pożarowy** — podstawowa reakcja dla wszystkich czujek pożarowych.
2. **Pożarowy potwierdzony** — opcja zwiększająca niezawodność. W każdym pomieszczeniu należy zainstalować co najmniej 2 czujki pożarowe o tych samych ustawieniach.
3. **Pożarowy natychmiastowy** — używany przede wszystkim w obiektach, gdzie zwykle występuje dym (restauracje, warsztaty spawalnicze itp.), a wykrywanie odbywa się dopiero po uzbrojeniu systemu.
4. **Gaz** — specjalna reakcja czujek pożarowych z identyfikacją palnego, trującego gazu do raportowania takiego zdarzenia do SMA.

### 8.5.4 Alarm panika

Alarm panika jest specjalnym zdarzeniem, które można aktywować w postaci 2 różnych zdarzeń, **Cichy alarm panika** i **Alarm panika z sygnałem dźwiękowym.** Każdy z nich posiada odrębne zachowanie.

1) **Cichy alarm panika** — specjalne zdarzenie nieprzypisane do grupy alarmów włamania, które sygnalizuje syrena lub klawiatura. Cichy alarm panika nie posiada zegara i to zdarzenie nie ma końca. Tym samym nie można go używać do sterowania statusem wyjścia PG. Służy jedynie do aktywacji cichego alarmu panika i może zapewnić pomoc w razie napadu bez świadomości atakującego. Cichy alarm panika można aktywować odpowiednim (ukrytym lub przenośnym) przyciskiem panika. Zwykle służy do tego przycisk ustawiony na cichy alarm panika, kombinacja przycisków A, B, C lub D na pilocie, klawiatura ze specjalnym przyciskiem funkcji ustawionym na cichy alarm panika (w takim przypadku alarm panika można opóźnić przy pomocy opcjonalnego zegara), naciśnięcie przycisku na syrenie wewnętrznej, wejście na module MAGISTRALI przeznaczone do urządzeń przewodowych lub wprowadzenie specjalnego kodu, uruchamiającego cichy alarm panika. Cichy alarm panika można także uruchomić w trakcie Antynapadowej kontroli dostępu (patrz rozdział 9.8), gdzie modyfikuje się standardowy kod użytkownika.
2) **Alarm panika z sygnałem dźwiękowym** — jest to zwykłe zdarzenie alarmowe, posiadające początek i koniec, sygnalizowane dźwiękowo syreną i przez klawiaturę. Można go używać do sterowania statusem wyjścia PG. Służy przede wszystkim do aktywacji alarmu panika z opcjonalnym wymogiem sygnalizacji lub do blokowania elektrycznych zamków w drzwiach itp. Alarm panika z sygnałem dźwiękowym można aktywować odpowiednim (ukrytym lub przenośnym) przyciskiem panika. Zwykle służy do tego przycisk przypisany do cichego alarmu panika, połączenie klawiszy na pilocie, klawiatura ze specjalnym przyciskiem funkcji ustawionym na cichy alarm panika (w takim przypadku alarm panika można opóźnić przy pomocy opcjonalnego pilota), naciśnięcie przycisku na syrenie wewnętrznej, wejście na module MAGISTRALI przeznaczone do urządzeń przewodowych.

   ***Uwaga**: Oba rodzaje alarmu panika mają szczególny charakter, ponieważ można je aktywować wielokrotnie bez ograniczeń ani automatycznej blokady.*

### 8.5.5 Alarm 24 h

Czujki zapewniające stałą ochronę (nadzór ich stanu), niezależnie od statusu systemu (uzbrojony lub rozbrojony), mogą posiadać zadaną reakcję 24 godziny lub na wypadek zalania. Ten rodzaj alarmu jest przypisany do grupy alarmów włamania, ale niezależnie od tego można go aktywować przy rozbrojeniu systemu. Zgodnie ze stanem systemu alarm sygnalizują syreny wewnętrzne i zewnętrzne, patrz powyższa tabela. Alarm raportuje się w ten sam sposób jak inne alarmy.

## 8.6 Błędy systemu

Błąd jest sygnałem ostrzegawczym, pochodzącym z systemu, który sygnalizuje jakąś nieprawidłowość centrali alarmowej, komunikacji lub urządzeń. Problem może być związany z modułem radiowym, uzupełniającym modułem GSM lub komunikatorem LAN, maskowaniem czujek (z funkcją antymaskowania), z zasilaniem (zasilanie sieciowe lub z baterii) lub zasilaniem awaryjnym. Błąd/błędy sygnalizują klawiatury systemy przy użyciu żółtej kontrolki. Raporty dotyczące błędów pochodzą z każdego źródła, a przy 4. aktywacji błędu źródło błędu zostaje pominięte, co oznacza brak zgłoszenia 4. błędu.

W poniższej tabeli znajduje się zestawienie ogólnych błędów systemu:

| Źródło błędu | Przyczyna |
|---|---|
| Centrala alarmowa | Zasilanie sieciowe odłączone przez ponad 30 minut |
| | Wadliwa bateria awaryjna lub niski poziom energii w takiej baterii w centrali alarmowej |
| Komunikator | Utrata połączenia LAN, utrata sygnału GSM lub awaria linii PSTN na co najmniej 15 minut |
| | Zdarzenia niedostarczone do SMA w zadanym czasie |
| Moduł radiowy | Tłumienie pasma radiowego 868 MHz |
| | Utrata komunikacji MAGISTRALI |
| Klawiatury | Utrata komunikacji radiowej lub MAGISTRALI (patrz rozdział 8.7) |
| Syreny | |
| Moduły | |
| Czujki | |
| Czujki | Maskowanie czujek ruchu (antymaskowanie)<br>Błąd czujki wewnętrznej (czujka wycieku gazu)<br>Błąd wywołany zmniejszeniem intensywności promieni podczerwonych (bariera podczerwieni) |



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

## 8.7 Błąd spowodowany utratą urządzenia

Każde urządzenie (MAGISTRALI lub bezprzewodowe) w systemie jest nadzorowane przez centralę alarmową przy aktywnym parametrze Nadzór (patrz zakładka Parametry / kolumna Nadzór) po utracie komunikacji z centralą alarmową (brak reakcji w zadanym czasie). W takim przypadku system aktywuje zdarzenie „Aktywacja błędu", a zależnie od „Utrata urządzenia MAGISTRALI" może po nim nastąpić alarm sabotażu. Jest to opcjonalne i może zostać uruchomione, gdy moduł radiowy wykryje tłumienie RF lub pewien rodzaj zakłóceń RF przez co najmniej 30 sekund na 2 poziomach detekcji. Może także uruchomić alarm sabotażu w przypadku zwarcia w MAGISTRALI systemu, co uniemożliwia poprawną komunikację urządzeń MAGISTRALI. Czas braku komunikacji ma stałą długość, której nie można zmienić. Dla urządzeń MAGISTRALI wynosi on 8 sekund, zaś dla bezprzewodowych 120 minut od chwili ostatniej komunikacji.

Opcja zmieniająca reakcję centrali alarmowej na utratę urządzeń MAGISTRALI nazywa się „**Utrata urządzenia MAGISTRALI**", patrz oprogramowanie F-Link, zakładka Parametry. Oferuje ona następujące opcje:

- **Błąd** — centrala alarmowa zawsze przetwarza utratę urządzenia w MAGISTRALI lub zwarcie MAGISTRALI jako Błąd.
- **Sabotaż zawsze** — centrala alarmowa przetwarza utratę urządzenia w MAGISTRALI lub zwarcie MAGISTRALI jako alarm sabotażu przy każdym wystąpieniu takiego zdarzenia. Jeżeli dla modułu radiowego aktywowano wykrywanie tłumienia RF, i faktycznie dojdzie do wykrycia takiego tłumienia, również uruchomi on alarm sabotażu. Po alarmie sabotażu także występuje błąd, a kiedy błąd zniknie, skasuje się także alarm sabotażu.
- **Sabotaż po potwierdzeniu** — centrala alarmowa przetwarza utratę pierwszego urządzenia jako błąd, a jeżeli w zadanym czasie, wynikającym z parametru „Okres oczekiwania na potwierdzenie alarmu", wystąpi kolejna utrata urządzenia, system ją potwierdzi i aktywuje alarm sabotażu. Po usunięciu błędu wszystkich utraconych urządzeń system anuluje błąd i alarm sabotażu.

# 9 Opcje sterowania systemem

Systemem bezpieczeństwa można sterować na różne sposoby. Podstawowe opcje sterowania to opcje lokalne lub zdalne. Inne opcje wymieniono w poniższej tabeli:

| Typ | Sposób/tryb | Urządzenie | Stan | Opis sterowania |
|---|---|---|---|---|
| Lokalne | Klawiatura (uwierzytelnienie i przycisk funkcji) | JA-110E, JA-150E | Moduł radiowy JA-111R dla klawiatury bezprzewodowej | Czynność można wykonać po uwierzytelnieniu użytkownika i naciśnięciu odpowiedniego przycisku funkcji lub za pośrednictwem menu klawiatury. |
| | Czytnik RFID (wyłącznie uwierzytelnienie) | JA-110E, JA-150E | Moduł radiowy JA-111R dla klawiatury bezprzewodowej | Czynność można wykonać po uwierzytelnieniu użytkownika lub przy pomocy breloka RFID bądź po wprowadzeniu kodu |
| | Kalendarz | 10 czynności z kalendarza | | Każda czynność z kalendarza posiada opcje, pozwalające wybrać zdarzenie, czas jego realizacji i dzień tygodnia. Może sterować strefami i wyjściami PG. Wyjścia PG można zablokować. |
| | Program F-Link lub J-Link | Komputer z systemem Windows | Przewód USB | Strefami i wyjściami PG można sterować po uwierzytelnieniu. |
| Zdalne | Menu głosowe | Telefon | Uzupełniające urządzenie GSM lub PSTN do automatycznego wybierania numerów | Ustanowienie połączenia z numerem telefonu w systemie i systemem sterowania za pomocą tonów DTMF po uwierzytelnieniu. |

| | | | | |
|---|---|---|---|---|
| | Manipulator zdalny | JA-16xJ | Moduł radiowy JA-111R | Uzbrajanie i rozbrajanie przez naciśnięcie zadanego przycisku na pilocie. |
| | Komunikat SMS | Telefon komórkowy | Uzupełniające urządzenie GSM do automatycznego wybierania numerów | Uwierzytelnione polecenie do uzbrajania lub rozbrajania stref, a także sterowania wyjściami PG. |
| | Ustanowienie połączenia z uwierzytelnionego numeru telefonu | Telefon (wyłącznie sterowanie PG) | Uzupełniające urządzenie GSM lub PSTN do automatycznego wybierania numerów | Dla każdego uwierzytelnionego numeru telefonu można sterować jednym konkretnym wyjściem PG. |
| | Program F-Link lub J-Link | Komputer z systemem Windows (XP SP 3 i wyższa) | Uzupełniające urządzenie GSM lub LAN do automatycznego wybierania numerów | Strefami i wyjściami PG można sterować po uwierzytelnieniu za pomocą klawiatury wirtualnej. |

Wszystkie powyższe sposoby można wykorzystać do sterowania systemem (uzbrajanie, uzbrajanie częściowe, rozbrajanie) oraz wyjściami PG (WŁ., WYŁ., czas).

## 9.1 Sposób uwierzytelniania

Uwierzytelnianie jest kluczowym elementem sterowania systemem oraz weryfikacji, czy użytkownik faktycznie posiada uprawnienia do obsługi. Zależnie od procedury uwierzytelniania system określa, czy użytkownik ma prawo uzbrajać lub rozbrajać sekcje, włączać lub wyłączać wyjścia PG przy użyciu przycisków funkcji, czy też może jedynie przeglądać status systemu i dziennik historii przy użyciu menu klawiatury. Każdy użytkownik może posiadać przypisane różne opcje uwierzytelniania:

- Kod dostępu (numer4 lub 6-cyfrowy, zależnie od wybranego profilu systemu: domyślny, EN, INCERT)
- Karta lub brelok RFID
- Numer telefonu do uwierzytelniania podczas dostępu zdalnego przez połączenie telefoniczne lub SMS (w przypadku podłączenia uzupełniającego urządzenia GSM do automatycznego wybierania numerów)

Aby dostosować poziom bezpieczeństwa, poziom uwierzytelniania można ustawić na 2 poniższych poziomach:

1. **Standardowy** — uwierzytelnianie odbywa się przez przyłożenie karty/breloka RFID lub wprowadzenie prawidłowego kodu dostępu
2. **Uwierzytelnienie podwójne** — w przypadku uwierzytelnienia za pomocą klawiatury systemu zawsze należy wprowadzić prawidłowy kod dostępu i skorzystać z breloka/karty RFID (niezależnie od kolejności uwierzytelnienia). Podczas dostępu zdalnego zawsze następuje weryfikacja numeru telefonu oraz wprowadzenia poprawnego kodu. Program F-Link monitoruje, czy kod i karta zostały przypisane do użytkownika w Zakładce Użytkownicy (w przeciwnym razie F-Link nie pozwoli na zapisanie konfiguracji).

**Uwaga:** Potwierdzenie kodu użytkownika kartą RFID zmniejsza ryzyko nieuprawnionej obsługi lub obejścia systemu przez osoby trzecie.

## 9.2 Sterowanie systemem z klawiatury

Najlepszy sposób sterowania systemem zabezpieczeń i jego monitorowania polega na wykorzystaniu klawiatury systemu, gdzie dzięki kolorowej kontrolce statusu systemu na głównym przycisku sterowania zawsze można sprawdzić błędy i alarmy. Przy użyciu innych przycisków funkcji można sterować statusem stref i wyjść PG, a także opcjami systemu, jak sygnalizacja pamięci alarmów, aktywacja alarmu panika lub problemy zdrowotne. Przy pomocy klawiatury można przeglądać menu wewnętrzne, aby uzyskać informacje na temat błędów, zdarzeń, czujek aktywnych lub pominiętych, bądź czujek uniemożliwiających uzbrojenie systemu — zawsze po odpowiednim uwierzytelnieniu. Brak uwierzytelnienia = brak dostępu do menu klawiatury, zależnie od indywidualnych ustawień klawiatury może dojść do ukrycia pozycji menu, co chroni system przed eksploatacją przez osoby nieuprawnione.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

Najbardziej podstawową funkcją klawiatury systemu jest uzbrajanie i rozbrajanie stref. System można uzbroić całkowicie lub częściowo. Sterowanie zawsze można wykonać na kilka sposobów:

1. Za pomocą przycisków funkcji — naciśnięcie przycisku może całkowicie, bądź jedynie częściowo, bądź częściowo i całkowicie uzbroić system. Po uzbrojeniu możne nastąpić uwierzytelnienie (w historii rejestruje się, kto uzbroił którą strefę) lub nie (kod nie jest konieczny, więc z historii nie wynika, kto uzbroił strefę). Podczas uzbrajania systemu przyciskami funkcji uwierzytelnienie jest zawsze konieczne, by w pamięci centrali alarmowej zarejestrować, kto rozbrajał strefę.

2. W menu klawiatury — nacisnąć „*" po uwierzytelnieniu i uzbroić częściowo, całkowicie lub rozbroić.
3. Wyłącznie w drodze uwierzytelnienia — uwzględniając ustawienia, można uzbroić częściowo (jedynie) i rozbroić wyłącznie w drodze uwierzytelnienia za pomocą kodu lub przyłożenia karty/breloka RFID. Aby wejść do menu klawiatury, należy przed uwierzytelnieniem nacisnąć przycisk „*".

**Procedura uzbrajania:**

**1. Pełne uzbrojenie strefy przed opuszczeniem chronionego obiektu (w obiekcie nie ma już innych osób):**

Całkowite uzbrojenie systemu oznacza czerwony przycisk funkcji lub całkowicie podświetlony numer strefy na wyświetlaczu LCD klawiatury podczas sterowania przy użyciu menu.

Na potrzeby sterowania systemem za pomocą klawiatury umieszczonej w chronionym obiekcie należy zapewnić ścieżkę do wyjścia i wejścia, chronioną czujkami o opóźnionej reakcji. Strefy opóźnienia i następnego opóźnienia nie uczestniczą w strzeżeniu natychmiast po uzbrojeniu strefy, ale uczestniczą w nim strefy z reakcją natychmiastową. Użytkownik musi być w stanie opuścić chroniony obiekt po uzbrojeniu systemu, ale przed wygaśnięciem czasu opóźnienia na wyjście. A w przypadku aktywacji opóźnienia na wejście w strefie z opóźnieniem użytkownik musi być w stanie przejść ścieżką wejściową do klawiatury, za pomocą której dokona rozbrojenia systemu. Jeżeli użytkownik nie rozbroi strefy na czas (przed wygaśnięciem czasu na wejście), system aktywuje alarm w strefie z opóźnieniem. W przypadku włamania ścieżką inną niż ścieżka na wejście system uruchomi alarm w strefie alarmu natychmiastowego — natychmiast uruchomi syrenę.

**2. Uzbrojenie częściowe, użytkownik pozostaje w obiekcie:**

Częściowe uzbrojenie systemu sygnalizuje żółty przycisk funkcji lub całkowicie podświetlony numer strefy na wyświetlaczu LCD klawiatury podczas sterowania przy użyciu menu.

Przy częściowym uzbrojeniu systemu użytkownik pozostaje w chronionym obiekcie, a strzeżenie odbywa się jedynie przy pomocy czujek ochrony terenu (zapewnia to swobodę ruchu w obiekcie). Istnieją dwa warianty sterowania:

a) Sterowanie za pomocą klawiatury umieszczonej wewnątrz chronionego obiektu z ochroną terenu (hol wejściowy itp.). Wszystkie czujki w holu wejściowym muszą posiadać zadaną reakcję opóźnioną, dzięki czemu po uzbrojeniu systemu ich aktywacja zapewni pewien czas na wejście, by rozbroić system.
b) Sterowanie za pomocą klawiatury umieszczonej poza chronionym obiektem z ochroną terenu (hol wewnętrzny, schody, sypialnia itp.). Ten wariant nie pozwala na wejście jakiejkolwiek osoby bez natychmiastowego uruchomienia alarmu. Do obiektu można wejść po wcześniejszym rozbrojeniu za pomocą manipulatora zdalnego, zaś w przypadku podłączonego uzupełniającego modułu GSM za pomocą menu głosowego i wiadomości SMS. W tym przypadku czujki posiadają zadaną reakcję natychmiastową / opóźnioną.

**Sterowanie systemem z klawiatury — procedura:**

System posiada kilka profili systemu, spełniających wymogi różnych norm, a także zmienia zachowanie klawiatury oraz, rzecz jasna, sposób sterowania nim.

**Uzbrajanie systemu:**

1. Nieuzbrojoną strefę sygnalizuje przycisk funkcji świecący na zielono.
2. Naciśnięcie przycisku funkcji zgłasza żądanie uzbrojenia strefy. Zależnie od liczby wykorzystanych przycisków funkcji można wybrać większą liczbę żądań.
3. Jeżeli do uzbrojenia strefy koniecznie jest uwierzytelnienie, czerwone (uzbrojenie całkowite) lub żółte (uzbrojenie częściowe), powolne miganie przycisku funkcji wskazuje czas do spodziewanego uwierzytelnienia (8 sekund).
4. Przyłożenie karty / breloka RFID lub wprowadzenie kodu umożliwia uwierzytelnienie (w przypadku, gdy wymagany jest zarówno kod, jak i karta, ich kolejność nie ma znaczenia).
5. Jeżeli po naciśnięciu przycisku funkcji nie ustanie miganie czerwonej lub żółtej kontrolki (8 sekund), system wykrywa przeszkodę uniemożliwiającą uzbrojenie (patrz rozdział 9.11 Obstacles preventing setting the system).
6. Udane uzbrajanie lub uzbrajanie częściowe potwierdza świecący światłem ciągłym czerwony lub żółty przycisk funkcji.

**Rozbrajanie sytemu:**

1. Uzbrojoną strefę sygnalizuje przycisk funkcji świecący na czerwono lub żółto. Po wykryciu włamania do chronionego obiektu uruchamia opóźnienie na wejście, co sygnalizuje szybkie miganie odpowiedniego przycisku funkcji.

2. Naciśnięcie właściwego przycisku funkcji (lub kolejno większej liczby przycisków) oznacza żądanie rozbrojenia strefy, a powolne miganie przycisku funkcji wskazuje niezbędne uwierzytelnienie.
3. Przyłożenie karty / breloka RFID lub wprowadzenie kodu umożliwia uwierzytelnienie (w przypadku, gdy wymagany jest zarówno kod, jak i karta, ich kolejność nie ma znaczenia).
4. Udane rozbrojenie potwierdza świecenie światłem ciągłym zielonego przycisku funkcji.
5. Jeżeli po rozbrojeniu strefy nie ustaje szybkie miganie przycisku funkcji, sygnalizuje to pamięć alarmów w strefie. Sygnalizację można skasować kolejnym naciśnięciem tego przycisku z uprawnieniami do kasowania pamięci alarmów lub przy pomocy menu klawiatury, gdzie należy wybrać opcję „Anuluj ostrzeżenie".

**Sygnalizacja systemu klawiatury — przegląd statusów:**

| | |
|---|---|
| Zielona kontrolka WŁ. | Zwykła praca. Strefy sterowane za pomocą klawiatury są OK, bez błędów. |
| Żółta kontrolka WŁ. | Zwykła praca, w niektórych sterowanych strefach wykryto błąd. Po uwierzytelnieniu użytkownika na podstawie praw dostępu za pomocą menu klawiatury można uzyskać bardziej szczegółowe informacje. Obracające się logo Jablotron na klawiaturze, pojawiające się po sygnalizacji błędu, oznacza błąd komunikacji radiowej między centralą alarmową a klawiaturą. |
| Czerwona kontrolka WŁ. | Klawiatura w trybie ROZRUCHU podczas aktualizacji oprogramowania. |
| Miga na zielono (2 Hz) | Dokonano uwierzytelnienia, użytkownik może zmienić status systemu przyciskiem funkcji lub przeszukując menu klawiatury. Czas na uwierzytelnienie wynosi 8 sekund od ostatniego naciśnięcia przycisku. Można go anulować klawiszem ESC. |
| Miga na żółto (8 Hz) | Ostrzeżenie o nieudanym uzbrajaniu |
| Miga na czerwono (8 Hz) | Sygnalizacja aktualnie uruchomionego alarmu w konkretnej strefie na klawiaturze. Rodzaj alarmu, nazwę strefy, w której doszło do uruchomienia alarmu, oraz źródło uruchomionego alarmu są widoczne na klawiaturze. |
| Miga naprzemiennie na czerwono/żółto | Uruchomiony alarm z aktywnym błędem |
| Miga naprzemiennie na zielono/czerwono | Uwierzytelnienie z pamięcią alarmów |
| Miga naprzemiennie na zielono/żółto | Uwierzytelnienie z aktywnym błędem |
| Miga na żółto (2 x co 2 sekundy) | Programowanie / Tryb serwisowy. Wszystkie przyciski funkcji i menu klawiatury Administratora nie są dostępne dla użytkowników. Menu klawiatury jest dostępne wyłącznie dla serwisanta pod warunkiem podłączenia komputera do centrali alarmowej. |
| Miga na czerwono (2 x co 2 sekundy) | Sygnalizacja pamięci alarmów |
| Miga na żółto (1 x co 2 sekundy) | Sygnalizacja błędu na klawiaturze w trybie uśpienia (dotyczy jedynie profilu EN50131-1) |
| Miga na czerwono (1 x co 2 sekundy) | Sygnalizacja pamięci alarmów na klawiaturze w trybie uśpienia (dotyczy jedynie profilu EN50131-1) |
| Brak sygnalizacji | Klawiatura w trybie uśpienia |

**Przegląd sygnalizacji świetlnej przycisku funkcyjnego klawiatury:**

| | |
|---|---|
| Przycisk podświetlony na zielono | Status strefy to Rozbrojona lub Wyjście PG WYŁ. |
| Przycisk miga na zielono (4 Hz) | Trwa opóźnienie na wejście i system oczekuje na uwierzytelnienie, aby mógł dokonać rozbrojenia. |
| Przycisk miga na żółto | Status strefy to Częściowo uzbrojona. |
| Przycisk podświetlony na czerwono | Status strefy to Uzbrojona lub Wyjście PG WŁ. |
| Przycisk miga na żółto (4 Hz) | System oczekuje na uwierzytelnienie w przypadku częściowego uzbrojenia lub zgłasza błąd podczas częściowego uzbrojenia. |
| Przycisk miga na żółto (8 Hz) | Ostrzeżenie o nieudanym uzbrajaniu |
| Przycisk miga na czerwono (4 Hz) | System oczekuje na uwierzytelnienie podczas uzbrajania lub zgłasza problem podczas uzbrajania. |
| Przycisk miga na czerwono (8 Hz) | Sygnalizacja pamięci alarmów trwa do chwili anulowania. |
| Przycisk się nie zapala | Tryb serwisowy lub strefa zablokowana po alarmie. |

## 9.3 Sterowanie systemem za pomocą manipulatora zdalnego

W przypadku wymogu sterowania systemem przed dostępem do chronionego obiektu (przyjazd samochodem pod garaż) lub budynku strzeżonego tylko czujkami z reakcją natychmiastową zapewnia, że nikt nie może rozbroić systemu przy użyciu klawiatury wewnątrz chronionego obiektu (brak ścieżki wejściowej), ale wyłącznie manipulatorem zdalnym przed wejściem do budynku. W związku z tym moduł radiowy JA-111R musi być przypisany do systemu na potrzeby komunikacji z urządzeniami bezprzewodowymi. Należy go umieścić w odpowiednim miejscu, by zapewnić niezawodną komunikację z pilotem przy uwzględnieniu wymaganej odległości roboczej.

Każdy przycisk manipulatora może sterować wybraną strefą (przycisk z prawej strony zawsze uzbraja, zaś przycisk z lewej strony zawsze rozbraja). Manipulatory zdalne przestrzegają zasad uzbrajania systemu, w związku z czym w obecności jakichkolwiek przeszkód uniemożliwiających uzbrajanie nie można uzbroić systemu.

W przypadku wykorzystania pilota jednokierunkowego (JA-16xJ) dioda wskazuje jedynie naciśnięcie przycisku i wysłanie polecenia. Nie ma odpowiedzi z centrali alarmowej, a użytkownik powinien wykorzystać inny rodzaj sygnalizacji statusu do potwierdzenia zmiany statusu strefy, np. brzęczyk syreny, inną sygnalizację świetlną lub raporty SMS o uzbrojeniu/rozbrojeniu.

## 9.4 Sterowanie systemem przy użyciu kalendarza

Automatyczne sterowanie systemem można realizować przy użyciu wewnętrznego kalendarza centrali alarmowej. Kalendarz możnaustawić na 10 zadań (uzbrojenie całkowite, uzbrojenie częściowe, rozbrojenie wybranych stref, a także WŁĄCZENIE / WYŁĄCZENIE lub zablokowanie / odblokowanie wybranych wyjść PG).

Każda czynność może umożliwić ustawienie dni tygodnia (od poniedziałku do niedzieli) na ich wykonanie, co oznacza możliwość ustawienia jedynie dni roboczych lub weekendu. Dla każdego zadania należy wybrać godzinę oraz konkretne zadanie do wykonania, a także jedno zdarzenie (zadanie) do sterowania wyjściem PG. Tym samym o określonej godzinie strefa/strefy może/mogą zostać uzbrojona/e lub rozbrojona/e, a jednocześnie wyjście PG może być WŁĄCZONE lub WYŁĄCZONE. Do typowych zastosowań należy automatyczne uzbrajanie strefy w sklepach, uzbrajanie częściowe w budynku w godzinach nocnych lub sterowanie oświetleniem w nocy. Każde automatyczne zdarzenie rejestruje się w rejestrze historii pod nazwą źródła „Kalendarz".

**Opcje sterowania kalendarzem związane ze strzeżeniem:**

| | |
|---|---|
| **Uzbrojona** | Uzbraja zadaną strefę i zaczyna od czasu na wyjście sygnalizowanego brzęczykiem, trwającego 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej), a w tym czasie wszystkie strefy alarmowe zachowują się jak strefy z reakcją opóźnioną. Przedłużony czas sygnalizacji dźwiękowej wyjścia ostrzega użytkowników znajdujących się w chronionym obiekcie, informując ich o uzbrojeniu systemu przez automatyczny zegar. W tym czasie użytkownik musi natychmiast przejść do klawiatury systemu i rozbroić strefę w zwykły sposób lub opuścić chroniony obiekt. Jeżeli zignoruje to ostrzeżenie i pozostanie w budynku, po którym będzie się poruszał, dojdzie do aktywacji alarmu.<br>Centrala alarmowa w pełni przestrzega zasad uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Częściowo uzbrojona** | Uzbraja zadaną strefę częściowo i zaczyna od czasu na wyjście sygnalizowanego brzęczykiem, trwającego 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej), a w tym czasie wszystkie strefy alarmowe zachowują się jak strefy z reakcją opóźnioną. Przedłużony czas sygnalizacji dźwiękowej wyjścia ostrzega użytkowników znajdujących się w chronionym obiekcie, informując ich o częściowym uzbrojeniu systemu przez automatyczny zegar. Uzbrojenie częściowe zwykle nie posiada sygnalizacji dźwiękowej (sposób jej aktywacji znajduje się w zakładce Parametry). Centrala alarmowa w pełni przestrzega zasad uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Uzbrojona natychmiastowo** | Uzbraja zadaną strefę natychmiastowo, bez opóźnienia na wyjście ani sygnalizacji dźwiękowej. System zostaje uzbrojony natychmiast, w związku z czym nie jest możliwy ruch w chronionym obiekcie. Jeżeli po samoczynnym uzbrojeniu ktoś będzie nadal chodził po obiekcie, dojdzie do aktywacji alarmu w uzbrojonej strefie/strefach. Ta opcja służy do szybkiego i cichego uzbrajania bez ostrzeżenia. Centrala alarmowa w pełni przestrzega zasad uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Częściowo uzbrojona teraz** | Uzbraja zadaną strefę częściowo i natychmiastowo, bez opóźnienia na wyjście ani sygnalizacji dźwiękowej. System zostaje uzbrojony natychmiast w zadanym czasie. Ta opcja służy do szybkiego i cichego uzbrajania bez ostrzeżenia. Centrala alarmowa w pełni przestrzega wszystkich sposobów uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |

| | |
|---|---|
| **Uzbrój zawsze** | Uzbraja zadaną strefę i zaczyna od czasu na wyjście sygnalizowanego brzęczykiem, trwającego 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej), a w tym czasie wszystkie strefy alarmowe zachowują się jak strefy z reakcją opóźnioną. Centrala alarmowa nie przestrzega w pełni sposobów uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Uzbrój częściowo zawsze** | Uzbraja zadaną strefę częściowo i zaczyna od czasu na wyjście sygnalizowanego brzęczykiem, trwającego 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej), a w tym czasie wszystkie strefy alarmowe zachowują się jak strefy z reakcją opóźnioną. Centrala alarmowa nie przestrzega w pełni sposobów uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Uzbrój zawsze natychmiast** | Uzbraja zadaną strefę natychmiastowo, bez opóźnienia na wyjście ani sygnalizacji dźwiękowej.<br>System zostaje uzbrojony natychmiast, w związku z czym nie jest możliwy ruch w chronionym obiekcie.<br>Ta opcja służy do szybkiego i cichego uzbrajania bez ostrzeżenia. Centrala alarmowa nie przestrzega w pełni sposobów uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Uzbrój częściowo zawsze i natychmiast** | Uzbraja zadaną strefę częściowo i natychmiastowo, bez opóźnienia na wyjście ani sygnalizacji dźwiękowej. System zostaje uzbrojony natychmiast w zadanym czasie. Ta opcja służy do szybkiego i cichego uzbrajania bez ostrzeżenia. Centrala alarmowa nie przestrzega w pełni sposobów uzbrajania i sprawdzania gotowości systemów do uzbrojenia. |
| **Rozbrój** | Rozbrajanie zadanej strefy z dowolnego poziomu strzeżenia (uzbrojenie całkowite lub częściowe). |
| **Nie** | Brak zadanej funkcji sterowania. |

**Opcje sterowania wyjściem PG przy użyciu kalendarza:**

| | |
|---|---|
| **Aktywuj PG** | Aktywuje wyjścia programowalne, jeżeli nie są one zablokowane (np. przy użyciu kalendarza, urządzenia lub strefy). |
| **Dezaktywuj PG** | Dezaktywuje programowalne wyjścia PG. |
| **Zablokuj PG** | Blokuje zadane wyjścia PG. Tych wyjść nie będzie można włączyć, dopóki nie zostaną one odblokowane zadaniem kalendarza „Odblokuj PG". Wejście do lub opuszczenie trybu serwisowego<br>nie powoduje ich odblokowania. |
| **Odblokuj PG** | Odblokowuje blokadę zadanych wyjść PG. |
| **Nie** | Nie zadano funkcji blokowania. |

**Zadanie blokowania funkcji przy użyciu kalendarza:**

Każdą planowaną czynność można zablokować jednym opcjonalnym wyjściem PG. Blokowanie oznacza: kiedy wyjście PG jest aktywne, nie dojdzie do realizacji konkretnego zadania w zadanym czasie. Blokowaniem może być na przykład zablokowane zadanie kalendarza do rozbrojenia przed wyjazdem na wakacje. Blokowanie może sygnalizować przycisk funkcji na klawiaturze (zadany na WŁ/WYŁ wyjścia PG) o nazwie „Wakacje", itp.

## 9.5 Sterowanie systemem przy użyciu menu głosowego komunikatora uzupełniającego (GSM / PSTN)

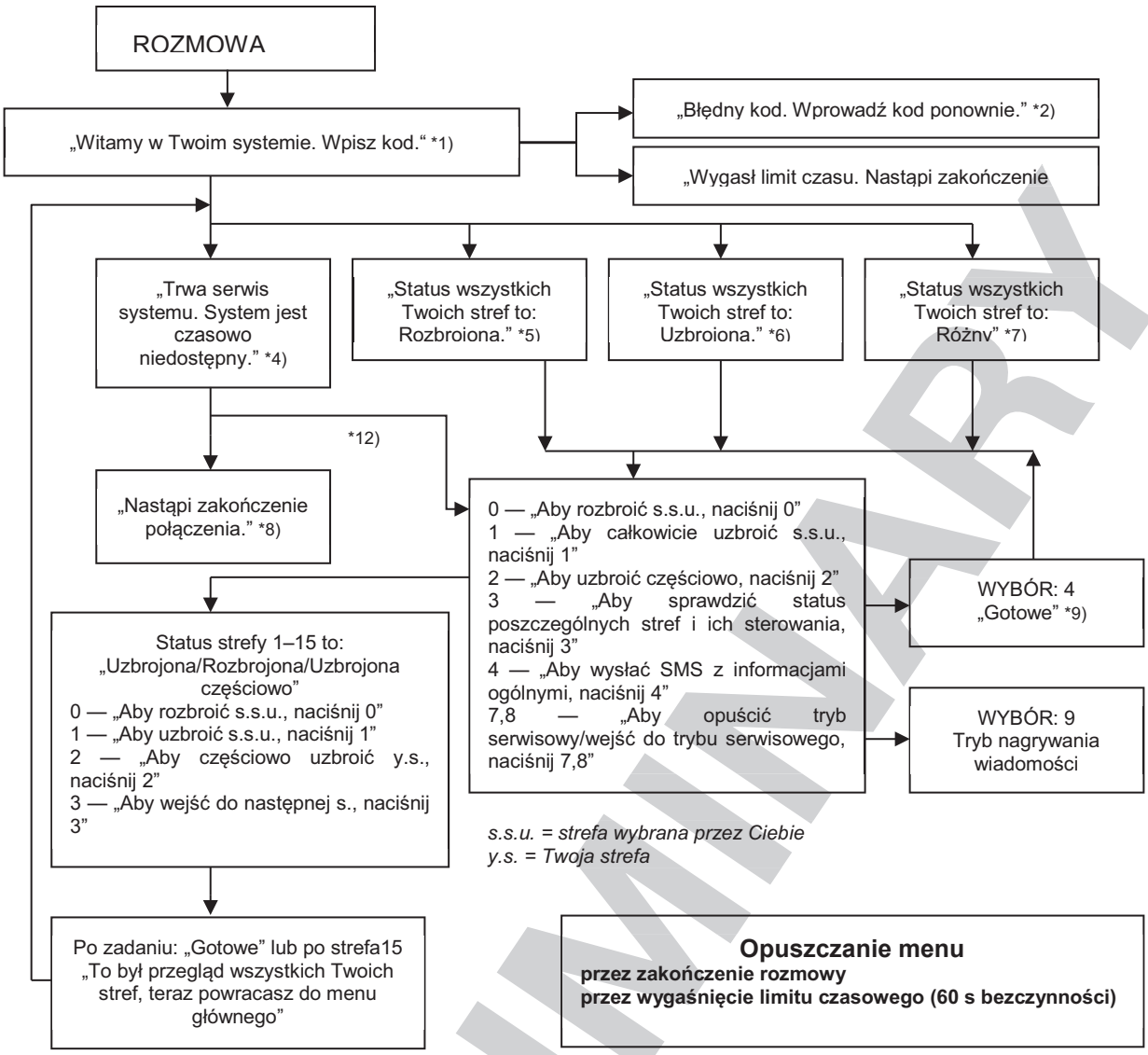
Systemem zabezpieczeń można sterować zdalnie przy użyciu komunikatora uzupełniającego (GSM lub PSTN) oraz tonów DTMF na telefonie komórkowym dzwoniącego. Ustanawiając połączenie ze znanego numeru telefonu z kartą SIM lub telefonu stacjonarnego, system wybiera połączenie po zadanej liczbie sygnałów (domyślnie 3 sygnały), centrala alarmowa odtwarza powitalną wiadomość głosową i, zależnie od ustawień, może wymagać wprowadzenia prawidłowego kodu. Dzwoniący musi dokonać uwierzytelnienia przy użyciu własnego kodu dostępu. Po udanej weryfikacji kodu system przekazuje status całego systemu i zależnie od uprawnień dzwoniącego oferuje dostępne opcje sterowania. Za pomocą menu głosowego można sterować strefami, wchodzić w tryb serwisowy i go opuszczać, a także rejestrować wiadomości głosowe z nazwami poszczególnych stref i raportami specjalnymi. Za pośrednictwem menu głosowego nie można sterować wyjściami PG.

***Uwaga**: Przed zdalnym uzbrojeniem systemu należy sprawdzić, czy w chronionym obiekcie nie ma innych osób.*



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

**Przegląd menu głosowego:**




*1) Odpowiada po 3 sygnałach. Liczbę sygnałów do odpowiedzi (1.10) można ustawić w zakładce Komunikacja oraz zakładce odpowiedniego komunikatora, gdzie można umożliwić wejście w menu głosowe bez kodu.
*2) Wprowadzenie błędnego kodu. Po trzecim wprowadzeniu błędnego kodu nastąpi zakończenie połączenia.
*3) Limit czasowy 60 s na wprowadzenie kodu. Żądanie „Wpisz kod” zostaje powtórzone co 5 s.
*4) Menu głosowego nie można używać podczas serwisu.
*5) Wszystkie strefy, którymi można sterować na podstawie uwierzytelnienia, są rozbrojone.
*6) Wszystkie strefy, którymi można sterować na podstawie uwierzytelnienia, są uzbrojone.
*7) Wszystkie strefy, którymi można sterować na podstawie uwierzytelnienia, posiadają różne statusy.
*8) Obowiązuje dla wszystkich uprawnień z wyjątkiem SMA / Serwis.
*9) Po wysłaniu SMS INFO na numer dzwoniącego.
*10) Punkty w menu, które nie mają sensu, zostają pominięte (np. jeżeli wszystko jest uzbrojone, wybór 1,2,3 nie obowiązuje).
*11) Menu dostosowuje się do aktualnego statusu strefy.
*12) Jeżeli użytkownik dokonał uwierzytelnienia przy użyciu kodu serwisowego, możliwy jest wybór 9 — „Aby wejść w tryb nagrywania wiadomości głosowych, naciśnij 9”
*13) Tryb nagrywania wiadomości głosowych **WYBÓR 9:**

0 — „Aby zarejestrować nazwę instalacji, naciśnij 0.”, a następnie „Naciśnij gwiazdkę (*)”
1 — „Aby zarejestrować nazwy stref, naciśnij 1”, a potem wpisz numer strefy, którą chcesz zarejestrować i „Naciśnij gwiazdkę (*)”.
9 — „Aby usunąć wszystkie nagrane wiadomości, naciśnij 9.”
# — „Aby powrócić do menu głównego, naciśnij #.”

**Uwagi:**

- 1 — „nie masz uprawnień do tego wyboru — zawsze, jeżeli użytkownik nie posiada uprawnień dla danej strefy ani sprawdzania statusu
- 2 — „wymagane zgłoszenie ważnej wiadomości, połączenie zostanie zakończonej w ciągu 30 sekund" — raporty / ważne wiadomości do SMA posiadają priorytet względem bieżącego menu głosowego
- Wprowadzenie w trybie rejestrowania jest sygnalizowane piknięciem. Zarejestrowany komunikat zostanie odtworzony tuż po jego rejestracji.
- Jeżeli nie są Państwo zadowoleni z nagrania, można natychmiast wybrać ponowne nagrywanie.
- Zaleca się rozpoczęcie nagrywania bezpośrednio po sygnale dźwiękowym, a po zakończeniu nagrywania naciśnięcie znaku końcowego*.
- Nazwa instalacji może trwać najwyżej 40 sekund. Każdy inny komunikat może mieć długość najwyżej 20 sekund.

## 9.6 Polecenia SMS

Systemem można sterować przy użyciu poleceń SMS dzięki uzupełniającemu komunikatorowi GSM. Polecenia SMS można wykorzystać do sterowania statusami poszczególnych stref (uzbrajanie, rozbrajanie), lub zadawania zapytań o statusy poszczególnych stref lub inne statusy całego systemu. Teksty polecenia używanego do sterowania wyjściami PG można edytować, pozostałych tekstów nie można zmieniać. Nie ma poleceń fabrycznych do sterowania wyjściami PG, należy je najpierw skonfigurować. Pozostałe teksty zostały skonfigurowane fabrycznie.

**Struktura polecenia SMS:**

**kkkk_polecenie**

gdzie: **kkkk** to kod użytkownika;

_ to spacja oddzielająca;

**polecenie** oznacza polecenie wykonawcze (patrz wykaz poleceń poniżej).

**Polecenia zapytania:**

informacje o statusie systemu można uzyskać także przy użyciu następujących poleceń

***DINFO, STATUS, COM i GSM*** (tekstów poleceń nie można zmienić).

**Polecenie sterowania:**

sterowanie konfiguracją **systemu** jako całości lub poszczególnych **stref** można realizować przy użyciu następujących poleceń:

***UZBRÓJ, ROZBRÓJ, lub UZBRÓJxxx, ROZBRÓJxxx, gdzie x oznacza numery stref, oddzielone spacją*** (tekstu poleceń nie można zmienić).

Polecenia sterowania do sterowania wyjściami **PG** nie zostały ustawione fabrycznie i w razie potrzeby należy je skonfigurować.

**Przestroga:** Jeżeli polecenia sterowania zawierają akcentowane znaki diakrytyczne (jak np. w języku GR i RU), należy aktywować parametr Znaki diakrytyczne w zakładce Komunikacja pod przyciskiem „Ustawienia JA-190Y", aby zapewnić prawidłowe i niezawodne funkcjonowanie. Po aktywacji znaków diakrytycznych należy zwracać uwagę na małe i wielkie litery. W przypadku zwykłych znaków wielkość nie ma znaczenia.



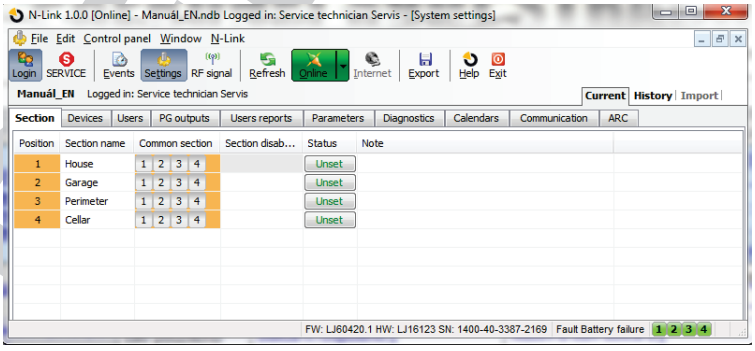
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

| Polecenie sterowania i uprawnienia | Odpowiedź (próbka) | Uwaga |
|---|---|---|
| **DINFO** (podstawowe informacje o instalacji)<br><br>**Uprawnienia:** Serwis, Administrator | JABLOTRON 100:<br>TYP: JA-100K,<br>Numer seryjny: 14004026532523,<br>Oprogramowanie: LJ60420,<br>Sprzęt: LJ16123,<br>RC: 79167-5FYA9-ZSQJ,<br>GSM: 90%, GPRS:ok,<br><br>LAN: wył.<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Typ centrali alarmowej<br>Numer seryjny<br>Wersja firmware<br>Wersja sprzętu<br>Kod rejestracji komunikatora GSM<br>Jakość sygnału GSM, dostępność danych GPRS<br><br>Status połączenia LAN (OK lub WYŁ)<br>Data i godzina przekazania SMS do sieci GSM |
| **STATUS** (status stref)<br><br>**Uprawnienia:** Serwis, Administrator, Użytkownik. Jeżeli użytkownik posiada jedynie dostęp do niektórych stref, zostanie zwrócony status stref, do których ma dostęp. | JABLOTRON 100:<br>Status:<br>Strefa 1: Rozbrojona;<br>Strefa 2: Uzbrojona;<br>Strefa 3: Rozbrojona;<br>Strefa 4: Uzbrojona, Błąd;<br><br>GSM: 90%;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Status:<br>Nazwa i status Strefy 1<br>Nazwa i status Strefy 2<br>Nazwa i status Strefy 3<br>Nazwa i status Strefy 4<br><br>Jakość sygnału GSM<br>Data i godzina wysłania SMS do sieci GSM |
| **COM** (informacje dot. komunikacji)<br><br>**Uprawnienia:** Serwis | JABLOTRON 100:<br>GSM: 90%,DANE: ok,<br>CELLID: 44905, OPID: 23003,<br>LAN: ok, MAC: hh:hh:hh:hh:hh:hh,<br>PSTN: wył.,<br>SMA: 1:ok, 2:ok, 3:wył., 4:ok, 5:wył.,<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Jakość sygnału GSM, dostępność danych GPRS<br>Numer telefonu komórkowego i operator zapewniający połączenie GSM<br>Status połączenia LAN i adres MAC<br>Status połączenia linii telefonicznej (możliwy w przypadku JA-190X)<br>Status aktywacji transmisji poszczególnych SMA<br>Data i godzina przekazania SMS do sieci GSM |
| **GSM** (ponowne uruchomienie GSM)<br><br>**Uprawnienia:** Serwis, Administrator, Użytkownik | JABLOTRON 100:<br>SMS przetworzony OK: GSM;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Potwierdzenie dostarczenia SMS (przed ponownym uruchomieniem)<br>Data i godzina przekazania SMS do sieci GSM |
| **UZBROJONY** (sterowanie całym systemem)<br><br>**Uprawnienia:** Wszystkie | JABLOTRON 100:<br>Status:<br>Strefa 1: Uzbrojona;<br>Strefa 2: Uzbrojona;<br>Strefa 3: Uzbrojona ze strefą aktywną;<br>Strefa 4: Uzbrojona, Błąd;<br><br>GSM: 90%;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Status:<br>Nazwa i status Strefy 1<br>Nazwa i status Strefy 2<br>Nazwa i status Strefy 3<br>Nazwa i status Strefy 4<br><br>Jakość sygnału GSM<br>Data i godzina wysłania SMS do sieci GSM |

| | | |
|---|---|---|
| **ROZBROJONY** (sterowanie całym systemem)<br><br>**Uprawnienia:** Wszystkie | JABLOTRON 100:<br>Status:<br>Strefa 1: Rozbrojona;<br>Strefa 2: Rozbrojona;<br>Strefa 3: Rozbrojona;<br>Strefa 4: Rozbrojona, Błąd;<br>GSM: 90%;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Status:<br>Nazwa i status Strefy 1<br>Nazwa i status Strefy 2<br>Nazwa i status Strefy 3<br>Nazwa i status Strefy 4<br>Jakość sygnału GSM<br>Data i godzina wysłania SMS do sieci GSM |
| **UZBROJONA 1 3** (sterowanie wybranymi strefami w systemie)<br><br>**Uprawnienia:** Wszystkie | JABLOTRON 100:<br>Status:<br>Strefa 1: Uzbrojona;<br>Strefa 3: Uzbrojona ze strefą aktywną;<br>GSM: 90%;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Status:<br>Nazwa i status Strefy 1<br>Nazwa i status Strefy 3<br>Jakość sygnału GSM<br>Data i godzina wysłania SMS do GSM |
| **ROZBROJONA 2 4** (sterowanie wybranymi strefami w systemie)<br>**Uprawnienia:** Wszystkie | JABLOTRON 100:<br>Status:<br>Strefa 2: Rozbrojona;<br>Strefa 4: Rozbrojona;<br>GSM: 90%;<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Status:<br>Nazwa i status Strefy 2<br>Nazwa i status Strefy 4<br>Jakość sygnału GSM<br>Data i godzina wysłania SMS do GSM |
| **CREDIT (KREDYT)** (sprawdzanie salda kredytów na karcie SIM typu pre-paid)<br>**Uprawnienia:** Wszystkie | JABLOTRON 100:<br>…<br>…<br>…<br>Godzina 17:01 22.7. | Nazwa instalacji zgodnie z zakładką Komunikacja<br>Tekst z odpowiedzi dostawcy GSM<br>Tekst z odpowiedzi dostawcy GSM<br>Tekst z odpowiedzi dostawcy GSM<br>Data i godzina wysłania SMS do GSM |

## 9.7 Sterowanie systemem przy pomocy programu F-Link

Program F-Link służy do lokalnego i zdalnego programowania całego systemu lub edycji użytkownika. Zapewnia przegląd statusów stref i sterowanie strefami. Sterowanie jest możliwe po kliknięciu zakładki „Strefa" w kolumnie „status", a także po kliknięciu numeru strefy na dolnym pasku statusu. System rejestruje sterowanie systemem w pamięci zdarzeń zgodnie z uprawnieniami po uwierzytelnieniu użytkownika w programie.




## 9.8 Sterowanie za pomocą aplikacji sieciowej MyJABLOTRON

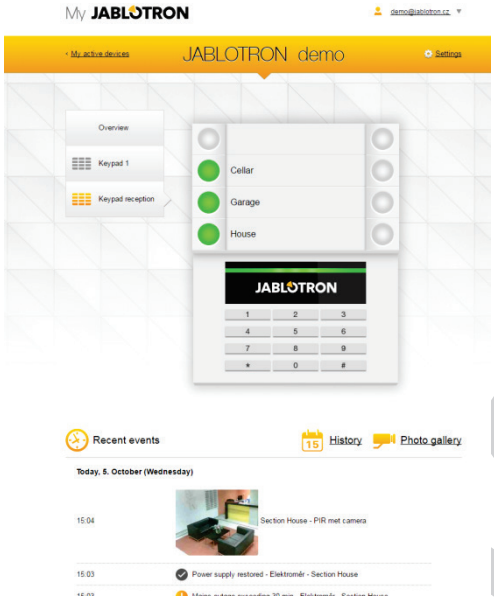
Zdalne sterowanie przy pomocy aplikacji sieciowej MyJABLOTRON jest najbardziej przyjaznym dla użytkownika sposobem sterowania systemem zabezpieczeń z dowolnej przeglądarki internetowej niezależnie od platformy komputerowej. Po zalogowaniu aplikacja pozwala sterować systemem nie tylko przy pomocy wirtualnej klawiatury każdej fizycznej klawiatury w systemie, ale także sterować strefami i wyjściami PG z listy ogólnej. Użytkownik może także przeglądać szczegółową historię zdarzeń, w tym wykonane zdjęcia. Na żądanie użytkownika można natychmiast wykonać nowe zdjęcia. W przeciwieństwie do systemu fizycznego, użytkownik może sprawdzić aktualne temperatury na termometrach, wartości na różnych licznikach, a także



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

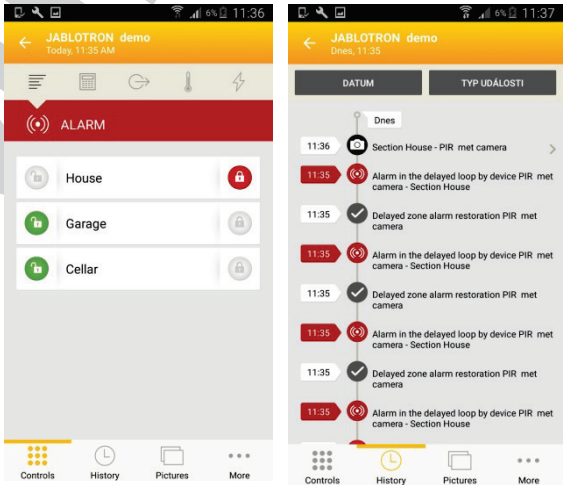
konfigurować wiadomości informujące o zdarzeniach w systemie lub przekroczeniu wartości zadanych przez użytkownika (jak temperatura).

Przy każdym logowaniu w celu sterowania systemem należy dokonać uwierzytelnienia przy pomocy kodu użytkownika. Uzbrajanie stref przy użyciu przycisków funkcyjnych odpowiada ich faktycznej konfiguracji. Jeżeli przyciski funkcji umożliwiają uzbrojenie częściowe, można uzbroić system częściowo zdalnie. We wszystkich innych przypadkach sterowanie przy użyciu listy zawsze uzbraja całe strefy.




## 9.9 Sterowanie za pomocą aplikacji mobilnej MyJABLOTRON

Użytkownicy aplikacji MyJABLOTRON mogą pobrać aplikację na urządzenia mobilne. Dostępna na system iOS i Android.Aplikacja mobilna jest najbardziej przyjaznym dla użytkownika sposobem sterowania systemem zabezpieczeń. Użytkownik może go nosić w kieszeni dzięki niemal nieograniczonemu dostępowi do internetu. Po zalogowaniu aplikacja pozwala sterować systemem nie tylko przy pomocy wirtualnej klawiatury każdej fizycznej klawiatury w systemie, ale także sterować strefami i wyjściami PG z listy ogólnej.




## 9.10 Sterowanie za pomocą Antynapadowej kontroli dostępu

Ta opcja, domyślnie wyłączona w ustawieniach fabrycznych, pozwala użytkownikom sterować (uzbrajać lub rozbrajać) systemem przy użyciu innego kodu w przypadku zagrożenia ze strony innej osoby. Kod dyskretnie zwróci uwagę na taką sytuację, uruchamiając cichy alarm panika bez sygnalizacji dźwiękowej ani świetlnej. Alarm panika uruchomi się po dodaniu 1 do istniejącego kodu użytkownika.

**Przykład:**

Kod użytkownika = 4444 Kod Antynapadowej kontroli dostępu = 444**5**

***Ostrzeżenie:*** Jeżeli kod użytkownika kończy się na cyfrę 9 podczas Antynapadowej kontroli dostępu, wówczas ostatnią cyfrą kodu będzie **0 (4449 – 4440).**

## 9.11 Przeszkody uniemożliwiające uzbrojenie systemu

Zgodnie ze **Sposobami uzbrajania** (patrz zakładka Parametry) centrala alarmowa może podczas uzbrajania poszczególnych stref systemu sprawdzać obecność statusu aktywacji lub błędu poszczególnych urządzeń lub danej strefy systemu. Zgodnie z tą opcją centrala alarmowa sygnalizuje pewne przeszkody podczas uzbrajania (przeszkody do obejścia) oraz niektóre statusy, a także może nawet uniemożliwić uzbrajanie systemu w razie ich wystąpienia (przeszkody niemożliwe do obejścia).

Jedną z najpowszechniejszych przeszkód jest błąd systemu (sygnalizowany żółtą kontrolą systemu), utrata połączenia z czujką bezprzewodową lub czujka aktywna (zwykle magnetyczny czujnik otwarcia) z reakcją opóźnioną (czujniki drzwi frontowych i bramy garażu), niski poziom baterii w systemie, długotrwała awaria zasilania lub błąd komunikacji na jednym z komunikatorów. Wpływa na to profil systemu.

Przeszkodą niemożliwą do obejścia, uniemożliwiającą uzbrojenie systemu, jest na przykład **aktywna czujka** (zwykle magnetyczna czujnik otwarcia drzwi) ustawiona na reakcję **natychmiastową**. Urządzenia należące do tej grupy to czujniki otwarcia okna, drzwi balkonowych lub drzwi tylnych, ale może chodzić także o krytyczne błędy systemu, jak błąd zasilania awaryjnego lub błąd komunikacji ze SMA. Przyczyny uniemożliwiające uzbrojenie systemu różnią się zależnie od zadanego profilu systemu. Wyjątkiem, który nie uniemożliwia systemowi uzbrojenia strefy, i w którym system nie sprawdza obecności aktywnych czujek lub błędów, jest automatyczne uzbrajanie przy pomocy kalendarza z aktywną opcją „Uzbrój ... zawsze". Kalendarz zawsze uzbroi każdą strefę pod warunkiem, że skonfigurowano go na wykonanie takiej czynności.

Aktywacja czujki impulsów (np. czujki ruchu, zbicia szyby, wychylenia, wstrząsów itp.) nie mogą uniemożliwić uzbrajania.

System powiadomi Państwa o uzbrojeniu ze strefą aktywną przy użyciu raportu SMS (dla grupy użytkowników z zadanymi raportami alarmów) ze szczegółowym opisem.

**Sposoby uzbrajania — zestawienie w tabeli**

| | Klawiatura systemu | Za pomocą menu głosowego/SMS/ manipulatora zdalnego/kalendarza | F-Link J-Link | Aplikacja sieciowa i mobilna |
|---|---|---|---|---|
| **Uzbrój zawsze** | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń |
| **Uzbrój z ostrzeżeniem** | Podczas próby uzbrajania w obecności błędu lub aktywnego urządzenia klawiatura miga przez 8 sekund, a później system dokonuje automatycznego uzbrojenia. Można uzbroić system przez ponowne naciśnięcie przycisku funkcji lub klawisza Enter. | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zależnie od „Sposobów uzbrajania" w zakładce Konfiguracja serwisowa |
| **Uzbrój po potwierdzeniu** | Podczas próby uzbrajania w obecności błędu lub aktywnego urządzenia klawiatura miga przez 8 sekund, a później system dokonuje automatycznego uzbrojenia. Można uzbroić system przez ponowne naciśnięcie przycisku funkcji lub klawisza Enter. | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zawsze, pomimo błędów lub stanu aktywnych urządzeń | Uzbroi zgodnie ze „Sposobami uzbrajania" (z opcją Uzbrój z kontrolą / Uzbrój bez kontroli) w zakładce Konfiguracji serwisowej |
| **Nie uzbroi z aktywnym elementem** | Podczas próby uzbrajania w obecności błędu lub aktywnego urządzenia klawiatura miga przez 8 sekund, a później system dokonuje automatycznego uzbrojenia. Można uzbroić system przez ponowne naciśnięcie przycisku funkcji lub klawisza Enter. | Nie uzbroi, kiedy aktywną czujkę ustawiono na reakcję NATYCHMIASTOWĄ | Uzbroi zawsze pomimo błędów lub aktywnego statusu urządzeń | Nie uzbroi, kiedy aktywną czujkę ustawiono na reakcję NATYCHMIASTOWĄ |



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

## 9.12 Niepowodzenie uzbrojenia

Jest to funkcja bezpieczeństwa, dzięki której centrala alarmowa sprawdza w czasie opóźnienia na wyjście, czy można uzbroić system i czy zabezpieczenie chronionego obiektu nie jest ograniczone w poniższych przypadkach. Jeżeli ta funkcja jest aktywna, **niepowodzenie uzbrojenia** może wynikać z:

1. Natychmiastowej aktywacji czujki w dowolnej chwili podczas opóźnienia na wyjście (ktoś wejdzie do już chronionego obszaru)
2. stałej aktywacji czujki z reakcją opóźnioną po wygaśnięciu czasu na wyjście (użytkownik zapomniał zamknąć drzwi główne, bramę garażu lub bramę itp.)

Jeżeli uzbrojenie systemu nie jest możliwe, aktywuje się zdarzenie „Niepowodzenie uzbrojenia", co sygnalizuje gwałtowne miganie żółtej kontrolki systemu na klawiaturze oraz brzęczyk, a także sygnał dźwiękowy syreny zewnętrznej. Jednocześnie zostano ono zgłoszone konkretnemu użytkownikowi lub administratorowi systemu w formie raportu „Aktywowano niepowodzenie uzbrajania, patrz program F-Link, zakładka Komunikacja".

Aby anulować sygnalizację niepowodzenia uzbrajania, należy w menu klawiatury zaznaczyć opcję „Anuluj ostrzeżenie" lub uzbroić daną sekcję, jeżeli zadano „Domyślny" profil systemu.

## 9.13 Zestawienie tabelaryczne Grup zdarzeń zgłaszanych użytkownikom

W przypadku podłączenia uzupełniającego komunikatora GSM lub PSTN zdarzenia w systemie można wysłać nie tylko do SMA, ale także do maks. 8 użytkowników (alarmy, połączenia głosowe i raporty SMS). Zdarzenia zgłaszane użytkownikom podzielono na 5 grup. Każdą grupę można swobodnie przypisywać do użytkowników. Użytkownicy, którym przypisano grupę, otrzymają raporty z tej grupy. Jeżeli podstawowe ustawienia grup nie wystarczą, można wykorzystać 2 specjalne grupy, określane przez użytkowników. Do tych grup można dodać wybrane zdarzenia, i na tej podstawie są one zgłaszane tylko konkretnym użytkownikom.

**Przegląd tabelaryczny:**

| Porządek | Zdarzenie | Grupa |
|---|---|---|
| 1 | Uzbrojenie | SMS dot. Uzbrojenia / Rozbrojenia (3) |
| 2 | Rozbrojenie | SMS dot. Uzbrojenia / Rozbrojenia (3) |
| 3 | Uzbrojenie częściowe | SMS dot. Uzbrojenia / Rozbrojenia (3) |
| 4 | Awaria zasilania 30 minut | Alerty SMS (1) / Połączenie alarmowe (2) |
| 5 | Przywrócenie zasilania po upływie 30 minut | Alerty SMS (1) / Połączenie alarmowe (2) |
| 6 | Alarm natychmiastowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 7 | Anulowano alarm natychmiastowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 8 | Alarm opóźniony | Alerty SMS (1) / Połączenie alarmowe (2) |
| 9 | Anulowano alarm opóźniony | Alerty SMS (1) / Połączenie alarmowe (2) |
| 10 | Alarm sabotażowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 11 | Anulowano alarm sabotażowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 12 | Alarm pożarowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 13 | Anulowano alarm pożarowy | Alerty SMS (1) / Połączenie alarmowe (2) |
| 14 | Alarm panika | Alerty SMS (1) / Połączenie alarmowe (2) |
| 15 | Anulowano alarm panika | Alerty SMS (1) / Połączenie alarmowe (2) |
| 16 | Problemy zdrowotne | Alerty SMS (1) / Połączenie alarmowe (2) |
| 17 | Zalanie | Alerty SMS (1) / Połączenie alarmowe (2) |
| 18 | Próba złamania kodu | Alerty SMS (1) / Połączenie alarmowe (2) |
| 19 | Uzbrojono ze strefą aktywną (przy aktywnym potwierdzeniu) | Alerty SMS (1) / Połączenie alarmowe (2) |
| 20 | Strefa bez ruchu | Alerty SMS (1) / Połączenie alarmowe (2) |
| 21 | Aktywacja przegrzania | Alerty SMS (1) / Połączenie alarmowe (2) |
| 22 | Dezaktywacja przegrzania | Alerty SMS (1) / Połączenie alarmowe (2) |
| 23 | Aktywacja zamarzania | Alerty SMS (1) / Połączenie alarmowe (2) |
| 24 | Dezaktywacja zamarzania | Alerty SMS (1) / Połączenie alarmowe (2) |
| 25 | Uruchomienie systemu (poza trybem serwisowym) | SMS o błędzie i serwisie (5) |
| 26 | Niski poziom baterii w urządzeniu | SMS o błędzie i serwisie (5) |
| 27 | Poziom baterii w urządzeniu OK | SMS o błędzie i serwisie (5) |
| 28 | Błąd (urządzenie, komunikator) | SMS o błędzie i serwisie (5) |

| | | |
|---|---|---|
| 29 | Koniec błędu | SMS o błędzie i serwisie (5) |
| 30 | Wejście w tryb serwisowy | SMS o błędzie i serwisie (5) |
| 31 | Wyjście z trybu serwisowego | SMS o błędzie i serwisie (5) |
| 32 | Niski poziom BATERII | SMS o błędzie i serwisie (5) |
| 33 | BATERIA OK | SMS o błędzie i serwisie (5) |
| 34 | Błąd komunikacji z SMA | SMS o błędzie i serwisie (5) |
| 35 | Przywrócenie komunikacji ze SMA | SMS o błędzie i serwisie (5) |
| 36 | Tłumienie RF | SMS o błędzie i serwisie (5) |
| 37 | Koniec tłumienia RF | SMS o błędzie i serwisie (5) |
| 38 | Niskie saldo kredytu | SMS o błędzie i serwisie (5) |
| 39 | Zdjęcie alarmowe | Zdjęcie (4) |

Przypisywanie zdarzeń rozpoznawanych przez system do grup podano w tabeli. W chwili wystąpienia zdarzenia system generuje wiadomość SMS w następującym formacie:

**Nazwa instalacji** (patrz zakładka Konfiguracja komunikacji):

**Godzina** (wystąpienia zdarzenia), **Zdarzenie** (patrz tabela).

**Źródło zdarzenia** (patrz zakładka Urządzenia/Nazwa lub Użytkownik/Nazwa), **Strefa** (gdzie wystąpiło zdarzenie);

**Godzina** (godzina i data wysłania)

*Przykładowa, wysłana wiadomość SMS:*

***JABLOTRON 100*** *(nazwa instalacji)*
***17:01:10, Alarm opóźniony*** *(godzina zdarzenia, zdarzenie)*
***Magnes drzwiowy, Parter*** *(nazwa czujki, nazwa strefy)*
***17:01:25, Alarm natychmiastowy*** *(godzina zdarzenia, zdarzenie)*
***Ruch na klatce schodowej, na górze*** *(nazwa czujki, nazwa strefy)*
***Godzina 17:01 22.7.*** *(godzina wysłania)*

## 9.14 Sygnalizacja dźwiękowa systemu

Sygnalizacja dźwiękowa systemu może wskazywać nie tylko status alarmu, ale także informować o innych statusach lub ich zmianach. Przegląd sygnalizacji dźwiękowej podano w następujących tabelach:

**Sygnalizacja dźwiękowa ze strony klawiatury / czytnika:**

| Dźwięk | Opis działania |
|---|---|
| Jeden krótki dźwięk | Potwierdzenie naciśnięcia przycisku |
| Jeden długi dźwięk | Aktywacja przycisku funkcji, uzbrajanie strefy lub włączanie PG |
| Dwa długie dźwięki | Dezaktywacja przycisku funkcji, rozbrajanie strefy lub wyłączanie PG |
| Dwa długie, powtórzone dźwięki | Niepowodzenie uzbrojenia |
| Trzy długie dźwięki | Rozbrojenie strefy z sygnalizacją pamięci alarmów |
| Ciągłe pikanie | Opóźnienie na wyjście |
| Dźwięk ciągły | Opóźnienie na wejście |
| | Alarm |

**Sygnalizacja dźwiękowa przez syreny wewnętrzne / zewnętrzne:**

| Dźwięk | Opis działania |
|---|---|
| Jeden krótki dźwięk | Uzbrajanie strefy |
| | Włączenie wyjścia PG |
| Dwa krótkie dźwięki | Rozbrajanie strefy |
| | Wyłączenie wyjścia PG |
| Trzy krótkie dźwięki | Rozbrojenie strefy z sygnalizacją pamięci alarmów |
| | Niepowodzenie uzbrojenia |
| | Uzbrojenie ze strefą aktywną (tylko do FW 13) |
| Ciągłe, szybkie pikanie | Sygnalizacja statusu PG — szybkie pikanie |
| Ciągłe, powolne pikanie | Opóźnienie na wyjście |
| | Sygnalizacja statusu PG — powolne pikanie |



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

| | |
|---|---|
| Dźwięk ciągły | Opóźnienie na wejście |
| | Sygnalizacja statusu PG — ciągłe piszczenie |
| Trąbienie | Alarm w strefie |

**Sygnalizacja dźwiękowa czujek pożarowych (dym, temperatura, gaz):**

| Dźwięk | Opis działania |
|---|---|
| Ciągłe, szybkie pikanie | Alarm pożarowy |
| Ciągłe wołanie | |

## 9.15 Dezaktywacja i blokowanie opcji

### 9.15.1 Dezaktywacja

Przed uzbrojeniem systemu może wystąpić sytuacja, w której konieczne będzie celowe pominięcie urządzenia w procesie zapewniania ochrony (np. w garażu ze względu na prace budowlane lub zostawienie psa w zwykle chronionym pomieszczeniu). Tę opcję nazywa się **Dezaktywacją urządzenia**. Jest ona dostępna dla serwisanta w menu klawiatury lub za pośrednictwem programu F-Link i można ją zrealizować na dwóch poziomach zależnie od uprawnień użytkownika:

1. **Blokowanie wyjścia (BLK)** — funkcja służy do blokowania wejścia czujki (blokuje jego aktywację). System ignoruje wszelkie aktywacje czujki = nie aktywuje się alarm, nie zgłasza aktywacji PG. Cały czas trwa nadzór pod kątem alarmów sabotażu, błędów lub raportów niskiego stanu baterii. W programie F-Link sygnalizuje je żółta kropka. Do blokowania uprawniony jest Administrator oraz Serwisant.
2. **Dezaktywacja urządzenia (DIS)** — ta funkcja służy do dezaktywacji czujki. System ignoruje wszystkie funkcje urządzenia = nie aktywuje alarmów, w tym alarmów sabotażu, raportów ani błędów. W programie F-Link sygnalizuje je czerwona kropka. Do dezaktywacji uprawniony jest jedynie Serwisant.

Można **Dezaktywować** nie tylko urządzenie, ale także strefę, przy czym może być to wyłącznie strefa bez centrali alarmowej, dotyczy to także użytkowników z wyjątkiem pozycji 0 (serwisant) i 1 (Administrator), wyjść PG lub zadań kalendarzowych. Dezaktywacja ma charakter trwały do chwili jej anulowania przy pomocy procedury stosowanej do jej włączenia.

***Uwaga**: Nie można zablokować ani dezaktywować centrali alarmowej ani urządzenia z reakcją panika!*

## 9.16 Funkcje niealarmowe — Funkcje wyjść PG

System zabezpieczeń pozwala uprawnionym użytkownikom (zgodnie z ustawieniami) sterować funkcjami systemu, nie tylko funkcjami związanymi ze strzeżeniem stref, ale także sterowaniem programowalnymi wyjściami PG (włączanie / wyłączanie). Korzystając z modułów przekaźnika lub modułu ze specjalnymi wyjściami półprzewodnikowymi, mogą oni włączać takie urządzenia, jak kontrolki, światła uliczne, sygnalizację dźwiękową oraz inne urządzenia powiązane z takim systemem zabezpieczeń, jak oświetlenie, systemy kontroli dostępy, blokowanie ogrzewania przy otwartym oknie lub przy uzbrojonej strefie, podlewanie ogrodu itp., tj. automatykę budynkową.

| Funkcja wyjścia PG | Opis | Przykład |
|---|---|---|
| WŁ. / WYŁ. | Status wyjścia bistabilnego można zmienić dowolnym poleceniem lub urządzeniem. | Ręczne WŁĄCZANIE urządzeń przyciskiem funkcji, wiadomością SMS lub dowolnym urządzeniem z opcją ręcznego wyłączania bez ograniczeń. Zwykle sterowanie ogrzewaniem, klimatyzacją, oświetleniem |
| Impuls | Status wyjścia monostabilnego z zadanym czasem | Włączanie impulsowe dodatkowych obwodów sterowania, jak sterowanie bramą, roletami, żaluzjami, podlewaniem ogrodu, zamkami w drzwiach itp. |
| Kopiuj | Status wyjścia z logiką OR. Wyjście będzie aktywne, jeśli co najmniej jedno urządzenie będzie także aktywne, ale dezaktywacja nastąpi, gdy wszystkie urządzenia sterujące będą nieaktywne. | Przydatne do sygnalizacji statusów indywidualnych lub grupowych (zwykle otwartych okien, bramy garażu itp.) przyciskiem funkcji na klawiaturze. W podobny sposób można sygnalizować także statusy wszystkich stref, alarmów, pamięci alarmów, błędów i wielu innych zdarzeń, gdzie podano początek i koniec. |

System oferuje także takie funkcje użytkownika, jak pomiar temperatury, co można pokazać na klawiaturze LCD i w aplikacji MyJABLOTRON.

# 10 Konfiguracja systemu za pomocą programu F-Link

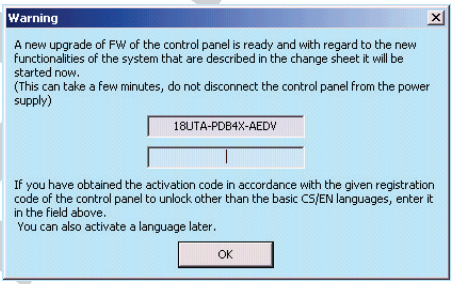
System JABLOTRON 100 programuje się wyłącznie przy użyciu komputera, a dokładniej programu F-Link. Aktualną wersję programu F-Link można uzyskać od dystrybutora lub dostawcy, lub po uwierzytelnieniu pobrać ze strony www.myjablotron.com.

Tuż po otwarciu okna powitalnego w celu wyboru połączenia można przełączyć program F-Link na żądany język. W tym celu należy kliknąć ikonkę języka (flagi). Język można zmienić w dowolnej chwili w menu F-Link. Okno powitalne oferuje następujące opcje:

1. **Połącz lokalnie** — do łączenia komputera z centralą alarmową. Konieczny jest kabel USB (ze złączami A-B).
2. **Połącz zdalnie** — pozwala wybrać instalacje zapisane wcześniej w bazie danych w celu ustanowienia połączenia zdalnego. Aby ustanowić zdalną komunikację z centralą alarmową, komputer musi posiadać dostęp do internetu, a centrala alarmowa musi posiadać komunikator LAN połączony z internetem, a także uzupełniający komunikator GSM z kartą danych SIM. Aby zapewnić bezproblemowe połączenie, należy spełnić inne wymogi, np. aktywna konfiguracja zdalna w centrali alarmowej, poprawny kod rejestracji, kod serwisowy, a przy braku użytkowania komunikatora LAN również odpowiedni sygnał GSM w miejscu umieszczenia centrali alarmowej.
3. **Ustawienia offline** — aby zapewnić dostęp do danych konfiguracji centrali alarmowej. Tutaj można przejść do listy urządzeń i rejestrów ostatniej wymiany baterii itp.

## 10.1 Uruchamianie programu F-Link i konfiguracja wielkości systemu

1. Podłączyć komputer do centrali alarmowej przewodem USB — komputer dokona inicjacji nowego urządzenia USB (może to zająć więcej czasu podczas pierwszego podłączania centrali alarmowej).
2. Po podłączeniu komputer wyświetli dwa nowo znalezione dyski: FLEXI_CFG i FLEXI_LOG. W przypadku ich wyświetlenia w nowym oknie można je po prostu zaznaczyć.
3. Uruchomić program F-Link. Jeżeli centrala alarmowa posiada ustawienia domyślne, otworzy się okno Ustawienia,
   a system automatycznie przejdzie w tryb serwisowy. Jeżeli centralę alarmową skonfigurowano już wcześniej (zmieniono jej kod serwisowy), program poprosi o ponowne wprowadzenie kodu — należy go wprowadzić w formacie **nnnn** (domyślne ustawienie kodu serwisowego to 1010). Można skorzystać także z opcji **Zapamiętaj**, aby program zapisał kod do czasu zamknięcia bazy danych. Wykorzystać opcję **Wyświetl kod** do sprawdzenia wprowadzonego kodu, np. w przypadku korzystania z klawiatury alfanumerycznej, gdzie można zrobić błąd.
4. Po poprawnym uwierzytelnieniu może przedstawić następujący komunikat:




W takim przypadku zalecamy ulepszenie. Kliknięcie przycisku OK powoduje pobranie nowego pakietu oprogramowania, co może potrwać kilka minut. Po zakończeniu procesu ulepszania wyświetli się okienko kreatora w zakładce Konfiguracja początkowa.

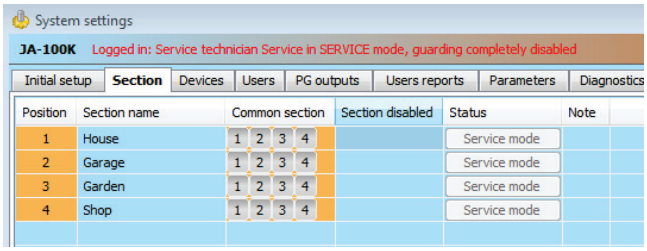
Uwaga: Po ustanowieniu połączenia przy użyciu przewodu USB dezaktywuje się możliwość wprowadzenia zmian ustawień za pomocą klawiatury LCD (dezaktywuje się pozycja menu Ustawienia). W ciągu kilku sekund po odłączeniu przewodu ta pozycja pojawi się ponownie w menu .

## 10.2 Zakładka strefy

Służy do konfiguracji parametrów stref z niezależnym sterowaniem i monitorowaniem. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com




**Nazwa strefy** — nazywanie stref służy do przygotowywania tekstowych raportów zdarzeń (SMS), wyświetlania na klawiaturze i odczytu pamięci, co pozwala lepiej rozpoznać w przypadku raportu (np. parter, skład...).

**Strefa wspólna** — pozwala wybrać, która strefa będzie automatycznie uzbrojona w przypadku uzbrojenia wszystkich stref z nią powiązanych (odpowiednia dla korytarzy, klatek schodowych i innych obszarów wspólnych). Ostrzeżenie o ograniczeniu możliwego stosowania przycisku funkcji klawiatury dla funkcji strefy wspólnej: jeżeli jakiekolwiek strefy rozbrojono oddzielnie, przycisku funkcji strefy wspólnej **nie można** wykorzystać do rozbrojenia pozostałych stref. Te strefy należy rozbrajać oddzielnie.

**Strefa nieaktywna** — dezaktywacja możliwości uzbrojenia strefy, (blokowanie strefy oznacza, że wszystkie urządzenia przypisane do strefy zostają jednocześnie dezaktywowane), co sygnalizuje czerwona kropka. Strefy, do której przypisano centralę alarmową, nie można zablokować. Strefę może zablokować jedynie serwisant (przy użyciu programu F-Link).

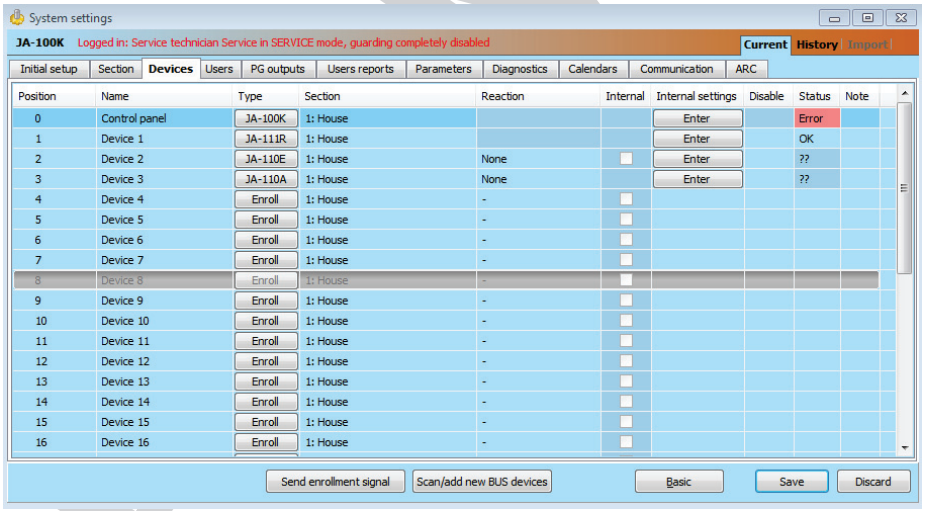
*Ostrzeżenie: Jeżeli strefa, do której przypisano moduł radiowy, jest zablokowana, ten moduł radiowy przestaje otrzymywać sygnały ze wszystkich stref. Dlatego właśnie zalecamy przypisanie go do strefy 1, gdzie przypisana jest także centrala alarmowa. Kiedy zablokowana zostaje strefa wchodząca w skład Wspólnego przycisku funkcji, sygnalizuje ją kolor żółty (nie pokazuje, czy wszystkie strefy są uzbrojone w pełni lub rozbrojone).*

**Status** — ten przycisk wskazuje aktualny status strefy (Rozbrojony, Uzbrojony, Opóźnienie na wyjście, Opóźnienie na wejście, Częściowo uzbrojony, Alarm, Pamięć alarmu, Dezaktywacja, Tryb serwisowy). Naciskając przycisk, można sterować systemem zgodnie z uprawnieniami nadanymi przez logowanie (zmienia status strefy — częściowo uzbrojony/rozbrojony/uzbrojony ...).

**Uwaga** — pozwala podać dane strefy, aby ułatwić orientację podczas przeglądów rocznych itp.

## 10.3 Zakładka urządzenia

Służy do przypisywania zainstalowanego urządzenia w systemie i ustawiania jego parametrów. Centrala alarmowa zostaje automatycznie przypisana w Pozycji 0 w Strefie 1 i nie można jej przenieść ani usunąć. Aby wprowadzić zmiany w zakładce, należy wejść w tryb serwisowy.




**Nazwa** — używana w raportach tekstowych zdarzeń oraz odczycie pamięci (przykład Wejście główne).

**Typ** — wyświetla typ przypisanego urządzenia. Pusta pozycja pozwala przypisać nowe urządzenie. **Przypisywanie urządzeń**, patrz rozdział 8.4.1 Enrolling and erasing devices.

**Strefa** — określa, do której strefy monitorowania urządzenie będzie zgłaszać zdarzenia (alarm, sabotaż, błąd...). Uwaga: podział budynku na strefy — patrz rozdział 10.2 Sections tab.

**Reakcja** — określa, którą reakcję wywoła aktywacja danego urządzenia. Jeżeli urządzenie nie posiada wejścia alarmowego (np. modułu dostępu MAGISTRALI), reakcji nie można przypisać. Kompletny wykaz reakcji dla urządzeń wyświetla się po aktywacji Ustawień zaawansowanych. Opis reakcji znajduje się w rozdziale 8.4.2 List of applicable reactions.

**Wewnętrzne** — ten parametr jest dostępny wyłącznie dla czujek włamania. Sygnałów z urządzeń o tej sygnalizacji nie uznaje się za sygnały alarmowe w przypadku częściowego uzbrojenia strefy. Częściowe uzbrojenie strefy — patrz rozdział 10.2 Sections tab.

**Ustawienia wewnętrzne** — dostęp do ustawień parametrów wewnętrznych urządzeń połączonych z MAGISTRALĄ lub zapewniających dwukierunkową komunikację bezprzewodową. Poszczególne urządzenia posiadają różne parametry wewnętrzne (niektóre nie posiadają żadnych). Ustawienia wewnętrzne klawiatury opisano w rozdziale 10.3.1 Keypad configuration. Ustawienia pozostałych urządzeń opisano w odpowiadających im instrukcjach.

**Dezaktywuj** — można wykonać na 2 poziomach nadanych przez posiadane uprawnienia:

1. **Blokada wejścia** (żółta kropka) służy do trwałego blokowania wejścia czujki (BLK). System ignoruje aktywację wszelkich urządzeń = brak aktywacji alarmu i sterowania PG, przy zwykłej rejestracji alarmów sabotażu i awarii.
2. **Dezaktywacja urządzenia** (czerwona kropka) służy do całkowitej dezaktywacji urządzenia (Dezaktywacja). System ignoruje wszelkie funkcje podłączonych urządzeń = brak aktywacji alarmu, sabotażu, PG, Awarii, raportów,...).

Nie można dezaktywować centrali alarmowej ani urządzenia, której reakcję ustawiono na Panikę.

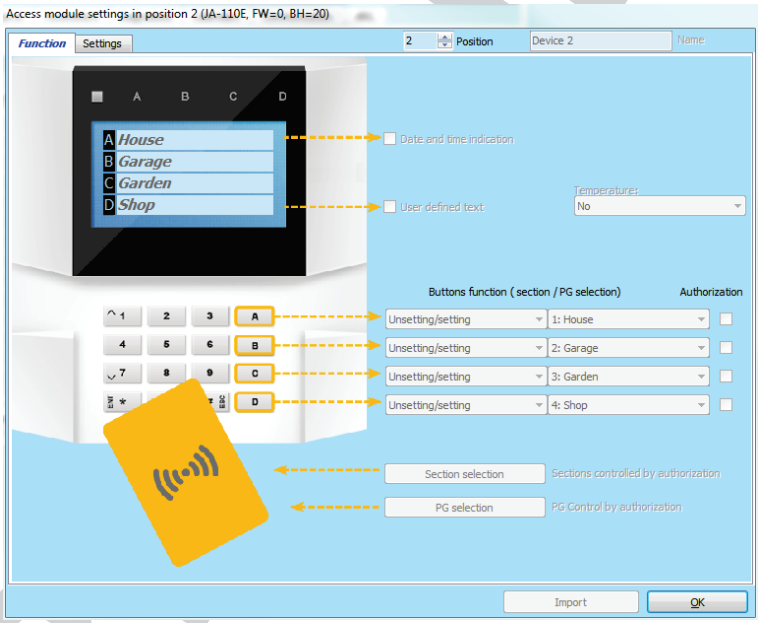
**Status** — wskazuje aktualny status urządzenia. OK = wszystko w porządku, TMP = sabotaż, ACT = aktywacja wejścia alarmu, BLK = zablokowany, Disabled = dezaktywacja, ERR = błąd, ?? = brak komunikacji z urządzeniem, Mains supply = awaria zasilania, Battery = rozładowana lub odłączona bateria w centrali alarmowej, Charging – ładowanie baterii awaryjnej w urządzeniu lub centrali alarmowej, BOOT – trwa ulepszanie urządzenia lub niepowodzenie ulepszania (powtórz ulepszanie). Przesunięcie kursora myszy na STATUS urządzenia wyświetli szczegółowe dane.

**Uwaga** — pozwala opisać szczegółowe informacje o urządzeniu, np. lokalizację, datę ostatniej wymiany baterii, średnią siłę sygnału RF podczas ostatniego sprawdzania itp.

### 10.3.1 Konfiguracja klawiatury

Przy wprowadzaniu ustawień wewnętrznych klawiatury (zakładka Urządzenia) otworzy się następujące okienko (przykład dotyczy klawiatury JA-110E).

**Zakładka Funkcja:**




**Data i godzina** Pozwala wyświetlić aktualną godzinę w systemie w prawym górnym rogu klawiatury

**Tekst użytkownika** — pozwala wyświetlić dowolnie wybrany tekst na klawiaturze LCD (nr telefonu instalatora, itp.). Aktywacja takiej opcji dezaktywuje przycisk funkcji „D".

**Temperatura** — pozwala wyświetlić zmierzoną temperaturę dla wybranej czujki w lewym dolnym rogu klawiatury

**Przyciski funkcji** — z lewej strony proszę wybrać przycisk funkcji, z prawej strony strefę lub wyjście PG, do którego przypisano funkcję. Do przycisku funkcji można przypisać następujące: Brak, Rozbrojenie/Uzbrojenie, Rozbrojenie/Uzbrojenie częściowe, Rozbrojenie/Uzbrojenie częściowe/Uzbrojenie, Wskazanie strefy, Cicha panika, Pożar, Panika z sygnałem dźwiękowym, Zagrożenie dla zdrowia, PG WYŁ./WŁ., PG WŁ., PG WYŁ., wskazanie PG, wskazanie odwrócone PG, wspólny przycisk funkcji.

**Uwierzytelnienie** — do uzbrojenia i rozbrojenia konieczne jest uwierzytelnienie użytkownika. Jeżeli ten parametr jest nieaktywny, wszystkimi przyciskami funkcji można sterować bez uwierzytelnienia z wyjątkiem funkcji Rozbrój strefę, który zawsze wymaga uwierzytelniania. W odniesieniu do aktywacji i dezaktywacji wyjść PG dla obu elementów sterowania obowiązuje ustawienie funkcji Uwierzytelnianie / Bez uwierzytelniania.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

**Importuj** — pozwala kopiować aktualne ustawienia klawiatury do innych klawiatur tego samego typu, na przykład w przypadku, gdy chroniony budynek posiada więcej wejść, a każde wejście wymaga posiadania klawiatury o tych samych funkcjach. Dla tego samego typu klawiatury można wykonać kopię. Można ją także wykorzystać w przypadku wymiany klawiatury na nową. Przycisk Importuj zapewnia historię ostatnich znanych ustawień klawiatury w danym położeniu.

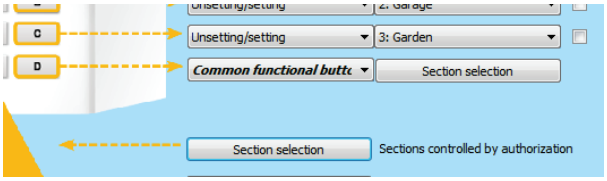
**Wybór strefy** — zadane strefy z możliwością sterowania wyłącznie w drodze uwierzytelnienia (karta/brelok RFID lub kod).

**Sterowanie PG** — wybór wyjść PG do sterowania wyłącznie w drodze uwierzytelniania (karta/brelok RFID lub kod).

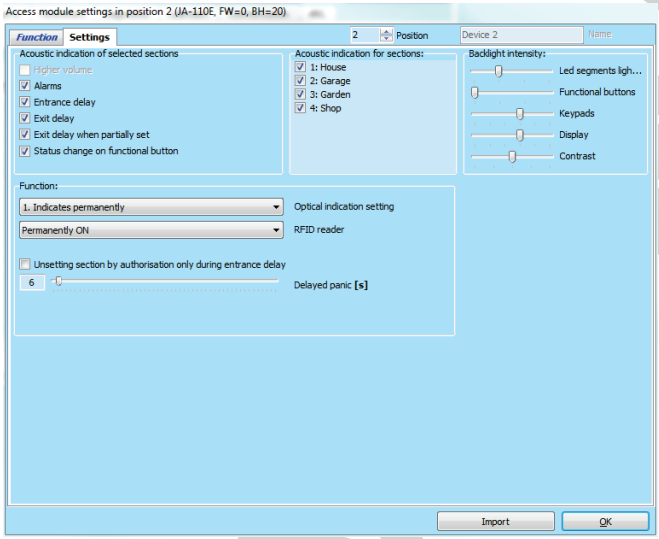
| | |
|---|---|
| **Brak** | Przycisk funkcji nie posiada funkcji; nieaktywny |
| **Rozbrój / Uzbrój** | Sterowanie strefą. Wskazanie przycisku funkcji: strefa rozbrojona = zielony, uzbrojona = czerwony. |
| **Rozbrój / Uzbrój częściowo** | Umożliwia aktywację trybu częściowego uzbrajania strefy (jeżeli aktywne w zakładce Strefy). Wskazanie przycisku funkcji: strefa rozbrojona = zielony, uzbrojona częściowo = żółty. |
| **Rozbrój / Uzbrój częściowo / Uzbrój** | Pozwala wybrać poziom uzbrajania. Po naciśnięciu przycisku funkcji (Uzbrój) nastąpi uzbrojenie częściowe, po kolejnym naciśnięciu nastąpi uzbrojenie całkowite systemu. Kiedy system jest w pełni uzbrojony, naciśnięcie przycisku funkcji powoduje jego całkowite rozbrojenie. Wskazanie przycisku: strefa rozbrojona = zielony, uzbrojona częściowo = żółty, uzbrojona całkowicie = czerwony. |
| **Sygnalizuje strefę** | Przycisk funkcji wskazuje jedynie status strefy, ale nie umożliwia sterowania nią (odpowiednie np. do sygnalizacji statusu stref wspólnych, klatki schodowej itp.) W przypadku aktywacji alarmu pozwala na jego anulowanie przez naciśnięcie zielonego przycisku na przycisku funkcji z późniejszym prawidłowym uwierzytelnienie przez użytkownika. |
| **Panika (cicha)** | Przycisk funkcji uruchamia cichy alarm Panika. Po naciśnięciu przycisku ze strefy, do której jest przypisany przycisk, zostanie wysłany raport Panika bez sygnalizacji dźwiękowej. Alarm Panika można opóźnić o regulowaną długość czasu, z możliwością anulowania przed wygaśnięciem zadanego czasu (patrz Panika opóźniona). Uzbrojona strefa nie zostanie rozbrojona. |
| **Pożar** | Przycisk funkcji uruchamia alarm pożarowy. Następnie alarm pożarowy aktywuje się w strefie, do której przypisano przycisk funkcji. |
| **Panika z sygnałem dźwiękowym** | Przycisk funkcji aktywuje głośny alarm panika. Po naciśnięciu następuje aktywacja głośnego alarmu Panika ze strefy, do której przypisano przycisk funkcji. Głośny alarm Panika można opóźnić o regulowaną długość czasu, z możliwością anulowania przed wygaśnięciem zadanego czasu (patrz Panika opóźniona). Uzbrojona strefa nie zostanie rozbrojona. |
| **Zagrożenia medyczne** | Przycisk funkcji pozwala wysłać raport dotyczący problemów ze zdrowiem (bez aktywacji syreny) ze strefy, do której przypisano przycisk funkcji. |
| **Dezaktywuj PG / Aktywuj PG** | Przycisk funkcji pozwala sterować wyjściem PG. Wskazanie: PG nieaktywne = zielony, PG aktywne/aktywowane = czerwony |
| **Aktywuj PG** | Przycisk funkcji można wykorzystać jedynie do aktywacji wyjścia PG (np. włączenia oświetlenia na zadany czas). |
| **Dezaktywuj PG** | Przycisk funkcji można wykorzystać jedynie do dezaktywacji wyjścia PG (np. funkcja przycisku STOP w nagłym wypadku). |
| **Sygnalizuje PG** | Przycisk funkcji wyłącznie sygnalizuje status wyjścia bez możliwości sterowania nim (czerwony sygnalizuje status aktywny). |
| **Sygnalizacja odwrócona PG** | Przycisk funkcji wyłącznie sygnalizuje status wyjścia z logiką odwróconą (zielony sygnalizuje status aktywny) bez możliwości sterowania |
| **Wspólny przycisk funkcji** | Umożliwia jednoczesne sterowanie kilkoma strefami przy użyciu przycisku funkcji na klawiaturze. Po naciśnięciu wspólnego przycisku funkcji polecenie Rozbrój/Uzbrój realizowane jest łącznie dla zadanych przycisków stref. Jeżeli niektóre strefy sterowane wspólnym przyciskiem są uzbrojone, a inne rozbrojone, wykorzystanie wspólnego przycisku funkcji spowoduje rozbrojenie pozostałych przycisków (krótkie naciśnięcie) lub ich całkowite uzbrojenie (długie naciśnięcie). Jeżeli dla jednego z wybranych przycisków funkcji aktywowano Uzbrojenie częściowe (szczegółowe informacje w 9.2 System control by keypad), przycisk wspólny będzie się zachowywał następujący: 1. naciśnięcie Uzbrój = |

| | |
|---|---|
| | uzbrojenie częściowe, 2. naciśnięcie Uzbrój = uzbrojenie całkowite. Nie wolno łączyć wspólnego przycisku funkcji ze Strefami/Strefą wspólną.<br>Wskazanie przycisku wspólnego: wszystkie strefy rozbrojone = zielony, wszystkie strefy w pełni uzbrojone = czerwony, dowolna strefa uzbrojona (częściowo) = żółty.<br>Strefy przypisuje się do wspólnego przycisku funkcji w otwartym oknie po wybraniu takiej opcji. |

**Wspólny przycisk funkcji:**




## Zakładka Ustawienia:




**Sygnalizacja dźwiękowa wybranych stref:**

| | |
|---|---|
| Większa głośność | Konfiguracja głośności sygnalizacji z wyjątkiem głośności alarmu |
| Alarmy | Sygnalizacja dźwięków alarmu (dźwięk syreny) |
| Opóźnienie na wejście | ciągłe gwizdanie podczas opóźnienia na wejście |
| Opóźnienie na wyjście | powolne, przerywanie pikanie (1/s) |
| Opóźnienie na wyjście przy uzbrojeniu częściowym | powolne, przerywane pikanie (domyślnie wyłączone) |
| Zmiana statusu przycisku funkcji | sygnalizacja dźwiękowa z zastosowaniem jednego piknięcia na zmianę |

**Funkcje:**

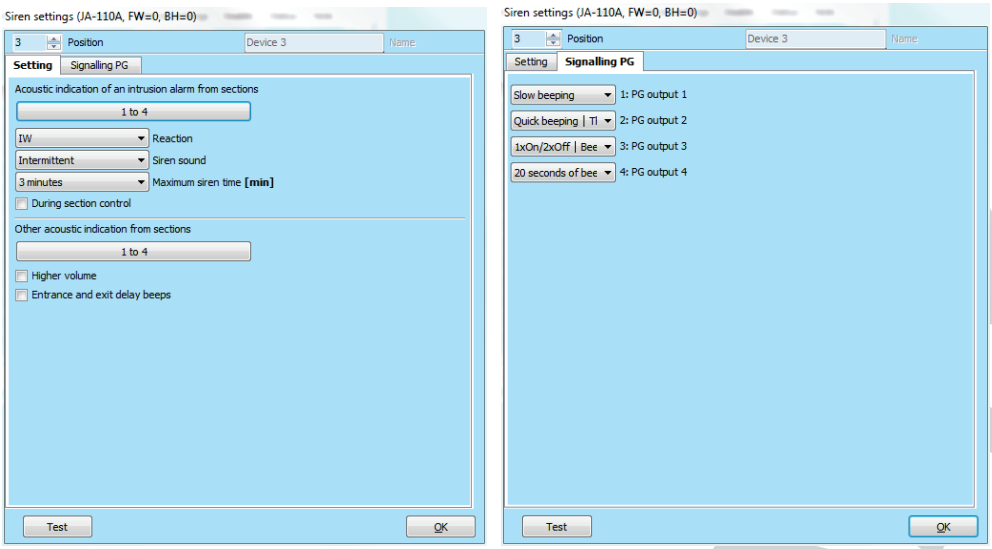
| | | |
|---|---|---|
| Czytnik RFID | Aby zapewnić oszczędność energii, działanie czytnika można ograniczyć do 3 s od naciśnięcia jego pokrywy. Czytnik RFID można też całkowicie wyłączyć. To ustawienie dotyczy klawiatur bezprzewodowych zasilanych w energię elektryczną ze źródła zewnętrznego. W przeciwnym razie czytnik RFID zawsze wyłącza się automatycznie. | |
| | Stale włączony | Czytnik RFID jest stale aktywny. W przypadku klawiatury MAGISTRALI nie przestrzega ustawienia wzbudzania. |
| | Aktywacja przez naciśnięcie | Wzbudzanie czytnika RFID na 3 s po aktywacji na klawiaturze. |
| | Wyłączony | Czytnik RFID jest trwale wyłączony. |
| | Po naciśnięciu lub wymóg autoryzacji | Wzbudza czytnik RFID po aktywacji klawiatury lub wymogu uwierzytelniania. |
| Ustawienia sygnalizacji | 1. Sygnalizacja stała | Klawiatura MAGISTRALI sygnalizuje nieprzerwanie. Klawiatura bezprzewodowa będzie sygnalizować nieprzerwanie jedynie przy zasilaniu zewnętrznym. Bez zasilania zewnętrznego zachowuje się |

| | | |
|---|---|---|
| świetlnej | | jak opcja 2. |
| | 2. Po zmianie statusu strefy na klawiaturze | Klawiatura sygnalizuje zmianę statusu strefy / PG. Zmianę statusu sygnalizuje jedynie dany przycisk funkcji. Opóźnienie na wejście i alarm sygnalizuje cała klawiatura. |
| | 3. Po zmianie statusu strefy — kontrolka | Zmianę statusu strefy / PG sygnalizuje jedynie dany przycisk funkcji. |
| | 4. Zmiana kontrolki statusu na klawiaturze | Opóźnienia na wejście i alarmy są sygnalizowane tylko dźwiękiem. Zmianę statusu sygnalizuje jedynie dany przycisk funkcji. Ta opcja jest ustawieniem domyślnym. |
| | 5. Po wejściu i alarmie | Klawiatura sygnalizuje opóźnienie na wejście i alarm na danym przycisku funkcji. Nie zachodzi sygnalizacja zmiany statusu wyjścia PG i statusu strefy. |
| | 6. Wzbudzanie przez naciśnięcie | Klawiatura zapewnia sygnalizację świetlną i dźwiękową wyłącznie po otwarciu pokrywy przedniej; naciśnięcie przycisku, przycisku funkcji lub pokrywy przedniej |
| Rozbrajanie strefy przez uwierzytelnianie wyłącznie podczas opóźnienia na wejście | | Jeżeli ta opcja jest aktywna, strefę, w której uruchomiono opóźnienie na wejście, rozbraja się prawidłową kartą/brelokiem RFID użytkownika lub po uwierzytelnieniu przy użyciu kodu. W przypadku klawiatur bezprzewodowych uwierzytelnienia można dokonać po uruchomieniu opóźnienia na wejście. PRZESTROGA: Zalecamy wyłączenie tej funkcji, gdy dla stref wspólnych zwykle włącza się opóźnienie na wejście zwykle. W przeciwnym razie wszystkie strefy przypisane do strefy wspólnej zostaną rozbrojone w wyniku danego uwierzytelnienia. |
| Wzbudzanie klawiatury przy pomocy karty RFID | | Zbliżenie karty RFID powoduje wzbudzenie klawiatury. Nie zalecamy aktywacji tej funkcji w przypadku istnienia wielu przeszkód wokół klawiatury, jak metalowe przedmioty i okablowanie elektryczne. Jeżeli zdecydują się Państwo na jej aktywację, należy dopilnować, by klawiatury nie można było uruchomić przypadkowo, co skróci żywotność baterii. |
| Panika opóźniona | | Ta funkcja służy do odraczania aktywacji cichego alarmu panika lub alarmu panika z sygnałem dźwiękowym o zadany czas. Można określić odstęp czasu podczas anulowania aktywacji wielokrotnym naciśnięciem tego samego przycisku funkcji z zadaną wartością dla cichego alarmu panika lub alarmu panika z sygnałem dźwiękowym. Po włączeniu uwierzytelniania, jest ono wymagane także do aktywacji i dezaktywacji. Opóźnienie można regulować w zakresie od 1 do 255 sekund. |

**Intensywność podświetlenia:**

| | |
|---|---|
| Kontrolki | Regulacja podświetlenia kontrolek |
| Przyciski funkcji | Regulacja przycisków funkcji |
| Klawiatura | Regulacja podświetlenia klawiatury |
| Wyświetlacz | Konfiguracja podświetlenia wyświetlacza LCD |
| Kontrast | Konfiguracja kontrastu wyświetlacza LCD |

### 10.3.2 Ustawienia syreny wewnętrznej:




**Sygnalizacja dźwiękowa alarmu włamania ze stref** — służy do wyboru stref, dla których alarm będzie posiadał sygnalizację dźwiękową w postaci syren

**Reakcja** — wybór opcji sygnalizacji alarmu jako EW (zewnętrzna sygnalizacja ostrzeżenia) lub IW (wewnętrzna sygnalizacja ostrzeżenia). Różnicę opisano w tabeli 8.5 Types of alarms.

**Dźwięk syreny** — wybór dźwięku syreny: Przerywany (50/50) / Ciągły

**Maksymalny czas działania syreny** — ograniczenie maksymalnego czasu sygnalizacji do 1 do 5 minut (przy założeniu, że alarm centrali alarmowej trwa dłużej. W przeciwnym razie ustaje wraz z alarmem centrali alarmowej).

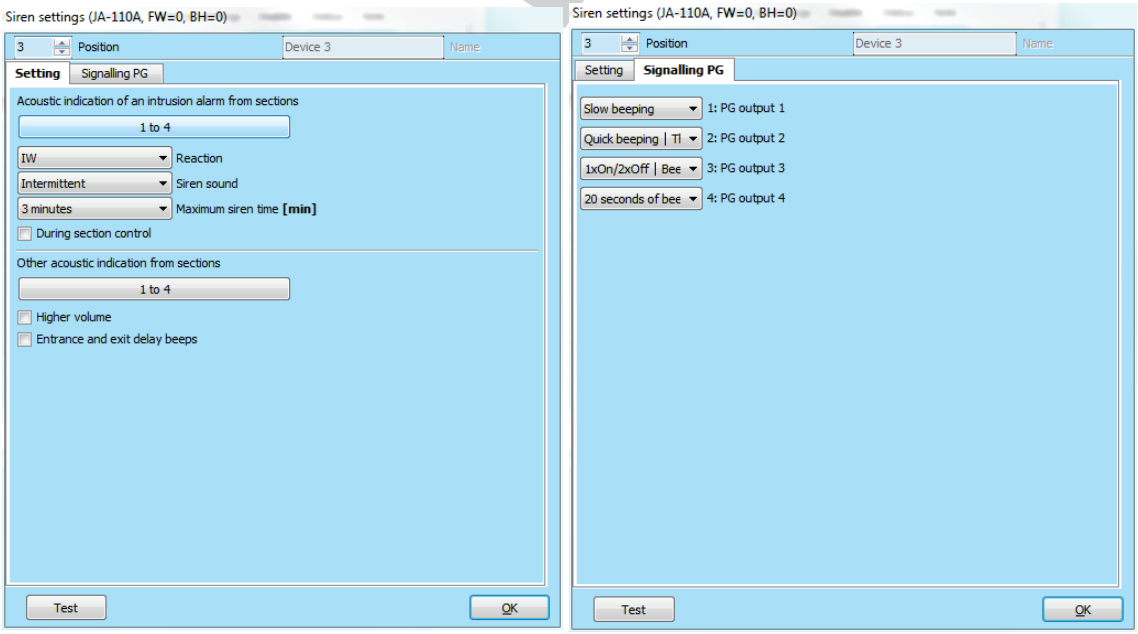
**Podczas sterowania strefą** — dźwiękowe potwierdzenie zmian statusu strefy (pika 1x — uzbrojona / 2x rozbrojona)

**Inna sygnalizacja dźwiękowa ze stref** — wybór stref do innej sygnalizacji dźwiękowej (opóźnienie na wejście/wyjście)

**Większa głośność** — możliwość ustawienia wyższej lub niższej głośności sygnalizacji opóźnienia na wejście i wyjście oraz sygnalizacji sterowania wyjściem PG. Nie wpływa na dźwięk alarmu, który zawsze posiada najwyższą głośność.

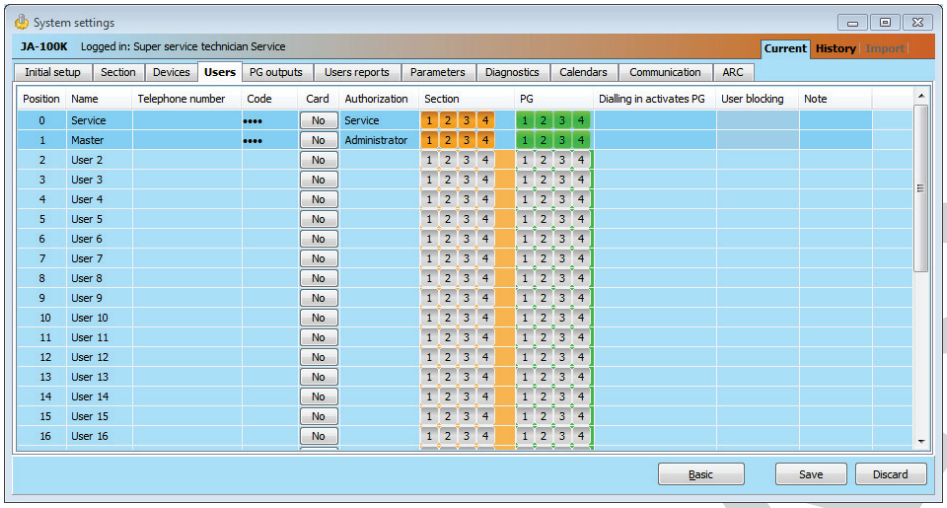
**Pikanie sygnalizujące opóźnienie na wejście i wyjście** — sygnalizacja dźwiękowa opóźnienia na wejście / wyjście

**Test** — przycisk do przeprowadzenia 3 sek. testu dźwiękowej i optycznej sygnalizacji alarmów



## 10.4 Zakładka Użytkownicy

Służy do ustanawiania nowych użytkowników systemu i ich praw. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**Nazwa** — nazwy użytkowników wykorzystuje się w tekstowych raportach zdarzeń w odczytach historii zdarzeń, w zakładkach raportów, ustawieniach uwierzytelniania lub do uwierzytelniania na klawiaturze lub w raportach SMS wysyłanych przez uzupełniający komunikator GSM.

**Numer telefonu** — służy do raportowania zdarzeń w przypadku podłączenia komunikatorów uzupełniających lub do identyfikacji użytkowników w przypadku sterowania systemem przy użyciu telefonu z menu głosowym lub do aktywacji wyjść PG przez połączenie głosowe i SMS. Numer telefonu należy zawsze wprowadzać w formacie międzynarodowym (np. +420710123456).

**Kod** — kod dostępu użytkownika wprowadza się w formacie **nnnn** (4 lub 6 cyfr zależnie od profilu systemu). Kodu w pozycjach 0 i 1 nie można skasować (Serwis i Administrator główny).

**Karta** — służy do przypisywania kart dostępu RFID (breloków). Każdy użytkownik może posiadać jedną kartę RFID.

Karty/breloki można przypisać:

— przez wprowadzenie numeru seryjnego (można go odczytać za pomocą czytnika kodów paskowych z karty/breloka RFID)

— przy pomocy czytnika JA-190T ze złączem USB do komputera **oraz zbliżenia** karty/breloka RFID

— przy pomocy dowolnej klawiatury i zbliżenia karty/breloka RFID

**Uwierzytelnianie** — określa prawa użytkowników. Uprawnień w pozycji 0 i 1 nie można zmienić. Szczegółowe informacje — patrz rozdział 8.3 Authorisation of users.

**Strefa** — określa, którymi strefami użytkownik może sterować. Administrator może także ustawić kody oraz karty użytkowników w przypisanych strefach. Strefy nie można przypisać do użytkownika uprawnionego wyłącznie do sterowania wyjściami PG.

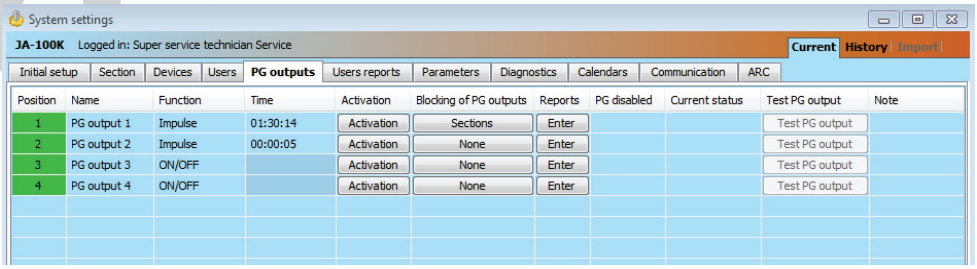
**PG** — określa, do sterowania którymi wyjściami PG uprawniony jest użytkownik (jeżeli do sterowania wyjściami konieczne jest uwierzytelnienie).

**Dezaktywuj** — możliwość zablokowania użytkownika. Nie można dezaktywować użytkowników w pozycji 0 (serwisant) i 1 (administrator główny. Dezaktywację użytkownika sygnalizuje czerwona kropka. Prawo dezaktywacji użytkowników posiada administrator (przy użyciu klawiatury) oraz serwisant (za pośrednictwem programu F-Link).

**Notatka** — pozwala podać uprawnienia użytkownika, np. uprawnienia do dostępu poza godzinami pracy itp.

## 10.5 Zakładka wyjścia PG

Służy do ustawiania funkcji i łączy wyjść programowalnych. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**Nazwa** — identyfikacja wyjścia (np. Klimatyzacja, Drzwi magazynu,...)

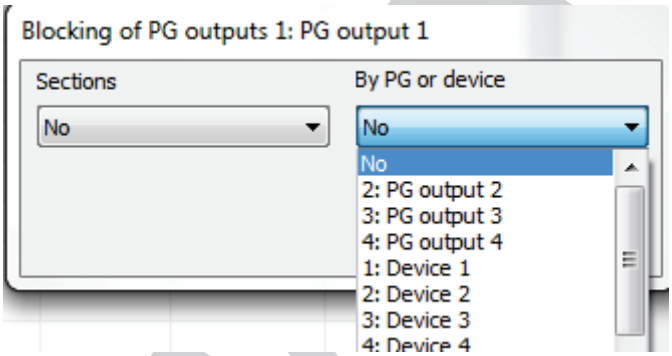
**Funkcja** — określa zachowanie wyjścia po aktywacji.

| | |
|---|---|
| **Impuls** | umożliwia aktywację z ograniczeniem czasowym (czas ustala się przyciskiem Czas). |
| **ON/OFF** | polecenie aktywacji spowoduje włączenie, polecenie dezaktywacji spowoduje wyłączenie, przy braku sprawdzenia statusu źródła lub czasu trwania, ostatnie polecenie zawsze realizuje żądanie |
| **Kopiuj** | kopiuje aktywację czujki lub status wewnętrzny. W przypadku żądania od dwóch urządzeń stosuje się logikę OR. |

**Czas** — ustawienia czasu dla funkcji Impuls. Czas ustawia się w formacie *gg:mm:ss* w zakresie od 00:00:01 do 23:59:59.

**Aktywacja** — Otwarcie Mapy aktywacji wyjścia PG — patrz rozdział 10.5.1 Activation Map of a PG outputs.

**Blokowanie PG** — w celu zablokowania wyjścia na podstawie statusu strefy, czujki lub innego wyjścia PG. Blokowanie uniemożliwia aktywację danego PG, a jeśli jest ono włączone, powoduje jego dezaktywację. Służy np. do blokowania zamka w drzwiach po uzbrojeniu danej strefy. W przypadku blokowania na podstawie statusu strefy można wybrać, czy blokowanie ma nastąpić w chwili, gdy strefa jest uzbrojona czy rozbrojona, a w przypadku blokowania za pomocą urządzenia, czy ma nastąpić w wyniku jego aktywacji czy dezaktywacji. Obie opcje blokowania (za pomocą strefy i urządzenia lub strefy i wyjścia PG) można stosować jednocześnie.




**Dezaktywuj** — możliwość zablokowania wyjścia PG. Dezaktywację (blokowanie) wyjścia sygnalizuje czerwona kropka.Do dezaktywacji wyjścia uprawniony jest serwisant (przy pomocy F-Link).

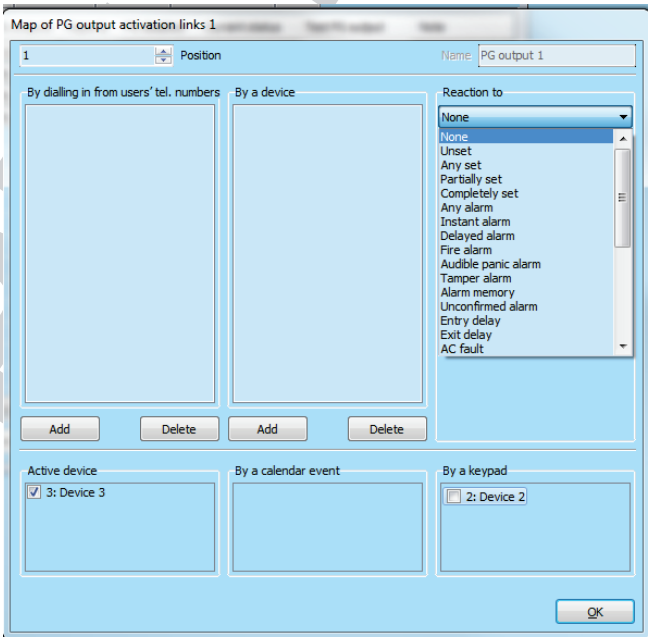
**Aktualny status** — oznaczone kolorami informacje na temat aktualnego statusu wyjścia PG. Opis w kolorze zielonym odpowiada zielonej kontrolce na przycisku funkcji, opis w kolorze czerwonym odpowiada czerwonej kontrolce na przycisku funkcji.

**Test** — możliwość sterowania wyjściem ręcznie z komputera przy pomocy programu F-Link. Zależnie od wybranej funkcji aktywuje (lub dezaktywuje) konkretne wyjście PG, jeżeli w danej chwili nie jest ono zablokowane.

**Notatka** — pozwala podać dane wyjścia PG, jego przeznaczenie, specjalne zachowanie, powiadomienie o aktywacji łącznie z innymi wyjściami itp.

### 10.5.1 Mapa aktywacji wyjść PG

Wybór Aktywacji w zakładce wyjść PG pozwoli przejść do mapy łączy aktywacji. Mapa określa, na jakie działanie reaguje wyjście.




**Przez połączenie głosowe z numerów telefonu użytkownika** — z określeniem użytkowników uprawnionych do aktywacji wyjścia PG przez połączenie głosowe z telefonu po podłączeniu uzupełniającego komunikatora GSM lub PSTN. Numery telefonu stosowane do aktywacji sygnału dźwiękowego nie mogą być ukryte (usługa CLIP nie może zostać wyłączona). Termin „sygnał dźwiękowy" oznacza, że po wybraniu numeru telefonu osoba dzwoniąca czeka przez co najmniej jeden sygnał dźwiękowy i kończy połączenie, zanim odbierze je centrala alarmowa (patrz liczba



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

sygnałów dźwiękowych dla rozmów przychodzących w ustawieniach komunikatora). Wyjście PG włącza się z chwilą rozłączenia. Jeżeli centrala alarmowa odbierze połączenie, wyjście się nie aktywuje.

**Przez urządzenie** — umożliwia aktywację wyjścia PG przez urządzenie (aktywacja czujki, naciśnięcie wypustki itp.) Ustawienie jest powiązane z zakładką Urządzenia. Jedno urządzenie może aktywować tylko jedno wyjście PG.

**Reakcja na** — umożliwia aktywację wyjścia przez wybrane zdarzenie w systemie (np. uzbrojenie, alarm, awaria zasilania, błąd itp.). Dla statusu wewnętrznego (łącznie 29 statusów wewnętrznych, patrz poniższa tabela) można ustawić grupę stref, z których sygnał zostanie przyjęty (logika OR). Dane wyjście PG można ustawić ma kopiowanie statusu innego wyjścia PG lub kilku innych wyjść z możliwością wyboru wzajemnej logiki (OR lub AND). Ostatnia pozycja w menu pozwala ustawić aktywację wyjścia i jego dezaktywację w odpowiedzi na całkowicie inne zdarzenie (np. aktywację w przypadku alarmu, ale dezaktywację wyłącznie przez rozbrojenie).

**Aktywowane przez urządzenie** — wykaz urządzeń aktywujących dane wyjście PG przy pomocy ich własnej aktywacji, na przykład zdjęcie z czujki PIR z kamerą (funkcję można ustawić w ustawieniach wewnętrznych urządzenia) lub sygnalizacja dźwiękowa syreny itp.

**Przez zdarzenie w kalendarzu** — wykaz planowanych zdarzeń, które aktywują lub dezaktywują lub blokują dane wyjście PG (okno informacji)

**Przez klawiaturę (przycisk funkcji)** — Przedstawia wykaz klawiatur i manipulatorów zdalnych w systemie z możliwością sterowania konkretnym wyjściem PG.

**Przez polecenia SMS** — kiedy podłączony jest uzupełniający komunikator SMS, umożliwia wysyłanie poleceń tekstowych w celu aktywacji i dezaktywacji wyjścia PG przy pomocy telefonu. Do sterowania wyjściami należy użyć SMS w formacie **kod_polecenie**, np. **2345_aktywuj_oświetlenie** (uwaga: znak _ oznacza spację). Kod przed poleceniem nie jest obowiązkowy, jeżeli w zakładce ***Komunikacja*** aktywowano pozycję „Menu głosowe i SMS sterujący bez kodu", i można zidentyfikować numer telefonu użytkownika uprawnionego do sterowania danym wyjściem PG.

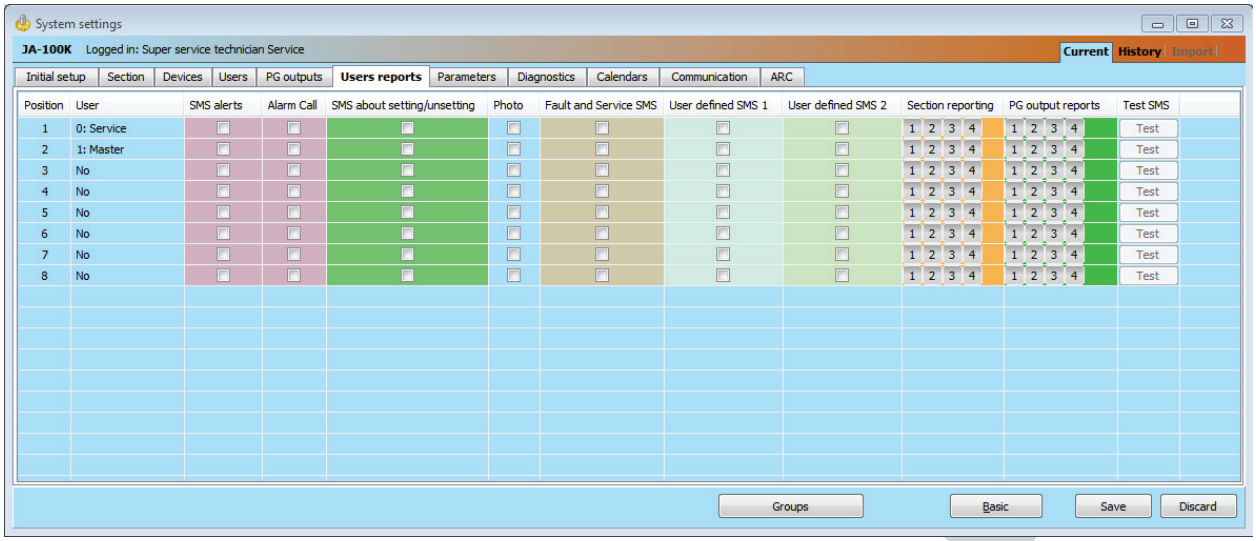
***Ostrzeżenie:*** *Wyjścia PG nie działają, jeżeli system znajduje się w trybie serwisowym. Naciśnięcie przycisku Test pozwala sprawdzić wszystkie wyjścia PG (przy użyciu programu F-Link). W chwili aktywacji trybu serwisowego następuje dezaktywacja wszystkich wyjść PG. Po opuszczeniu trybu serwis może nastąpić ich ponowna aktywacja.*

**Statusy wewnętrzne do sterowania wyjściami PG:**

| | | |
|---|---|---|
| 1. Rozbrój | 11. Pamięć alarmu | 21. Aktywna czujka |
| 2. Dowolny uzbrojony | 12. Alarm niepotwierdzony | 22. Niski poziom baterii w urządzeniu |
| 3. Częściowo uzbrojona | 13. Opóźnienie na wejście | 23. Urządzenie z aktywnym sabotażem |
| 4. Całkowicie uzbrojona | 14. Opóźnienie na wyjście | 24. Brak ruchu w strefie |
| 5. Dowolny alarm | 15. Awaria prądu stałego | 25. Żądanie kontroli corocznej |
| 6. Alarm natychmiastowy | 16. Awaria prądu stałego przez 30 minut | 26. Błąd GSM |
| 7. Alarm opóźniony | 17. Awaria baterii awaryjnej | 27. Błąd LAN |
| 8. Alarm pożarowy | 18. Ostrzeżenie wewnętrzne (IW) | 28. Błąd PSTN |
| 9. Alarm panika z sygnałem dźwiękowym | 19. Ostrzeżenie zewnętrzne (EW) | 29. Zdarzenie w systemie |
| 10. Alarm sabotażowy | 20. Błąd | |

## 10.6 Zakładka Raporty do użytkowników

Ta zakładka jest dostępna po podłączeniu uzupełniającego komunikatora GSM lub PSTN i służy do określania użytkowników, których system będzie informował o wybranych grupach zdarzeń za pośrednictwem wiadomości SMS lub połączeń głosowych na ich numery telefonu. Grupy i format wiadomości SMS opisano w załączonej tabeli. Podstawową strukturę menu głosowego opisano w załączonej tabeli 9.5. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**Użytkownik** — umożliwia wybór użytkownika z listy użytkowników.

**Alerty SMS** — grupa raportów alarmów do wyboru, w których przypadku wysyłany jest raport o zdarzeniu alarmowym w wybranej strefie, o awarii lub przywróceniu zasilania po upływie 30 minut, uzbrojeniu przy otwartej strefie, i ewentualnie o strefie rozbrojonej bez ruchu (patrz zakładka Parametry).

**Połączenie alarmowe** — grupa raportów, w których przypadku (po wysłaniu raportów SMS) system przekazuje
każdemu użytkownikowi alarmowy komunikat głosowy. Przy braku odebrania połączenia w ciągu 30 sekund system wykonuje połączenie do kolejnego użytkownika na liście. Odebranie połączenia powoduje wielokrotne odtwarzanie komunikatu głosowego. Komunikat posiada następującą strukturę: Twoje raporty alarmów — Typ alarmu — Nr strefy. Kiedy użytkownik rozłączy połączenie najpóźniej po upływie 50 sekund dochodzi do zakończenia rozmowy i wyboru numeru kolejnego użytkownika. Użytkownik może potwierdzić otrzymanie połączenia, naciskając przycisk **#** na telefonie, a po komunikacie głosowym użytkownik musi wprowadzić poprawny kod. Po wprowadzeniu poprawnego kodu **alarm wyłącza się, a kolejny użytkownik nie otrzymuje połączenia.** W przypadku raportów głosowych system zawiera zadane uniwersalne komunikaty głosowe. Komunikaty głosowe można nagrać ponownie, zastępując nazwy wymaganymi w menu głosowym.

**Uwaga**: raportowanie zdarzenie głosowego ogranicza się do maks. 5 użytkowników.

**SMS o uzbrojeniu / rozbrojeniu** — grupa raportów, dla których wysyłana jest wiadomość tekstowa dotycząca uzbrojenia i rozbrojenia. Raport uzbrojenia wysyłany jest ze stałym **opóźnieniem 60 sekund** po uzbrojeniu. Uzbrajanie i rozbrajanie nie zostaje zgłoszone użytkownikowi, który go dokonał. Wyjątek stanowi uzbrojenie strefy wspólnej (przez centralę alarmową, nie przez użytkownika).

**Zdjęcie** — wysyła użytkownikowi wiadomość SMS, z której wynika, że wykonano zdjęcie alarmowe, w przypadku instalacji urządzeń do weryfikacji zdjęciowej. Więcej szczegółów — patrz instrukcje obsługi danych czujek z kamerą.

**SMS o błędzie i serwisie** — wysyła raporty tekstowe dotyczące błędów (rozładowane baterie, wejście w tryb serwisowy itp.)

**Zdefiniowana przez użytkownika 1** — specjalna, pierwsza grupa, gdzie instalator może przenieść pewne zdarzenia do raportowania (zwykle raporty o awariach i przywróceniu zasilania, ewentualnie uzbrojenie pomimo aktywnego urządzenia) wyłącznie dla wybranych użytkowników (administrator itp.)

**Zdefiniowana przez użytkownika 2** — specjalna, druga grupa, gdzie instalator może przenieść pewne zdarzenia do raportowania (zwykle niski poziom baterii w urządzeniach lub niski poziom baterii awaryjnej) wyłącznie dla wybranych użytkowników (zwykle instalator itp.).

**Raportowanie strefy** — określa, z której strefy będą raportowane wybrane grupy zdarzeń. W przypadku zaznaczenia SMS o błędach i serwisie i braku wyboru strefy zgłaszane będą wyłącznie błędy systemu (zawsze są przypisane do strefy nr 1). Nie ma powiązań między uwierzytelnieniem a możliwością sterowania strefą.

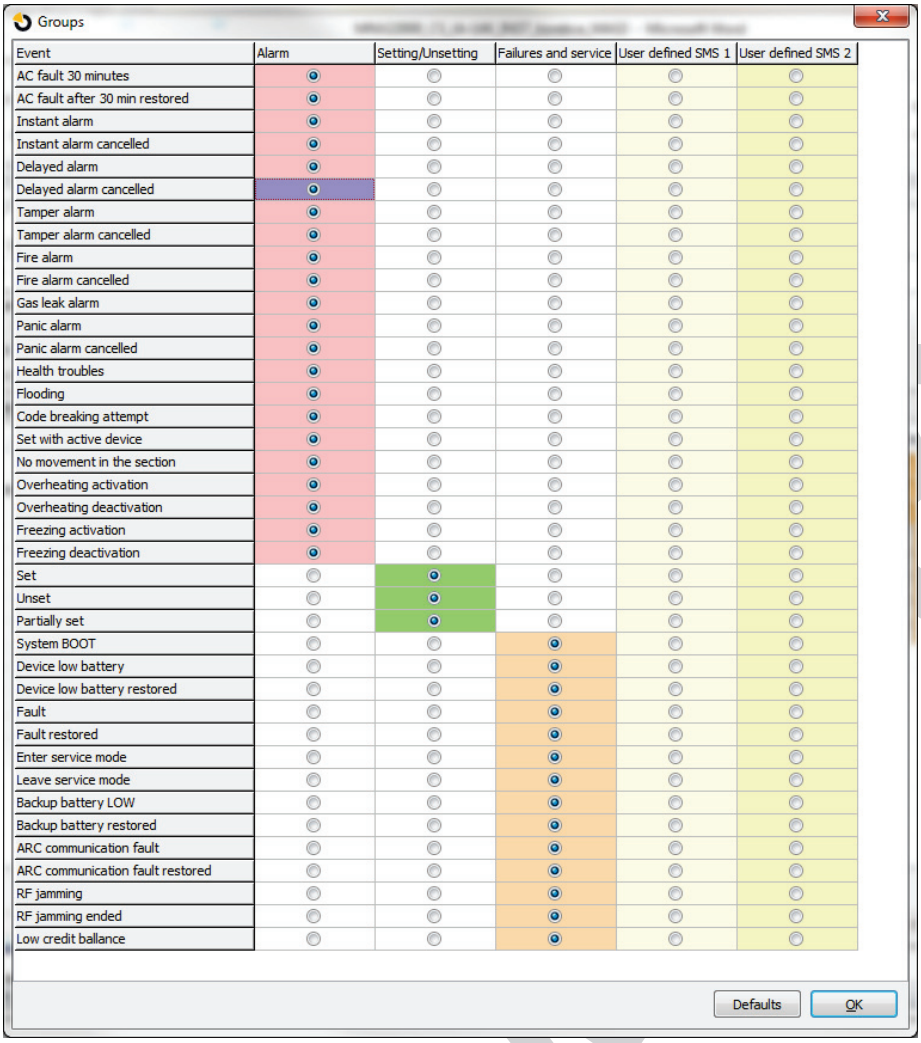
**Raporty wyjść PG*** możliwość raportowania włączenia/wyłączenia wyjść PG do użytkownika. Komunikaty są wysyłane ze stałym opóźnieniem 60 sekund. Teksty komunikatów SMS ustawia się w zakładce Wyjścia PG, patrz rozdział 10.5 PG outputs tab.

**Test** — naciśnięcie tego przycisku powoduje wysłanie testowego raportu SMS do użytkownika: „Raport testowy, Centrala alarmowa, Strefa 1”

**Tabela zdarzeń i zadanych grup:**

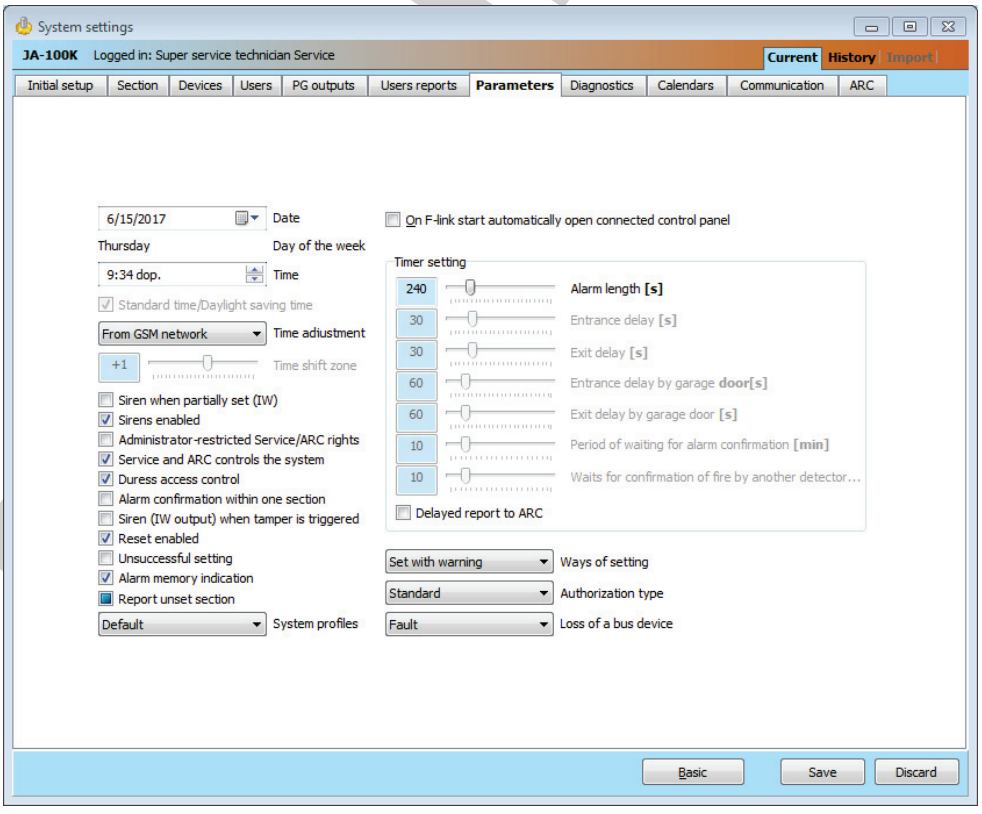


JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com




## 10.7 Zakładka Parametry

Służy do ustawiania parametrów i wybieralnych funkcji centrali alarmowej. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



| | | |
|---|---|---|
| **Data** | Wewnętrzne ustawienie kalendarza. | |
| **Dzień tygodnia** | Wyświetlanie dnia tygodnia | |
| **Godzina** | Wewnętrzne ustawienie zegara. | |
| **Czas standardowy / Czas zimowy*** | Do ręcznej regulacji czasu można wybrać jedynie automatyczne włączanie czasu zimowego i letniego. Zmiana następuje w ostatnią niedzielę marca lub października o godz. 1:00 UTC (tj. np. 2:00 CET, lub 3:00 CEST). | |
| **Regulacja czasu*** | Sposób regulacji wewnętrznego czasu i daty: | |
| | Ręcznie | Ręczne ustawianie godziny i daty przy użyciu programu F-Link |
| | Z sieci GSM | Godzinę i datę pobiera się od dostawcy usług GSM przy każdym logowaniu do sieci GSM |
| | Z serwera Jablotron (LAN / GSM) | Godzinę i datę reguluje się automatycznie zgodnie z serwerem komunikacji. Opcja nie działa, gdy ten rodzaj komunikacji ustawiono na „Bez programowania zdalnego" (domyślne ustawienie fabryczne) |
| **IW syreny przy uzbrojeniu częściowym** | Pozwala ustawić alarm dźwiękowy przy systemie IW, jeżeli strefa jest częściowo uzbrojona. Reakcje pożarowe i 24 h nie aktywują syreny w razie awarii, niezależnie od ustawienia tego parametru. | |
| **Syreny aktywne*** | Aktywuje wszystkie syreny MAGISTRALI i bezprzewodowe systemu (przeznaczone do dezaktywacji alarmu dźwiękowego podczas testów systemu). | |
| **Serwis ograniczony do Administratora i SMA** | Blokuje niezależny dostęp serwisantów i SMA do systemu.<br>Uwaga: W przypadku dostępu zdalnego serwisanta do systemu za pośrednictwem F-Link administrator może dokonać uwierzytelnienia przy pomocy klawiatury w budynku. W przypadku lokalnego połączenia przez serwisanta z centralą alarmową przy pomocy przewodu USB, z podłączonym uzupełniającym komunikatorem GSM / PSTN, administrator może dokonać własnego uwierzytelnienia zdalnie, korzystając z menu głosowego. | |
| **Sterowanie systemem przez serwisanta i SMA*** | To ustawienie umożliwia serwisantowi i serwisantowi SMA sterowanie systemem w odniesieniu do wszystkich stref. Jeśli ten parametr jest nieaktywny, serwisant nie ma prawa sterować strefami i może jedynie wejść w tryb serwisowy po rozbrojeniu wszystkich stref przez Administratora lub użytkownika. | |
| **Antynapadowa kontrola dostępu** | Służy do aktywacji cichego alarmu wyłącznie w drodze autoryzacji lub sterowania systemem (uzbrajanie, rozbrajanie, sterowanie PG itp.), kiedy użytkownik znajdzie się w obecności przestępcy. Alarm Panika aktywuje się podczas sterowania systemem przez wprowadzenie kodu, do którego ostatniej cyfry dodano 1. Przykład: kod użytkownika 4444, na potrzeby antynapadowej kontroli dostępu wpisz 4445. Uwaga: kiedy ostatnią cyfrą kodu użytkownika jest 9, w kodzie antynapadowej kontroli dostępu należy ją zastąpić 0. Przykład: Kod użytkownika = 4449, na potrzeby antynapadowej kontroli dostępu wpisać 4440 (0 na końcu).<br>Uwaga: aktywacja tej funkcji kasuje w systemie wszystkie predefiniowane kody!!! | |
| **Potwierdzenie alarmu w jednej strefie*** | Jeżeli dla czujki ustawiono reakcję z potwierdzeniem inną czujką, tę opcję potwierdzenia można wykorzystać do ograniczenia potwierdzenia wyłącznie **do tej samej** strefy (w przeciwnym razie alarm może potwierdzić czujka z dowolnej innej strefy). Dotyczy to zarówno czujek włamania, jak i czujek pożaru. | |
| **Syrena (wyjście IW) przy aktywacji sabotażu*** | Syrena z reakcją IW sygnalizuje dźwiękiem alarm sabotażu dla strefy rozbrojonej lub częściowo uzbrojone | |
| **Reset aktywny*** | Możliwość zablokowania resetowania centrali alarmowej za pomocą złącza na płytce. W przypadku zakazu resetowania i utraty kodu serwisowego centralę alarmową może odblokować wyłącznie producent. Resetowanie centrali alarmowej opisano w rozdziale 12 Reset of the control panel. | |
| **Niepowodzenie uzbrojenia** | Przetwarzanie tej funkcji zachodzi podczas każdej procedury uzbrajania. W przypadku aktywacji natychmiastowego w czasie opóźnienia na wyjście lub otwarcia strefy z opóźnieniem po wygaśnięciu czasu na wyjście nie nastąpi | |



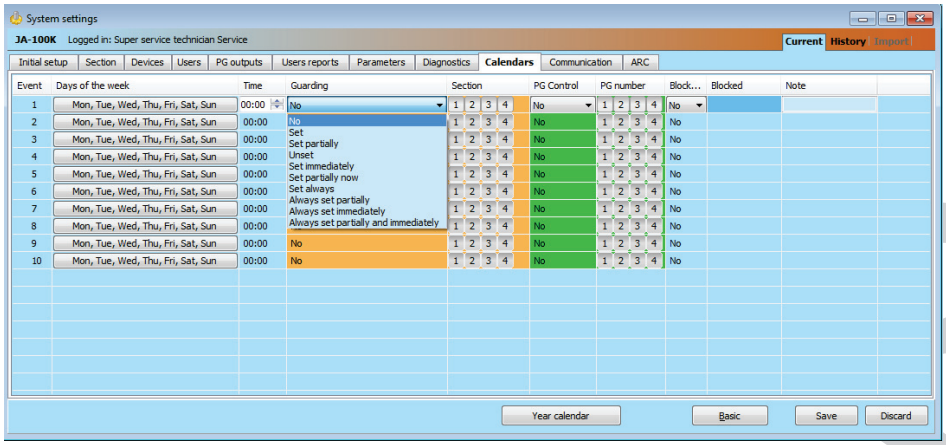
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

| | | |
|---|---|---|
| | uzbrojenie systemu, aktywuje się zdarzenie „Niepowodzenie uzbrajania", które zostanie zarejestrowane w historii. Zostanie ono zarejestrowane w historii, a także zgłoszone przez uzupełniający moduł GSM lub PSTN w przypadku jego podłączenia w postaci wiadomości SMS do zadanego użytkownika, jeżeli aktywowano możliwość wysłania zdarzenia „SMS o niepowodzeniu uzbrojenia". Wskazują je klawiatury oraz syrena zewnętrzna. Aby anulować sygnalizację niepowodzenia uzbrojenia, należy nacisnąć „Anuluj ostrzeżenie" w menu klawiatury. | |
| **Sygnalizacja pamięci alarmów** | Opcja umożliwia sygnalizację pamięci alarmów diodą wbudowaną w czujkę, która aktywowała alarm. Dostępne wyłącznie dla obsługiwanych urządzeń. | |
| **Profile systemu** | Wybór z zadanych profili systemu zgodnie z wymogami. | |
| | Domyślny | Parametry domyślne ustawione fabrycznie z opcją modyfikacji zależnie od potrzeb. |
| | EN50131-1, Klasa 2 | Niektóre parametry są zadane automatycznie zgodnie z normą EN50131-1, klasa 2 bez możliwości modyfikacji. |
| | INCERT, klasa 2 | Niektóre parametry są zadane automatycznie zgodnie z normą INCERT, klasa 2 bez możliwości modyfikacji. |
| **Sposoby uzbrajania** | Wybór sposobu, w jaki system zarządza procesem uzbrajania. Od najniższego poziomu, kiedy system można uzbroić niezależnie od aktywnych urządzeń i błędów w systemie do najwyższego poziomu, kiedy systemu nie można uzbroić z aktywnymi urządzeniami (alarm natychmiastowy). To ustawienie również łączy się z profilem systemu. | |
| | Uzbrój zawsze | Uzbraja zawsze niezależnie od statusu systemu (błędy, aktywne urządzenia,...) |
| | Uzbrój z ostrzeżeniem | Sygnalizuje optycznie (na przycisku funkcji i na wyświetlaczu) status systemu (błędy, aktywne elementy,<br>niski poziom baterii lub baterii awaryjnej) przez 8 sekund i po zakończeniu tego czasu uzbraja automatycznie. Uzbrojenie jest możliwe także przez wielokrotne naciśnięcie przycisku funkcji (lub klawisza ENTER). |
| | Uzbrój po potwierdzeniu | Sygnalizuje optycznie (przycisk funkcji i wyświetlacz) status systemu (błędy, aktywne elementy, niski poziom baterii lub baterii awaryjnej) przez 8 sekund. Można uzbroić WYŁĄCZNIE wielokrotnym naciśnięciem przycisku funkcji (lub naciśnięciem klawisza ENTER). |
| | Nie uzbrajaj z aktywnym elementem | Sygnalizuje optycznie (przycisk funkcji i wyświetlacz) status systemu (błędy, aktywne urządzenie, niski poziom baterii lub baterii awaryjnej) przez 8 sekund. System można uzbroić, wielokrotnie naciskając przycisk funkcji (lub klawisz ENTER), ale jedynie w przypadku, gdy aktywna czujka należy do typu reakcji OPÓŹNIONA lub NASTĘPNA OPÓŹNIONA. W ten sposób NIE MOŻNA uzbroić elementu aktywnego z jakąkolwiek inną reakcją alarmową. UWAGA!!! dotyczy to także sterowania zdalnego (menu głosowe, SMS, aplikacja sieciowa lub mobilna, działanie kalendarzowe). |
| **Typ uwierzytelniania** | Wybór sposobu, w jaki system przetwarza uwierzytelnienie użytkownika. Powiązane także ze sterowaniem wyjściem PG po uwierzytelnieniu. | |
| | Standardowy | Wprowadzenie kodu użytkownika lub korzystanie z breloka bądź karty RFID zapewni poprawne uwierzytelnienie. Do sterowania systemem konieczna jest tylko jedna z tych opcji. |
| | Uwierzytelnianie podwójne | Wprowadzenie kodu użytkownika i korzystanie z karty RFID zapewni poprawne uwierzytelnienie (niezależnie od kolejności uwierzytelniania). |

| | | |
|---|---|---|
| | | Program F-Link monitoruje, czy kod i karta zostały przypisane do użytkownika w Zakładce Użytkownicy (w przeciwnym razie F-Link nie pozwoli na zapisanie konfiguracji). Dostęp zdalny telefoniczny jest aktywny jedynie dla uprawnionych numerów. |
| **Utrata urządzenia MAGISTRALI** | Centrala alarmowa przetwarza utratę urządzenia lub zwarcie w MAGISTRALI systemu. Zależnie od wybranej opcji system zareaguje na zaistniałą sytuację: | |
| | Błąd | Centrala alarmowa zawsze przetwarza utratę urządzenia w MAGISTRALI lub zwarcie MAGISTRALI jako Błąd. |
| | Sabotaż zawsze | Centrala alarmowa przetwarza ewentualną utratę urządzenia MAGISTRALI lub zwarcie w MAGISTRALI w postaci alarmu sabotażu. Jeżeli dla modułu radiowego aktywowano wykrywanie tłumienia RF, i faktycznie dojdzie do wykrycia takiego tłumienia, również uruchomi on alarm sabotażu. Po alarmie sabotażu także występuje błąd, a kiedy błąd zniknie, skasuje się także alarm sabotażu. |
| | Sabotaż po potwierdzeniu | Centrala alarmowa przetwarza utratę pierwszego urządzenia jako błąd, a jeżeli w zadanym czasie, wynikającym z parametru „Okres oczekiwania na potwierdzenie alarmu”, wystąpi kolejna utrata urządzenia, system ją potwierdzi i aktywuje alarm sabotażu. Po usunięciu błędów wszystkich utraconych urządzeń system anuluje błąd i alarm sabotażu. |
| **Ustawienia zegara** | W każdej strefie osobno odmierza się opóźnienie na wejście i wyjście.<br>Jeżeli dla czujek w obrębie strefy określono różną długość opóźnienia, system zapewni najdłuższą z nich. W przypadku różnych długości czasu opóźnienia na wejście mierzy się czas dotyczący aktywnej czujki. W przypadku aktywności większej liczby czujek zapewnia się czas najkrótszego zdefiniowanego opóźnienia na wejście. | |
| **Długość alarmu** | Długość alarmu — dotyczy wszystkich stref. Zakres 5 sek.–20 min. | |
| **Opóźnienie na wejście** | Zegar. Zakres 5 sek.–2 min. | |
| **Opóźnienie na wyjście** | Zegar. Zakres 5 sek.–2 min. | |
| **Opóźnienie na wejście dla bramy garażu** | Zegar. Zakres 5 sek.–6 min. | |
| **Opóźnienie na wyjście dla bramy garażu** | Zegar. Zakres 5 sek.–6 min. | |
| **Oczekuje na potwierdzenie włamania z innej czujki** | Czas oczekiwania na potwierdzenie alarmu inną czujką w uzbrojonej strefie. Dotyczy wszystkich czujek z reakcją Potwierdzona natychmiastowa / Potwierdzona opóźniona (1–60 min). | |
| **Oczekuje na potwierdzenie pożaru z innej czujki** | Czas oczekiwania na potwierdzenie alarmu pożarowego inną czujką. Dotyczy wszystkich czujek z reakcją Pożarowa potwierdzona. (1–60 min.) | |
| **Zgłoś nieuzbrojoną strefę** | Strefa, która pozostała nieuzbrojona bez wykrycia ruchu przez ponad 16 godzin, zgłosi status „strefa rozbrojona”. | |
| **Opóźniony raport do SMA** | W przypadku aktywacji dojdzie do uruchomienia alarmu wewnętrznego po wygaśnięciu czasu na wejście, ale system odczeka 15 sekund przed wysłaniem raportu o alarmie do SMA. Dzięki temu użytkownik posiada kolejne 15 sekund na rozbrojenie systemu bez aktywacji alarmu zgłaszanego do SMA. | |

## 10.8 Zakładka Kalendarze

Tutaj można ustawić harmonogram czasowy zdarzeń, które system będzie realizował automatycznie i regularnie. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**Dni tygodnia** — określa, w które dni tygodnia należy wykonywać daną czynność (np. w każdy poniedziałek)

**Godzina** — określa, o której godzinie należy zrealizować daną czynność w określonym dniu.

**Ochrona** — pozwala realizować czynności „Uzbrój", „Uzbrój częściowo" z opcją „Natychmiast" (brak opóźnienia na wyjście lub sygnalizacji dźwiękowej) oraz opcją „Zawsze" (zawsze ignoruje zasady gotowości do uzbrojenia), a także „Rozbrój".

**Strefy** — określa, w której strefie (strefach) należy zrealizować czynność danego typu.

**Sterowanie PG*** — umożliwia ustawienie Aktywacji PG, Dezaktywacji PG, Blokowania PG lub Odblokowywania PG dla wyjść PG. Zablokowanymi wyjściami PG nie można sterować przyciskiem funkcji ani SMS.

**Numer PG*** — określa, które wyjście/a będą aktywne lub nieaktywne.

**Blokowanie** — tu znajdują się wyjścia PG, ich aktywacja umożliwia blokadę działania kalendarzowego.

**Dezaktywuj** — możliwość zablokowania konkretnego działania. Dezaktywację sygnalizuje czerwona kropka. Do dezaktywacji harmonogramu uprawniony jest serwisant (przy pomocy F-Link).

**Notatka** — pozwala dodać opis planowanych zdarzeń

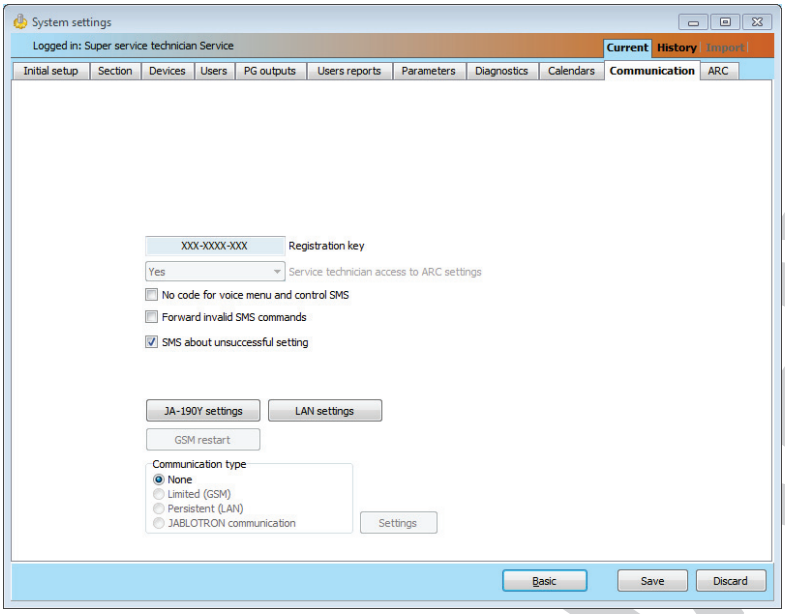
**Harmonogram roczny** — pozwala zmienić atrybut dnia na „Niedziela" dla poszczególnych dni w obecnym i przyszłym roku. Ten atrybut można zmienić (wielokrotnym) kliknięciem myszą na wybranym dniu. Przykład zastosowania: Dla przypadku święta państwowego (dnia wolnego od pracy), które przypada w środę, można zmienić atrybut dnia ze Środa na Niedziela. W tym dniu nie będą realizowane zdarzenia automatycznie planowane zgodnie z ustawieniami podstawowymi Harmonogramu i obowiązujące dla dni roboczych. Zostanie jednak zachowany program dla niedziel. W ten sposób można dostosować sterowanie Strefami lub Sterowanie PG np. także dla świąt firmowych itp. Atrybut „Wył." oznacza nieaktywny — w dniach oznaczonych w ten sposób nie realizuje się planowanych zdarzeń.

***Uwagi:***

- *Jedno zdarzenie harmonogramu może jednocześnie sterować (aktywacja i dezaktywacja) uzbrajaniem i wyjściami PG.*
- *Aplikację można na czas określony włączać i wyłączać na 2 sposoby. Można ustawić działanie do aktywacji i działanie do dezaktywacji wyjścia PG, lub jedynie działanie do aktywacji oraz impuls żądanej długości dla wyjścia PG.*
- *W przypadku wyboru Uzbrajania (Uzbrajania częściowego) określonej strefy o określonej godzinie aktywuje się najpierw opóźnienie na wyjście o stałej długości 3 minut. W ciągu tych 3 minut wszystkie czujniki w określonych strefach z reakcją Natychmiastową zostają dostosowane do reakcji Opóźnionej. W przypadku ustawienia Uzbrój natychmiast nie wystąpi opóźnienie na wyjście, a wszystkie czujki będą natychmiast aktywne (w tym czujki z opóźnieniem).*

## 10.9 Zakładka Komunikacja

Ta zakładka służy do ustawiania zachowania komunikatorów i sposobu komunikacji. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**Klucz rejestracji** — unikalny klucz rejestracji centrali alarmowej.

**Brak kodu do menu głosowego i SMS sterujących** — w przypadku korzystania z uwierzytelnionego telefonu do sterowania funkcją w drodze połączenia głosowego użytkownik nie musi wprowadzać kodu (uwierzytelnienie zachodzi przez wykonanie połączenia z własnego telefonu). Na potrzeby tej funkcji konieczna jest aktywacja identyfikacji rozmówcy (CLIP).

**Przekaż nieprawidłowe polecenia SMS do** — wybór, czy komunikaty SMS niezrozumiałe dla centrali alarmowej, mają zostać przesłane (np. informacje o fakturze od operatora) na numer telefonu Administratora w pozycji 1.

**SMS o niepowodzeniu uzbrajania** — w przypadku aktywacji tej opcji centrala alarmowa wysyła SMS o niepowodzeniu uzbrajania. W przypadku sterowania przez uprawnionego użytkownika centrala alarmowa wysyła SMS na telefon przypisany do tego użytkownika. Podczas sterowania bez uwierzytelniania centrala alarmowa wysyła SMS na numer telefonu administratora w pozycji 1.

Typ **komunikacji** — system oferuje kilka sposobów zdalnej komunikacji/konfiguracji

- **Bez konfiguracji zdalnej** — nie używa się żadnej komunikacji danych. Konfiguracja zdalna przy użyciu F-Link nie jest możliwa.
- **Ograniczona (GSM)** — centrala alarmowa może ustanowić połączenie danych z serwerem i umożliwia połączenie zdalne za pośrednictwem programu F-Link. Połączenie nie zużywa tak dużej ilości danych jak stała komunikacja (LAN). Tę opcję można aktywować, kiedy system jest wyposażony w komunikator GSM.
- **Stała (LAN)** — centrala alarmowa komunikuje się w sposób ciągły z serwerem i umożliwia połączenie zdalne za pośrednictwem F-Link. Kiedy system nie zawiera urządzenia GSM do automatycznego wybierania numerów, tę opcję można aktywować.
- **Komunikacja Jablotron** — rejestracja w chmurze JABLOTRON udostępnia wszystkie opcje oferowane przez system, jak połączenie zdalne za pośrednictwem F-Link i korzystanie z aplikacji MyJABLOTRON i MyCOMPANY.

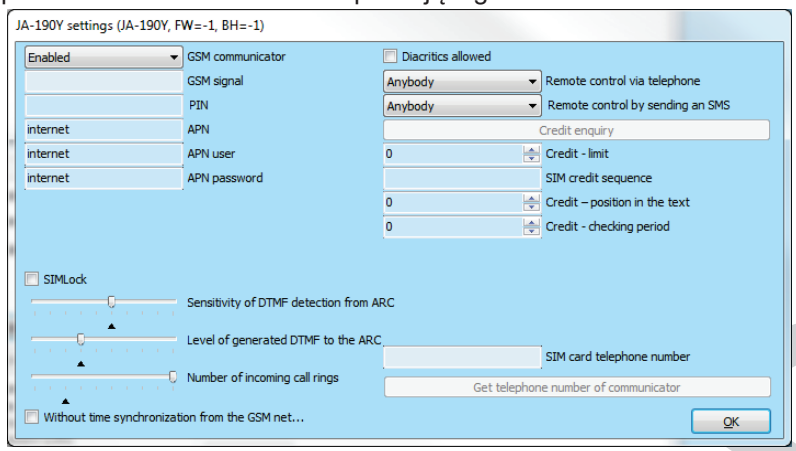
**Ustawienia** — wybór rodzaju centrali alarmowej z komunikacją zewnętrzną z serwerem JABLOTRON. Umożliwia zdalne łączenie za pośrednictwem F-Link, rejestrację systemu w chmurze i korzystanie z aplikacji MyJABLOTRON i MyCOMPANY.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

### 10.9.1 Ustawienia JA-190Y

Służą do ustawiania parametrów i zachowania uzupełniającego komunikatora GSM Ja-190Y.




**Komunikator GSM** — możliwość wyłączenia komunikatora.

**Sygnał GSM** — informacje na temat siły sygnału w procentach (mierzonej co minutę). Aby zapewnić poprawne działanie, siła sygnału powinna wynosić co najmniej 50%. W przypadku problemów związanych z jakością sygnału GSM zaleca się sprawdzenie karty SIM innego operatora. Nie zalecamy korzystania z kierunkowej ani wzmacniającej anteny GSM ogranicza podłączenie modułu do 1 komórki sieci = niestabilna komunikacja). Informacje o jakości sygnału można uzyskać także przy pomocy polecenia SMS STATUS (patrz 9.6 SMS commands).

**PIN** — Zalecamy stosowanie karty SIM z wyłączonym kodem PIN.

**APN*** — Ustawienia komunikacji danych GPRS. Komunikacja danych zapewnia dostęp do takich usług, jak dostęp zdalny serwisanta i użytkownika, komunikacja z CHMURĄ JABLOTRON, SMA itp. Oprócz ustawień APN konieczna jest obsługa transmisji danych przez używaną kartę SIM.

**Użytkownik APN***— nazwa (nie wpisywać, jeżeli sieć z niej nie korzysta).

**Hasło APN***— hasło (nie wpisywać, jeżeli sieć z niego nie korzysta).

**Czułość wykrywania DTMF ze SMA** — ustawienia czułości odbioru sygnałów generowanych przez SMA. Czułość ustawia się w 10 etapach, optymalną, domyślną wartością jest 6.

**Poziom generowanych DTMF do SMA** — ustawienia intensywności transmitowanych sygnałów tonalnych DTMF wygenerowanych przez centralę alarmową. Intensywność ustawia się w 10 etapach, optymalną, domyślną wartością jest 4.

**Liczba sygnałów połączeń przychodzących** — liczba sygnałów do chwili automatycznego odebrania przez komunikator. Można ustawić odebranie po 1 do 10 sygnałów (co odpowiada czasowi 5 do 50 sekund). Domyślna wartość to 3 (15 sekund).

**Znaki diakrytyczne dozwolone** — jeżeli dozwolone są międzynarodowe znaki akcentowane (ICC), raporty można wysyłać z systemu za pośrednictwem więcej niż jednego komunikatu tekstowego SMS. ICC należy włączyć np. w przypadku korzystania z alfabetu rosyjskiego itp.

**Zdalne sterowanie z telefonu** — ustawianie możliwości zdalnego sterowania systemem przy pomocy menu głosowego. W przypadku wyboru Użytkowników dostęp do menu można uzyskać jedynie z telefonów zdefiniowanych użytkowników (w zakładce Komunikacja można nawet umożliwić użytkownikom dostęp do menu głosowego bez wprowadzania kodu użytkownika — Menu głosowe bez kodu). Jeżeli wybrano opcję „Ktokolwiek”, dostęp do menu głosowego można uzyskać z dowolnego telefonu. Jednakże po uzyskaniu dostępu do menu użytkownik zawsze otrzyma prośbę o wprowadzenie kodu użytkownika.

**Zdalne sterowanie przez wybór SMS** — ustawianie możliwości sterowania systemem zdalnie przy pomocy poleceń SMS. W przypadku wyboru Użytkowników system przyjmuje jedynie polecenia SMS z telefonów zdefiniowanych użytkowników (w zakładce Komunikacja można nawet umożliwić użytkownikom korzystanie z poleceń SMS bez wprowadzania kodu użytkownika — Menu głosowe bez kodu). Jeżeli wybrano opcję „Ktokolwiek”, polecenie SMS można ustawić z dowolnego telefonu, zależy to jednak od wprowadzania kodu dostępu.

**Pytanie o kredyt** — naciskając ten przycisk, można bezzwłocznie pozyskać informacje o saldzie kredytu w formie odpowiedzi SMS od operatora (jeżeli ta funkcja jest obsługiwana).

**Limit kredytu** — możliwość ustawienia niższego kredytu do automatycznego sprawdzania limitu na karcie SIM typu pre-paid. Jeżeli ustalony kredyt znajdzie się poniżej tego poziomu, system wyśle SMS z informacją do osoby, do której przypisano raporty **SMS Błędy i serwis.** Uwaga: **nie zalecamy korzystania z kart pre-paid w systemie, ponieważ zwiększają one ryzyko awarii komunikacji.**

**Sekwencja kredytów SIM** — polecenie do automatycznego sprawdzania salda kredytów na karcie SIM typu pre-paid (jeżeli obsługiwane przez operatora). Można uzyskać polecenie od operatora.

**Pozycja kredytów w tekście** — pozycja (kolejny numer znaku) w raporcie salda kredytów od operatora, w której zaczyna się informacja numeryczna o saldzie kredytów (komunikator wyszukuje w raporcie jedynie liczebniki i ignoruje inne znaki)

**Okres sprawdzania kredytów** — ustawianie, jak często system sprawdza saldo kredytów (można ustawić od 0 do 99 dni, gdzie 0 oznacza wyłączone).

**Numer telefonicznej karty SIM** — tu pokazany jest numer telefonu włożonej karty SIM, system uzyskuje go z serwera.

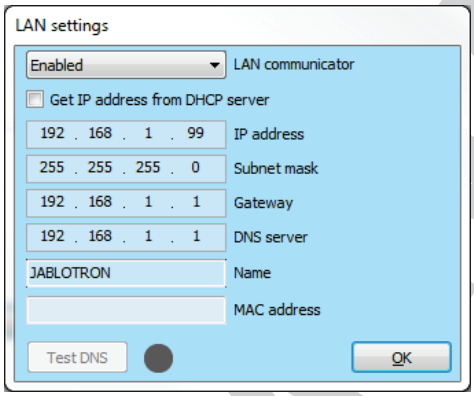
**Pozyskaj numer telefonu komunikatora** — Przycisk służy do ręcznego pozyskiwania numeru telefonu z serwera.

### 10.9.2 Restart modułu GSM

Przycisk do wylogowywania komunikatora i ponownego logowania go w sieci GSM. Ponowne zalogowanie komunikatora GSM w sieci może zabrać dziesiątki sekund (zależnie od aktualnego statusu systemu). Moduł GSM można zrestartować przy pomocy polecenia SMS GSM (patrz 9.6 SMS commands).

### 10.9.3 Ustawienia LAN

Służy do ustawiania komunikatora LAN.




**Komunikator LAN** — możliwość aktywacji i dezaktywacji komunikacji LAN.

**Pozyskaj adres IP z serwera DHCP** — automatyczne ustawienie parametrów sieci. Jeżeli sieć nie obsługuje tej funkcji, odpowiednie parametry należy wprowadzić ręcznie. Wprowadzanie ręczne jest możliwe po usunięciu zaznaczenia tej opcji.

**Adres IP** — ustawienie do ręcznego przypisywania adresu IP, które jest dostępne jedynie w przypadku, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne wynosi 192.168.1.99

**Maska podsieci** — ustawienie do ręcznego przypisywania IP maski podsieci, które jest dostępne jedynie w przypadku, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne wynosi 255.255.255.0.

**Bramka** — ustawienie do ręcznego przypisywania IP bramki domyślnej, które jest dostępne jedynie w przypadku, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne wynosi 192.168.1.1

**Serwer DNS** — ustawienie do ręcznego przypisywania IP serwera IP, które jest dostępne jedynie w przypadku, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne wynosi 192.168.1.1

**Nazwa** — nazwa urządzenia, ułatwiająca identyfikację w sieci lokalnej

**Adres MAC** — unikalny adres każdego urządzenia LAN (identyfikacja źródła danych)

Urządzenie LAN do identyfikacji źródła informacji

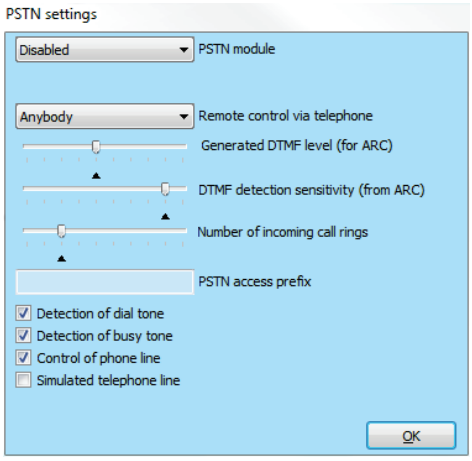
**Sprawdź DNS** — kiedy komunikator LAN jest połączony z internetem, można sprawdzić poprawność ustawień. Jeżeli po naciśnięciu przycisku pojawi się zielona kropka, ustanowiono połączenie z serwerem. Jeśli jednak po kilku sekundach pojawi się czerwona kropka, czas na ustanowienie połączenia wygasł, co oznacza nieprawidłowe ustawienie lub błąd łączenia komunikatora LAN.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

### 10.9.4 Ustawienia PSTN

Służy do ustawiania komunikatora telefonicznego (jeśli centrala alarmowa go posiada).




**Moduł PSTN** — możliwość aktywacji lub dezaktywacji komunikacji za pośrednictwem linii telefonicznej.

**Zdalne sterowanie z telefonu** — ustawianie możliwości zdalnego sterowania systemem przy pomocy menu głosowego. W przypadku wyboru Użytkowników dostęp do menu można uzyskać jedynie z telefonów zdefiniowanych użytkowników (w zakładce Komunikacja można nawet umożliwić użytkownikom dostęp do menu głosowego bez wprowadzania kodu użytkownika — Menu głosowe bez kodu). Jeżeli wybrano opcję „Ktokolwiek", dostęp do menu głosowego można uzyskać z dowolnego telefonu. Jednakże po uzyskaniu dostępu do menu użytkownik zawsze otrzyma prośbę o wprowadzenie kodu użytkownika.

**Poziom wygenerowanej DTMF (dla SMA)** — ustawienie intensywności przekazywanego sygnału wybierania numeru w DTMF wygenerowanej przez centralę alarmową. Intensywność ustawia się w 10 etapach, optymalną, domyślną wartością jest 4.

**Czułość wykrywania DTMF (ze SMA)** — ustawienia czułości odbioru sygnałów generowanych przez centrum odbioru alarmów (SMA). Czułość ustawia się w 10 etapach, optymalną, domyślną wartością jest 8.

**Liczba sygnałów dla połączeń przychodzących** — liczba impulsów sygnałów do czasu odebrania rozmowy przez komunikator. Odebranie można ustawić po 1 do 10 sygnałów (co odpowiada czasowi 5 do 50 sekund). Domyślna wartość wynosi 3 (15 sekund).

**Prefiks dostępu PSTN** — kod do wybierania numeru za pośrednictwem wewnętrznej centrali telefonicznej.

**Sygnał wyboru numeru** — jeśli ten parametr jest wyłączony, komunikator zacznie wybierać zadany numer telefonu niezależnie od rodzaju lub obecności sygnału wyboru numeru. Jeśli jest włączony, komunikator nie zacznie działać do chwili wykrycia sygnału wyboru numeru (np. opóźnienie przypisywania sygnału wyboru numeru w niektórych centralach telefonicznych).

**Wykrycie sygnału zajętości** — jeżeli komunikator wykryje sygnał zajętości, np. na linii równoległej, zakończy połączenie i powiadomi system. Ten parametr nie powinien być aktywny, ponieważ komunikator nie wykryje wówczas zakończenia połączenia.

**Kontrola linii telefonicznej** — komunikator całkowicie dezaktywuje wykrywanie napięcia w linii telefonicznej. Oznacza to, że nie będzie zgłaszał błędu wynikającego z niesprawnej linii telefonicznej. W przypadku takiej niesprawności sygnalizacja błędu nastąpi po upływie 30 minut od wykrycia utraty linii telefonicznej. Komunikator sygnalizuje błąd przy pomocy żółtej diody.

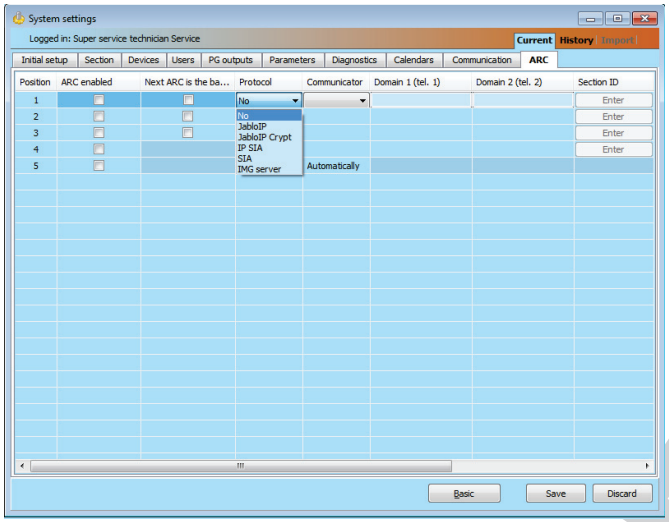
**Symulowana linia telefoniczna** — jeśli ten parametr jest aktywny, komunikator nie sprawdza obecności linii telefonicznej ani jej sygnałów. Tym samym nie wykryje błędu linii telefonicznej przy napięciu poniżej 15 V. Parametr przeznaczony do modemów radiowych.

Szczegółowy opis ustawień tego parametru znajduje się w instrukcji modułu komunikatora telefonicznego JA190X.

## 10.10 Zakładka SMA

Ta zakładka służy do konfiguracji komunikacji za pośrednictwem najwyżej 4 ścieżek transmisji lub 4 protokołów komunikacji. Z każdej ścieżki transmisji mogą korzystać najwyżej 4 różne centra odbioru alarmów lub, ogólnie, 4 różne odbiorniki raportów alarmów.

Serwisant posiada ograniczony dostęp do zakładki Komunikacja. Ten parametr może konfigurować jedynie osoba posiadająca uprawnienia na poziomie serwisanta SMA. Ta opcja nie jest dostępna także w przypadku zaznaczenia Komunikacja Jablotron, co znacznie upraszcza konfigurację części komunikacyjnej systemu. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.




**SMA aktywne** — możliwość dezaktywacji zadanej komunikacji

**Kolejne SMA jest awaryjne** — w przypadku aktywacji tego parametru kolejna pozycja zostanie wykorzystana wyłącznie, gdy danych nie można przesłać z aktualnego.

**Protokół** — ustawienia protokołu transmisji

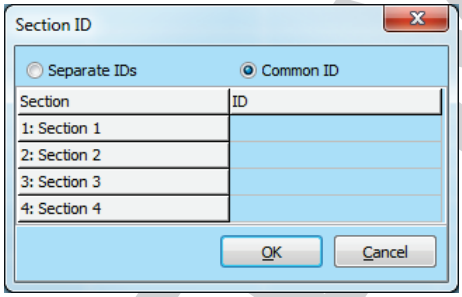
**Komunikator** — jeżeli wybrany protokół można transmitować na więcej sposobów, tutaj wybiera się rodzaj komunikatora

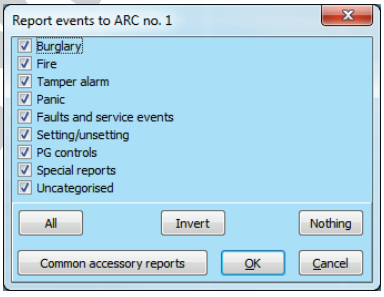
**Domena 1 (telefon 1)** — ustawienia domeny głównej (przy pomocy adresu URL lub IP), lub głównego numeru telefonu zależnie od używanego protokołu. W przypadku korzystania z komunikacji IP po adresie IP należy postawić dwukropek, a następnie wpisać port komunikacji. Port komunikacji i dane adresu IP można uzyskać ze SMA, do którego przekierowana jest komunikacja. Bez wpisanego portu komunikacji nie dojdzie do transmisji zdarzenia.

**Domena2 (telefon 2)** — ustawienie domeny awaryjnej (przy pomocy adresu URL lub IP), lub awaryjnego numeru telefonu, zależnie od używanego protokołu

**ID strefy** — ustawienie identyfikacji budynkowej (wspólnej dla całego budynku lub indywidualnej dla stref).

**Ostrzeżenie:** Domyślnym ustawieniem jest zero i wówczas komunikator nie wysyła żadnych raportów!




**Zgłaszane zdarzenia** — wybór rodzajów zgłaszanych zdarzeń i możliwość ustawienia kodów raportów uzupełniających (wyjścia PG)

**Ustawienia czasowe** — konfiguracja limitów czasu dla transmisji i ustawienia okresu sprawdzania połączenia.

**Test SMA** — naciśnięcie przycisku powoduje rozpoczęcie testu ręcznego w celu sprawdzenia połączenia z odpowiednim protokołem.

**Notatka** — tu można zanotować szczegółowe ustawienia SMA, datę rozpoczęcia eksploatacji itp.



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

### 10.10.1 Wymogi dotyczące konfiguracji ścieżek transmisji do SMA

Centrala alarmowa JA-100K może ustanowić ścieżki transmisji do SMA zgodnie z normami europejskimi EN 50136-1 i EN 50136-2. Poniższa tabela określa poszczególne parametry zgodne z daną klasą ATS. SMA musi w pełni obsługiwać klasy ATS.

| Klasa ATS | Interfejsy do użytku (Protokoły alarmowe) | Sprawdzenie połączenia w stałym czasie | Czas sprawdzania połączenia | Błąd w razie zbyt długiego opóźnienia raportu zdarzenia | Liczba powtórzeń | Okres oczekiwania po nieudanej próbie | Szyfrowanie<br>Godzina systemu<br>Godzina zdarzenia |
|---|---|---|---|---|---|---|---|
| SP2 | PSTN / GSM / LAN (JABLO IP, SIA IP, SIA CID) | Opcjonalnie | 1 x na 24 godz. | 120 s | 2 | 30 s | Opcjonalnie<br>Wymagane<br>Wymagane |
| SP3 | GSM / LAN (JABLO IP, SIA IP, SIA CID) | Niedozwolone | 1x 30 min | 60 s | 2 | 30 s | Opcjonalnie<br>Wymagane<br>Wymagane |
| SP4 | GSM / LAN (JABLO IP, SIA IP) | Niedozwolone | 1x 3 min | 60 s | 3 | 20 s | Wymagane<br>Wymagane<br>Wymagane |
| SP5 | GSM / LAN (JABLO IP, SIA IP) | Niedozwolone | 1x 1 min | 30 s | 6 | 5 s | Wymagane<br>Wymagane<br>Wymagane |
| DP2 | LAN + PSTN (JABLO IP, SIA IP) | Niedozwolone | 1x 30 min | 60 s | 2 | 30 s | Opcjonalnie<br>Wymagane<br>Wymagane |
| DP3 | LAN + GSM (JABLO IP, SIA IP) | Niedozwolone | 1x 3 min | 60 s | 3 | 20 s | Wymagane<br>Wymagane<br>Wymagane |

### 10.10.2 Ścieżki transmisji

Dla komunikacji GSM (GPRS) i LAN z użyciem protokołów IP:

1) Protokół ANSI SIA DC-09, SIA IP (DC9), metody DCS lub ADM_CID (przekaz danych)
   — szyfrowanie zgodnie z normą AES z kluczami 128-, 192- lub 256-bitowymi
   — dodane unikalne znaczniki czasu przekazu
   — bardzo dokładna synchronizacja czasowa między systemem alarmowym a SMA
2) Protokół JABLO_IP (przekaz danych)
   — autorski protokół Jablotron
   — szyfrowanie 256-bitowe
   — dodane unikalne znaczniki czasu przekazu
   — dokładna synchronizacja czasowa między systemem alarmowym a SMA
3) JABLO_SMS (przekaz danych przez SMS)
   — oparty na protokole JABLO_IP z pływającym szyfrowaniem danych

### 10.10.3 Kody JABLOTRON 100 CID i SIA

| CID | SIA | Zdarzenie EN | Kategoria raportu |
|---|---|---|---|
| 1101 | QA | Problem zdrowotny | Włamanie |
| 1110 | FA | Alarm pożarowy | Pożar |
| 1118 | FG | Niepotwierdzony alarm pożarowy | Pożar |
| 1120 | PA | Alarm panika | Panika |
| 1130 | BA | Alarm natychmiastowy | Włamanie |
| 1133 | BA | Alarm 24 h | Włamanie |
| 1134 | BA | Alarm opóźniony | Włamanie |
| 1138 | BG | Alarm niepotwierdzony | Włamanie |
| 1144 | TA | Sabotaż urządzenia | Sabotaż |
| 1151 | GA | Wyciek gazu | Pożar |
| 1154 | WA | Alarm zalania | Sabotaż |
| 1170 | UA | Reakcja specjalna A | Raporty specjalne |
| 1171 | UA | Reakcja specjalna B | Raporty specjalne |
| 1172 | UA | Reakcja specjalna C | Raporty specjalne |
| 1173 | UA | Reakcja specjalna D | Raporty specjalne |
| 1174 | UA | Nieużywana | Raporty specjalne |
| 1175 | UA | Nieużywana | Raporty specjalne |
| 1176 | UA | Nieużywana | Raporty specjalne |
| 1177 | UA | Szafka na klucze | Raporty specjalne |
| 1300 | ET | Błąd | Błędy i zdarzenia serwisowe |
| 1301 | AT | Utrata zasilania sieciowego | Włamanie |
| 6301 | AT | Utrata zasilania sieciowego przez ponad 30 min. (od FW 10) | Włamanie |
| 1302 | YT | Niski poziom baterii w centrali alarmowej | Błędy i zdarzenia serwisowe |
| 1305 | RR | Uruchomienie systemu | Błędy i zdarzenia serwisowe |
| 1306 | LB | Wejście w tryb serwisowy | Błędy i zdarzenia serwisowe |
| 1308 | RE | Zamknięcie systemu | Błędy i zdarzenia serwisowe |
| 1313 | YX | Zablokowany po alarmie — reset inżynierski | Nieskategoryzowany |
| 1314 | YG | Ustawienia SMA skasowane | Nieskategoryzowany |
| 1344 | XQ | Tłumienie RF / zakłócenia RF | Błędy i zdarzenia serwisowe |
| 1350 | YC | Nie dostarczono zdarzenia do SMA | Nieskategoryzowany |
| 1354 | YS | Nie dostarczono zdarzenia do SMA w zadanym czasie | Błędy i zdarzenia serwisowe |
| 1384 | XT | Niski poziom baterii w urządzeniu | Błędy i zdarzenia serwisowe |
| 1401 | OP | Rozbrój | Uzbrajanie / Rozbrajanie |
| 1402 | OG | Rozbrój częściowo | Uzbrajanie / Rozbrajanie |
| 1406 | BC | Alarm odwołany przez użytkownika | Włamanie |
| 1407 | OQ | Rozbrój zdalnie | Uzbrajanie / Rozbrajanie |
| 1412 | LF | Dostęp zdalny | Nieskategoryzowany |
| 1416 | LS | Konfigurację zapisano | Nieskategoryzowany |
| 1454 | CI | Strefa bez ruchu | Błędy i zdarzenia serwisowe |
| 1455 | CI | Niepowodzenie uzbrojenia | Nieskategoryzowany |
| 1461 | JA | Przekroczono liczbę prób złamania kodu | Sabotaż |
| 1521 | BL | Syrena wyciszona | Nieskategoryzowany |
| 1570 | EB | Pominięcie urządzenia (nieaktywne) | Nieskategoryzowany |
| 1572 | TB | Pominięcie sabotażu | Błędy i zdarzenia serwisowe |
| 1573 | BB | Pominięcie aktywacji | Błędy i zdarzenia serwisowe |
| 1574 | UB | Pominięcie strefy (nieaktywne) | Nieskategoryzowany |
| 1578 | UO | Pominięcie błędu | Błędy i zdarzenia serwisowe |
| 1601 | RX | Test ręczny | Błędy i zdarzenia serwisowe |
| 1602 | RP | Test okresowy / test łącza | Nieskategoryzowany |
| 1625 | JT | Reset czasu | Nieskategoryzowany |
| 1661 | RC | PG1 WŁ. | Sterowniki PG |
| 1662 | RC | PG2 WŁ. | Sterowniki PG |
| 1663 | RC | PG3 WŁ. | Sterowniki PG |
| 1664 | RC | PG4 WŁ. | Sterowniki PG |
| 3101 | QR | Problemy zdrowotne (dezaktywacja) | Włamanie |
| 3110 | FR | Alarm pożarowy (dezaktywacja) | Pożar |
| 3118 | FG | Niepotwierdzony alarm pożarowy (dezaktywacja) | Pożar |
| 3120 | PR | Panika (dezaktywacja) | Panika |



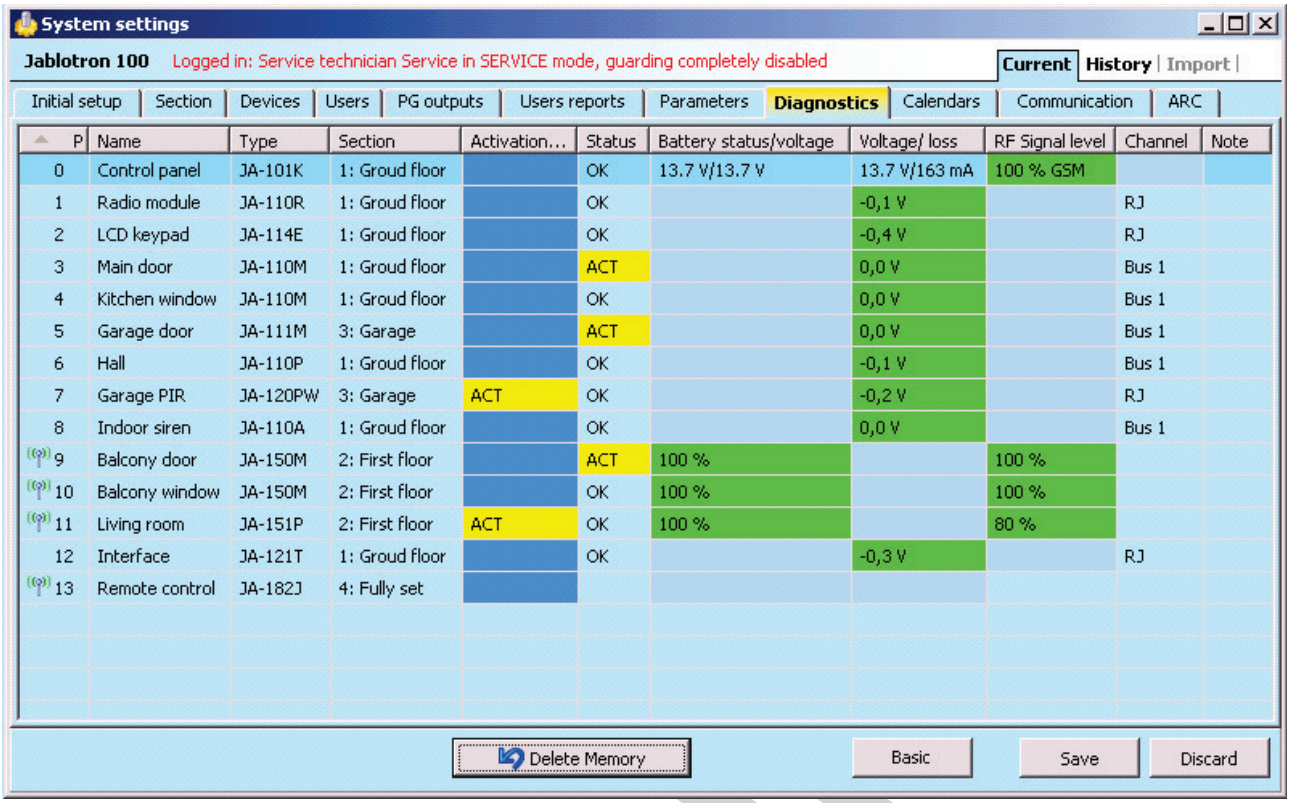
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

| | | | |
|---|---|---|---|
| 3130 | BR | Alarm natychmiastowy (dezaktywacja) | Włamanie |
| 3133 | BR | Alarm 24 h (dezaktywacja) | Włamanie |
| 3134 | BR | Alarm opóźniony (dezaktywacja) | Włamanie |
| 3138 | BG | Alarm niepotwierdzony (dezaktywacja) | Włamanie |
| 3144 | TR | Sabotaż (dezaktywacja) | Sabotaż |
| 3151 | GR | Wyciek gazu (dezaktywacja) | Pożar |
| 3154 | WR | Alarm zalania (dezaktywacja) | Sabotaż |
| 3170 | UR | Reakcja specjalna A (dezaktywacja) | Raporty specjalne |
| 3171 | UR | Reakcja specjalna B (dezaktywacja) | Raporty specjalne |
| 3172 | UR | Reakcja specjalna C (dezaktywacja) | Raporty specjalne |
| 3173 | UR | Reakcja specjalna D (dezaktywacja) | Raporty specjalne |
| 3174 | UR | Nieużywana | Raporty specjalne |
| 3175 | UR | Nieużywana | Raporty specjalne |
| 3176 | UR | Nieużywana | Raporty specjalne |
| 3177 | UR | Szafka na klucze (dezaktywacja) | Raporty specjalne |
| 3300 | ER | Błąd (dezaktywacja) | Błędy i zdarzenia serwisowe |
| 3301 | AR | Przywrócenie zasilania sieciowego | Nieskategoryzowany |
| 3302 | YR | Bateria awaryjna centrali alarmowej OK | Raporty specjalne |
| 3306 | LX | Wyjście z trybu serwisowego | Raporty specjalne |
| 3313 | YZ | Odblokowane po alarmie | Nieskategoryzowany |
| 3344 | YH | Zakłócenia RF / tłumienie RF (dezaktywacja) | Błędy i zdarzenia serwisowe |
| 3350 | YK | Przywrócenie komunikacji do SMA | Nieskategoryzowany |
| 3354 | YL | Nie dostarczono zdarzenia do SMA w zadanym czasie (dezaktywacja) | Błędy i zdarzenia serwisowe |
| 3384 | XR | Bateria urządzenia OK | Błędy i zdarzenia serwisowe |
| 3401 | CL | Uzbrojona | Uzbrajanie / Rozbrajanie |
| 3402 | CG | Częściowo uzbrojona | Uzbrajanie / Rozbrajanie |
| 3407 | CQ | Uzbrój zdalnie | Uzbrajanie / Rozbrajanie |
| 3412 | LE | Dostęp zdalny zamknięty | Nieskategoryzowany |
| 3417 | CU | Zdalnie uzbrojony częściowo | Uzbrajanie / Rozbrajanie |
| 3570 | EU | Koniec pominięcia urządzenia (dezaktywacja) | Nieskategoryzowany |
| 3572 | TU | Koniec pominięcia sabotażu | Sabotaż |
| 3573 | BU | Koniec pominięcia aktywacji | Nieskategoryzowany |
| 3574 | UU | Koniec pominięcia strefy (dezaktywacja) | Nieskategoryzowany |
| 3578 | UP | Pominięcie błędu (dezaktywacja) | Błędy i zdarzenia serwisowe |
| 3661 | RO | PG1 WYŁ. | Sterowniki PG |
| 3662 | RO | PG2 WYŁ. | Sterowniki PG |
| 3663 | RO | PG3 WYŁ. | Sterowniki PG |
| 3664 | RO | PG4 WYŁ. | Sterowniki PG |

| Kod źródłowy | Opis |
|---|---|
| 001–120 | Urządzenia |
| 501–800 | Kody użytkownika |
| 500 | Kod serwisowy |
| 901 | Centrala alarmowa |
| 921 | SMA1 |
| 922 | SMA2 |
| 923 | SMA3 |
| 924 | SMA4 |
| 912 | Komunikator LAN |
| 913 | Komunikator PSTN |
| 914 | Uzupełniający komunikator GSM |

## 10.11 Zakładka Diagnostyka

Służy do sprawdzania i weryfikacji statusu urządzeń i ich właściwości.




**Pamięć aktywacji** — rejestruje aktywacje urządzenia, które wystąpiły od ostatniego skasowania tej kolumny. Pamięć wszystkich aktywacji urządzeń można usunąć przy pomocy przycisku Usuń pamięć (dolny pasek). Pamięć wybranego urządzenia można skasować prawym klawiszem myszy. Aktywacja czujnika sabotażu (TMP) posiada najwyższy priorytet podczas rejestrowania zdarzeń w pamięci.

**Status** — wskazuje aktualny status urządzenia. OK = wszystko w porządku, TMP = sabotaż, ACT = aktywne wejście alarmowe, ERR = błąd, ?? = brak komunikacji z urządzeniem, Mains supply = awaria zasilania (lub całkowicie rozładowana bateria), Charging = ładowanie baterii awaryjnej w urządzeniu lub centrali alarmowej. Battery = rozładowana lub odłączona bateria w centrali alarmowej, BOOT = trwa ulepszanie urządzenia
lub awaria ulepszania (powtórz ulepszanie). Najechanie kursorem myszy na STATUS danego urządzenia pozwala wyświetlić szczegółowe informacje.

**Status baterii/napięcie*** — Jeżeli urządzenie zawiera baterię, wyświetli się jej status. Dla centrali alarmowej (pozycja 0) wyświetla się napięcie baterii awaryjnej. Jeśli nie ma danych dotyczących napięcia urządzenia bezprzewodowego, nie nastąpiła jeszcze komunikacja urządzenia — należy aktywować jego transmisję (np. za pomocą czujnika sabotażu lub przycisku Odśwież w programie F-Link) lub poczekać na automatyczne wystąpienie transmisji. Jeżeli klawiatury bezprzewodowe otrzymują zasilanie z zewnętrznego źródła energii, pojawi się komunikat „Zasilanie ze źródła zewnętrznego". Kod kolorystyczny stanu baterii: 10% czerwony, 20% żółty, 30% i więcej zielony.

**Napięcie/utrata*** — W pozycji centrali alarmowej (0) wyświetla się napięcie zacisków centrali alarmowej i natężenie pobierane przez urządzenia MAGISTRALI z centrali alarmowej. W przypadku urządzenia MAGISTRALI wyświetla się spadek napięcia w sieci w porównaniu z centralą alarmową. Spadek nie może przekraczać 2 V. W przeciwnym razie problem wymaga rozwiązania (np. przez dodanie wzmacniacza mocy MAGISTRALI).

**Poziom sygnału RF*** — sygnalizuje jakość sygnału, za którego pomocą centrala alarmowa komunikuje się przy użyciu GSM w przypadku podłączenia uzupełniającego komunikatora GSM lub bezprzewodowego urządzenia RF. Wartość powinna wynosić co najmniej 50%. Jeżeli nie ma takiego wskazania, nie ustanowiono jeszcze komunikacji urządzenia — aktywować transmisję (np. czujnikiem sabotażu) lub poczekać na wystąpienie automatycznej komunikacji. Wartość w wierszu centrali alarmowej oznacza siłę sygnału sieci GSM (zakłócenia między modułami radiowymi i modułem GSM opisano także w rozdziale 6.1 Installation of a JA-111R radio module).

Kod kolorystyczny sygnału GSM: 0–30% czerwony, 40–50% żółty i ponad 50% zielony.

Kod kolorystyczny sygnału RF: 10% czerwony, 20% żółty, 30% i więcej zielony.

**Kanał*** — informuje o MAGISTRALI używanej przez urządzenie do komunikacji. Rozróżnia się dwie ścieżki: Wyjście MAGISTRALI i złącze RF przeznaczone do modułu radiowego JA-11xR. Istnieje specjalna kolumna pt. Kanał, która wskazuje, za pośrednictwem których urządzeń dwukierunkowych następuje w danej chwili komunikacja.

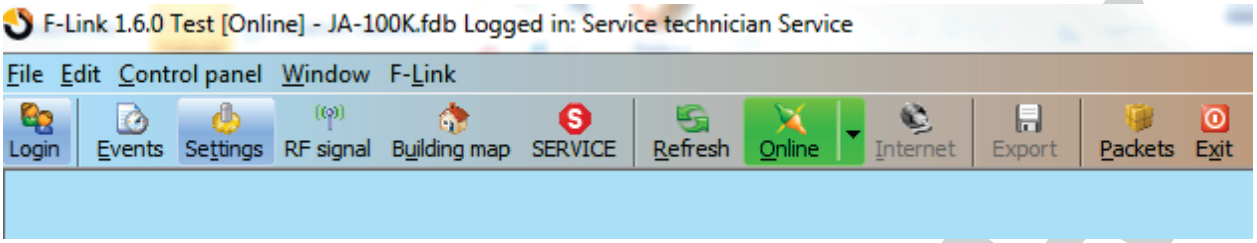


JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

# 11 Inne opcje programu F-Link

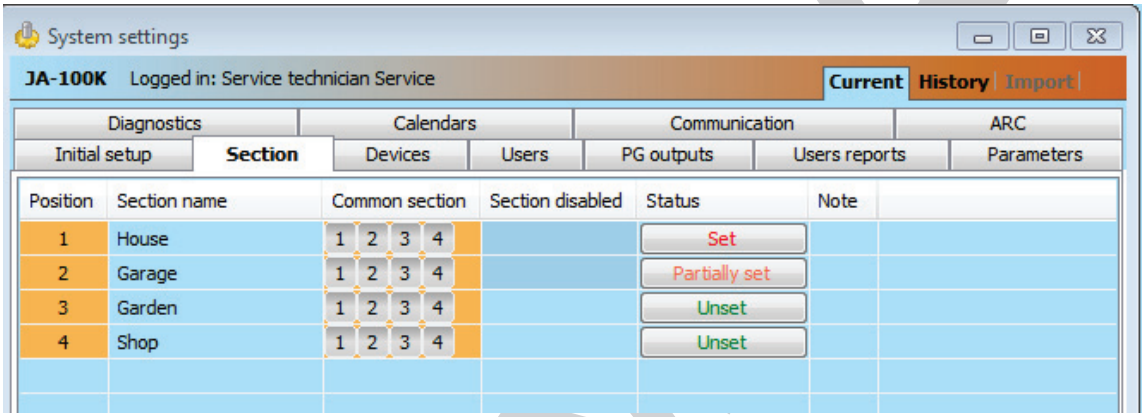
Wersja F-Link jest zawsze przedstawiona w górnym pasku za nazwą.

Pasek narzędzi zapewnia szybki dostęp do często używanych elementów, jak przycisk do zmiany trybów, zdarzeń systemu, ustawień, sygnał RF modułów radiowych, eksportu ustawień lub lokalnego i zdalnego dostępu do centrali alarmowej.

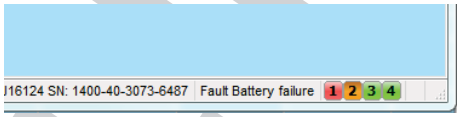



## 11.1 Sterowanie systemem za pomocą F-Link

Poszczególnymi strefami w programie F-Link można sterować lokalnie lub zdalnie na dwa sposoby. Pierwszy z nich to kliknięcie przycisku w zakładce Strefa, kolumna Status.



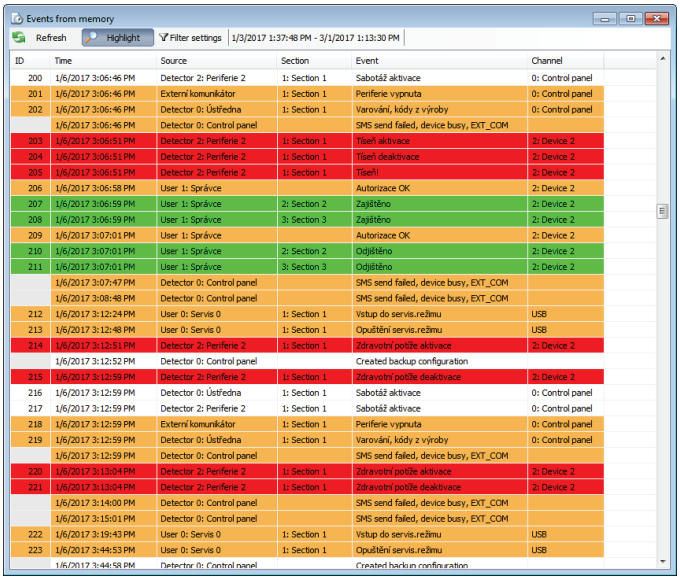

Drugi to kliknięcie ikon reprezentujących status systemu na dolnym pasku narzędzi. Uwierzytelnienie użytkownika rejestruje się w historii systemu w oparciu o aktualny kod używany do logowania w programie F-Link.




## 11.2 Historia zdarzeń:

Dostęp do historii zdarzeń można uzyskać w programie F-Link przez naciśnięcie przycisku Zdarzenie i wybór opcji „Historia zdarzeń”. W pamięci centrali alarmowej (karta microSD) można zapisać nawet kilka milionów rejestrów z kolejnym numerem, dokładną datą i godziną oraz źródłem zdarzenia.

**Zdarzenia z pamięci centrali alarmowej** (dostępne także po naciśnięciu F8) — wczytuje się około 100 kB zdarzeń (z karty microSD). Jeżeli zakres wczytywania jest niewystarczający, można kilkakrotnie wybrać opcję Wczytaj / Następne 100(500) kB lub Wszystkie. Ostrzeżenie: Wybór opcji Wczytaj/Wszystkie w przypadku centrali alarmowej z dłuższym czasem działania może spowodować, że wczytywanie potrwa kilka minut. Historia nie rejestruje zdarzeń, które wystąpią podczas konfiguracji systemu (rejestruje jedynie otwarcie i zamknięcie trybu serwisowego).



Wczytane zdarzenia można zapisać w pliku w menu Plik przy użyciu opcji Eksportuj (Shft+Ctrl+S) w kilku formatach (FDE, PDF, TXT, CSV, XML, HTM lub HTML). Przyrostek FDE pozwala programowi F-Link ponownie pobrać zdarzenia.

**Zdarzenia online**(dostępne także po naciśnięciu F7) — w tabeli tymczasowej rejestruje się wszystkie zdarzenia zapisane w historii zdarzeń, które wystąpią po aktywacji tej opcji, w tym zdarzenia podczas konfiguracji serwisowej.

**Sygnały online** (dostępne także po naciśnięciu of F6) — w tabeli tymczasowej rejestruje się wszystkie sygnały rejestrowane przez MAGISTRALĘ (np. także aktywacja i dezaktywacja czujników).

**Zdarzenia z pliku** — można otworzyć zdarzenia z historii zdarzeń zapisane w formacie pliku bazy danych FDE (patrz Zdarzenia z pamięci centrali alarmowej)

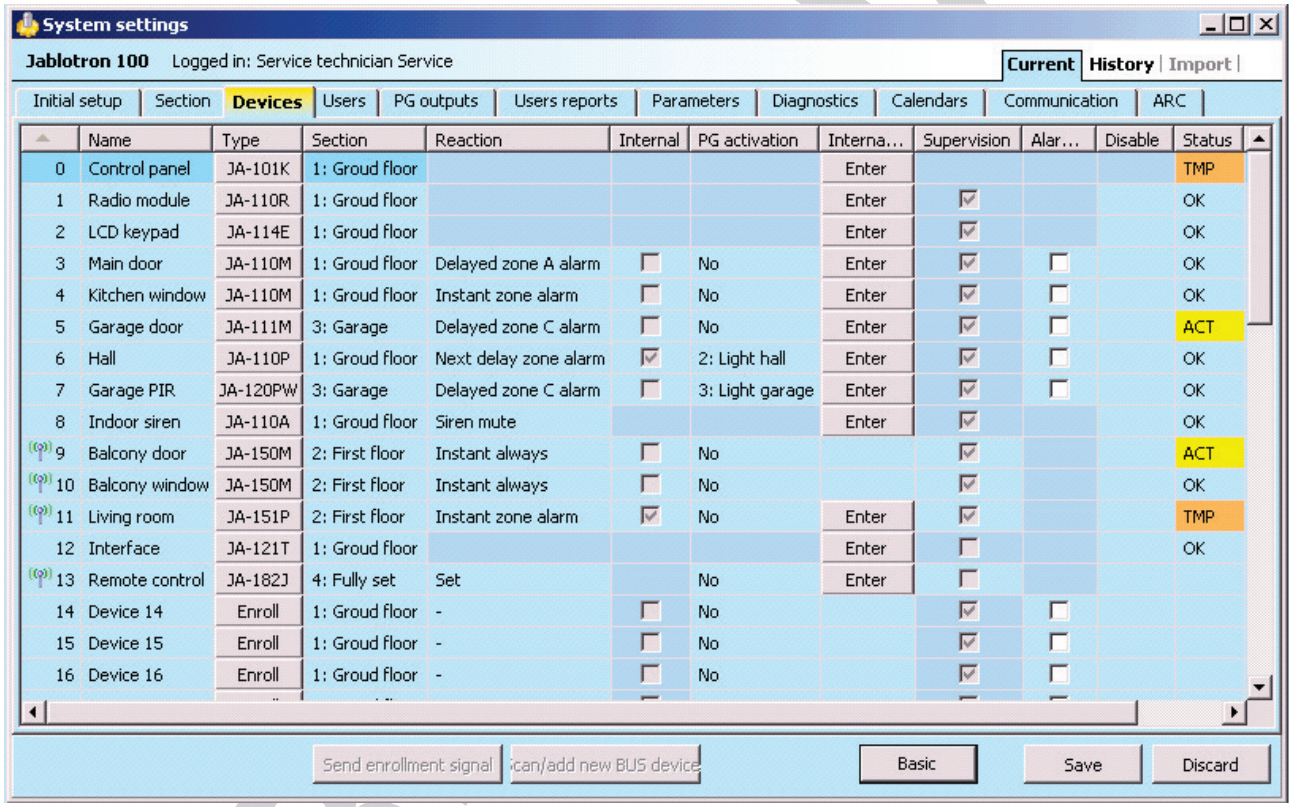
**Odśwież** — pozwala wczytać większą liczbę zdarzeń z historii w partiach po 100 kB, 500 kB (100 kB odpowiada około 1200 zdarzeniom) lub wszystkie zdarzenia.

**Wyróżnij** — wyróżnienie kolorem pozwala odróżnić rodzaje zdarzeń (alarm czerwony, sterowanie zielony, błąd pomarańczowy, sabotaż niebieski, neutralny jasnoniebieski, automatyka lub transmisje szary itp.)

**Ustawienia filtra** — filtr pozwala uzyskać tylko żądane informacje, klasyfikowane szczegółowo na podstawie godziny, rodzaju zdarzenia, stref, użytkowników, urządzeń lub wyjść PG. Filtry można łączyć, by zwiększyć skuteczność wyszukiwania w odległej historii.

## 11.3 Ustawienia systemu

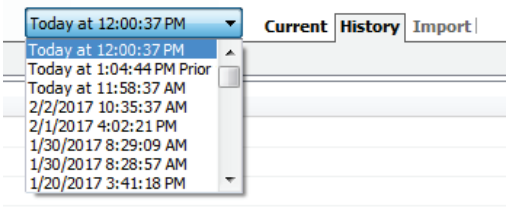
Dostępne jest okno używane do konfiguracji zachowania systemu, wszystkich urządzeń, stref, użytkowników, wyjść PG, komunikatorów oraz transmisji do SMA. Aby do niego wejść, należy nacisnąć przycisk Ustawienia na podstawowym górnym pasku.




1. Okno Ustawienia systemu otwiera się i zamyka przyciskiem **Ustawienia** 

na górnym pasku narzędzi.
2. W oknie można przełączać między następującymi **zakładkami: Strefy, Urządzenia, Użytkownicy, Wyjścia PG, Parametry,** …
3. Okno wyświetli **aktualną konfigurację centrali alarmowej** wczytaną po otwarciu programu F-Link (dalej wyłącznie program). Przycisk **Odśwież** na górnym pasku narzędzi można wykorzystać w dowolnej chwili do wczytywania aktualnej zawartości centrali alarmowej.
4. Jeśli chcą Państwo wyświetlić **starsze ustawienia centrali alarmowej, należy skorzystać z zakładki Historia** w prawym górnym rogu. Historii nie można zmienić, ale można ją zapisać w centrali alarmowej (na wypadek konieczności przywrócenia wcześniejszych ustawień). W historii rejestruje się 100 poprzednich ustawień (uporządkowanych na podstawie daty i godziny), a także wszystkie zmiany ustawień.

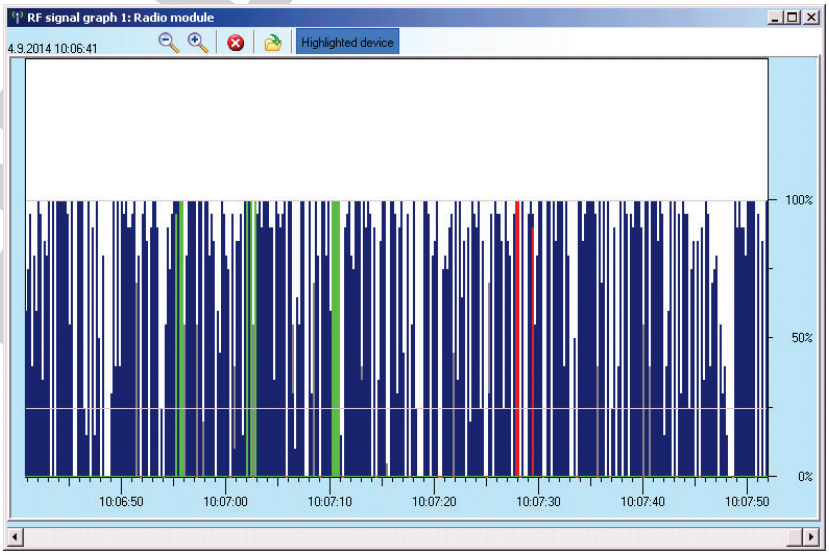
5. Można **zaimportować ustawienia** do systemu z innej instalacji, np. po wymianie starej centrali alarmowej na nową lub wykorzystaniu domyślnego szablonu. W przypadku wymiany centrali alarmowej na nową po podłączeniu na komputerze zostanie utworzona całkowicie nowa baza danych. Aby dokonać importu ustawień z innej bazy danych, na górnym pasku menu głównego należy zaznaczyć **Plik / Importuj** , a następnie plik, z którego chcą Państwo importować ustawienia. Po dokonaniu tego wyboru pojawi się przycisk **Importuj** w zakładce **Ustawienia systemu**.




6. **Zmiany ustawienia zostaną oznaczone tekstem w kolorze niebieskim** (również nazwa zakładki zmieni kolor na niebieski). Kolor niebieski zniknie natychmiast po zapisaniu zmian.
7. Można **Zapisać ustawienia** przyciskiem **Zapisz** (na dole z prawej strony). Podczas pierwszego zapisywania ustawień w centrali alarmowej program poprosi o **wprowadzenie nazwy pliku**. Na komputerze zostanie utworzony plik z przyrostkiem *FDB, w którym stopniowo będzie zapisywana historia ustawień (przy każdym zapisaniu ustawień w centrali alarmowej). Jeśli nie chcą Państwo zapisywać zmian, proszę zaznaczyć przycisk **Anuluj** i po otrzymaniu prośby o potwierdzenie wybrać **Ignoruj**. Parametry można zmienić w większej liczbie zakładek, a potem można zapisać wszystkie zmiany.
8. Przycisk **Przypisz nieprzypisane** (dolny pasek narzędzi w zakładce Urządzenia) otworzy okno dialogowe do łącznego przypisywania (bez możliwości wyboru pozycji) urządzeń podłączonych z MAGISTRALĄ ale nie podłączonych z systemem w inny sposób. Patrz rozdział 8.4.1Enrolling and erasing devices.
9. Przycisk **Wyślij sygnał przypisywania** (zakładka Urządzenia i wyjścia PG) zwolni wysyłanie kodu przypisywania centrali alarmowej do urządzeń bezprzewodowych, np. do bezprzewodowych modułów wyjść.
10. **Wszystkie parametry można skonfigurować jedynie w trybie serwisowym** (system nie jest w aktywnym trybie konfiguracji). Do aktywacji i dezaktywacji trybu serwisowego służy przycisk **Serwis** na górnym pasku narzędzi.
11. **Niektóre parametry można zmienić podczas eksploatacji.** Dlatego też można otworzyć zakładkę Serwis, nie wchodząc w tryb serwisowy. Można ustawić jedynie dostępne opcje.
12. **Program zawiera dymki pomocnicze** — po najechaniu kursorem myszy na dany element, wyświetli się opis tekstowy. Dymki pomocnicze można wyłączyć w rozwijanym menu programu F-Link.

## 11.4 Sygnał RF

Okno zawierające przedstawienie graficzne intensywności zakłóceń pasma radiowego z możliwością wyboru z używanych modułów radiowych. Obecność sygnałów w paśmie sygnalizuje kolor niebieski. Kolor czerwony identyfikuje sygnały komunikacji dla całego systemu (urządzenia przypisane), a zielony wyświetla wybrane urządzenie z listy pozycji **Urządzenie zaznaczone** (patrz ilustracja). Rejestrację monitorowanych zakłóceń (kiedy okno Sygnału RF jest otwarte) można eksportować z menu głównego do pliku z rozszerzeniem FDR, zaś przycisk  można wykorzystać do ponownego importu pliku do wyświetlenia.



## 11.5 Serwis


Przełączanie trybu centrali alarmowej między statusem Rozbrojona (kiedy zmiany ustawień można wprowadzać we wszystkich zakładkach z wyjątkiem zakładki Ustawień) a trybem serwisowym (zmiany można wprowadzać w zakładce Urządzenia, w tym przypisywanie, zmiany ustawień wewnętrznych i usuwanie urządzeń).

## 11.6 Odśwież

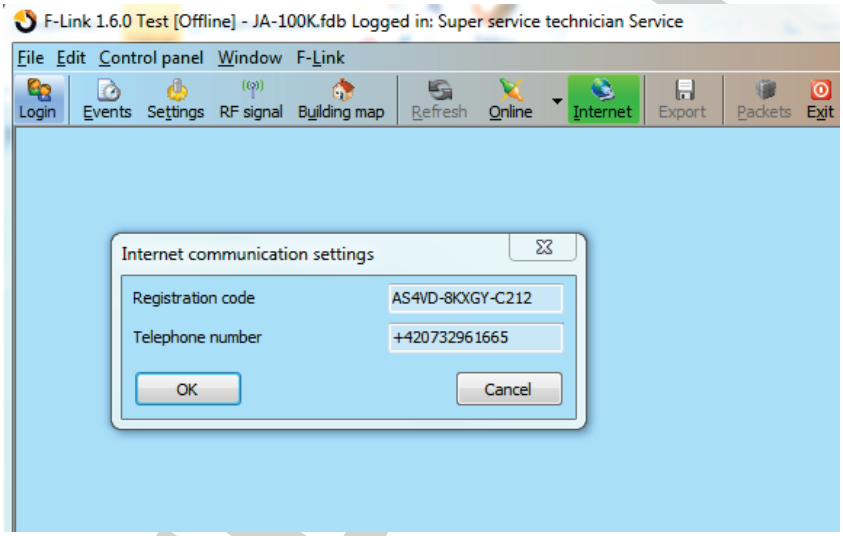

Aktualizacja ustawień wewnętrznych urządzeń po zmianie sprzętu.

## 11.7 Online


Podłączenie do lub odłączenie programu F-Link do/od centrali alarmowej za pomocą przewodu USB. Po podłączeniu program automatycznie znajdzie port, którego centrala alarmowa używa do komunikacji.

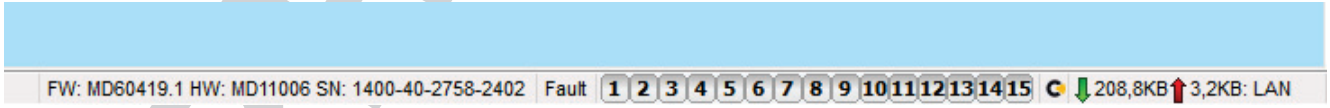
## 11.8 Internet

Zdalne podłączenie do lub odłączenie programu F-Link od centrali alarmowej za pośrednictwem internetu. Warunkiem wstępnym ustanowienia połączenia jest poprawnie wprowadzony kod rejestracji (jest on wprowadzany automatycznie z bazy danych używanej do programowania centrali alarmowej), numer telefonu ewentualnej karty SIM w centrali alarmowej (również wprowadzany z Informacji o instalacji) i komputer podłączony do internetu. Dostęp zdalny można wyłączyć w zakładce Komunikacja / Typ komunikacji = Bez komunikacji zdalnej.



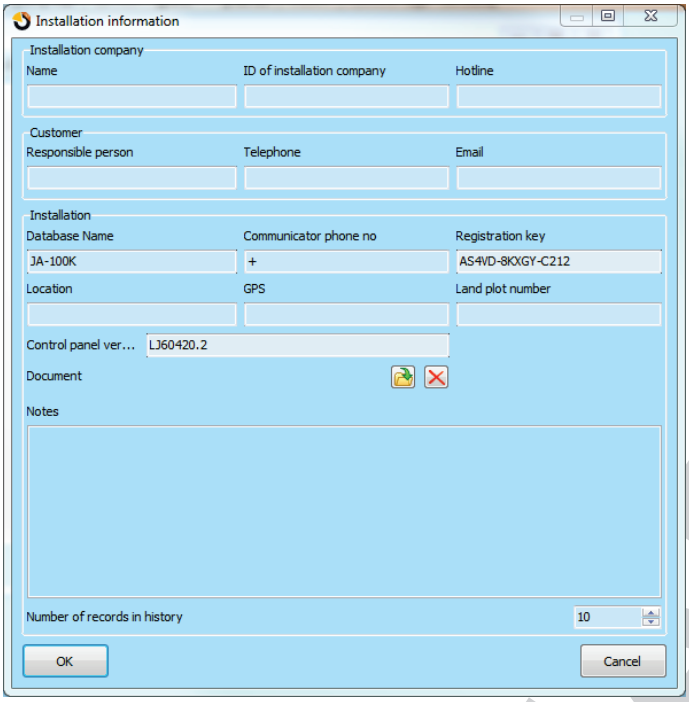

Kliknięcie przycisku Internet wyświetli okno dialogowe z wcześniej wprowadzonymi danymi. Jeśli łączą się Państwo z nowej, „pustej" bazy danych, kod rejestracji i numer telefonu wymaga wprowadzenia. W przypadku wykorzystania komunikatora LA i aktywacji komunikacji Jablotron numeru telefonu nie można wpisać (pole musi pozostać puste). Ustanowienie połączenia trwa zaledwie kilka sekund, ale pobieranie konfiguracji zależy od wielkości systemu i zwykle może zająć 1 do 2 minut.

***Uwaga**: Informacje o sposobie ustanawiania połączenia GPRS / LAN i o ilości wysłanych i otrzymanych danych wyświetlają się w prawym dolnym rogu.*



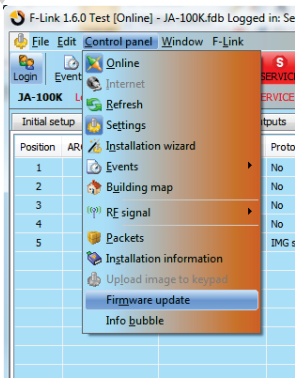

## 11.9 Informacje o instalacji

Okno zawiera pozycje, pozwalające firmie instalacyjnej zapisać ważne dane kontaktowe dotyczące właściciela systemu, całego systemu i ewentualnie dokumentu zewnętrznego dla całego budynku (oferta, rejestr odbioru, faktura itp.). W polu ext. instalator może wprowadzać notatki i informacje uzyskane podczas montażu, które mogą się przydać np. w przypadku rozbudowy systemu.



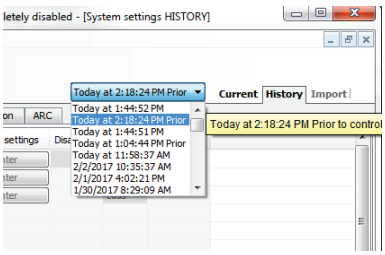

## 11.10 Aktualizacja firmware

Aktualizacja umożliwia zmianę zachowania urządzeń z możliwością aktualizacji (centrala alarmowa, moduły radiowe, klawiatury, czujki itp.) o pakiet firmware (FW), który producent oficjalnie umieszcza na serwerze Jablotron. Oprogramowanie F-Link pobiera je automatycznie z serwera Jablotron (po zapytaniu), jeśli aktywowano opcję Automatyczne aktualizacje w menu F-Link (ustawienie domyślne). Jeśli ta opcja nie jest aktywna, przed aktualizacją F-Link umożliwi ręczne znalezienie plików FWP w komputerze. Więcej informacji znajduje się w rozdziale 13 Firmware update.




## 11.11 Historia ustawień

Centrala alarmowa zapisuje na karcie SD ustawienia wszystkich urządzeń oraz zmiany ich programowania. Rejestruje w historii również zdarzenie „Utworzono konfigurację awaryjną”, zawierające informację o nazwie plików. Obejmuje to konfigurację przed realizacją zmiany, aby zapewnić możliwość przywrócenia wcześniejszych ustawień, przeszukiwania ich i sprawdzenia terminu wprowadzenia zmiany. Aby przeszukać zapisane zmiany konfiguracji, należy otworzyć Zdarzenia z pamięci centrali alarmowej i przeszukać zdarzenia zmiany konfiguracji na podstawie daty i godziny, do porównania z aktualnym programowaniem systemu, załadować je i zajrzeć do zakładki „Historia” w lewym górnym rogu w oknie „Ustawienia systemu”. Zmiany w konfiguracji są zaznaczone niebieską kursywą. Z zapisanego pliku kopii zapasowej można akceptować zmiany, a przyciskiem „Save” zapisywać je w centrali alarmowej, lub po przeszukaniu zmian przywracać aktualne ustawienia, klikając zakładkę „Aktualne”. Wszystkie zmiany konfiguracji zapisują się w folderze o nazwie KOPIA ZAPASOWA, w pliku CFGxxxxx.bak o numerze odpowiadającym kolejności wprowadzonych zmian.




Program F-Link zapisuje (3 do 10 w oknie Informacje o instalacji) historię ustawień od tyłu we własnej bazie danych. Tę historię ustawień program wykorzystuje do ulepszania oprogramowania firmware centrali alarmowej, ponieważ zmiana zawsze powoduje utratę poprzednich ustawień, a tę historię można wykorzystać do ich przywrócenia. Tę samą opcję można wykorzystać w przypadku Resetowania centrali alarmowej do ustawień domyślnych, wymiany karty SD, zmian języka z usuwaniem tekstów, które można w ten sposób przywrócić, lub po prostu w razie przypadkowej zmiany ustawień.

# 12 Resetowanie centrali alarmowej

Ustawienia domyślne centrali alarmowej można przywrócić jedynie w przypadku zaznaczenia opcji „Reset aktywny" w programie F-Link w zakładce Parametry. Jeżeli opcja Reset nie jest aktywna, a Państwo nie znają kodu serwisowego, nie mogą Państwo zresetować centrali alarmowej, a płytę centrali trzeba wysłać do dystrybutora.

Procedura:

1. Włączyć centralę alarmową w tryb serwisowy (nieobowiązkowe)
2. Otworzyć pokrywę centrali alarmowej: Reset wymaga aktywności styku sabotażu. Jeżeli centrala nie jest w trybie serwisowym, aktywuje się alarm.
3. Odłączyć przewód USB od centrali alarmowej.
4. Wyłączyć zasilanie (najłatwiej wyjąć bezpiecznik zasilania) i odłączyć baterię.
5. Podłączyć styki na płytce centrali alarmowej oznaczone RESET (przy pomocy przewodu wchodzącego w skład dostawy).
6. Najpierw podłączyć baterię, a następnie zasilanie centrali alarmowej i poczekać. Zaświeci się zielona, żółta i czerwona kontrolna przy przewodzie (jeśli pozostanie włączona tylko czerwona kontrolka, ustawienie Parametry / Reset nie jest aktywne).
7. Odczekać około 5 sekund, a następnie odłączyć przewód.
8. Wszystkie diody sygnału będą migać na potwierdzenie ukończenia resetu centrali alarmowej. Następnie dojdzie do ponownego uruchomienia napięcia centrali alarmowej i urządzeń MAGISTRALI.
9. W ten sposób centralę alarmową zresetowano do ustawień domyślnych, w tym wyboru języka. Jednakże reset centrali alarmowej nie powoduje usunięcia historii zdarzeń zapisanych na karcie SD. Jeżeli procedury resetowania nie przeprowadzono poprawnie, centrala alarmowa zachowa niezmienione pierwotne ustawienia.

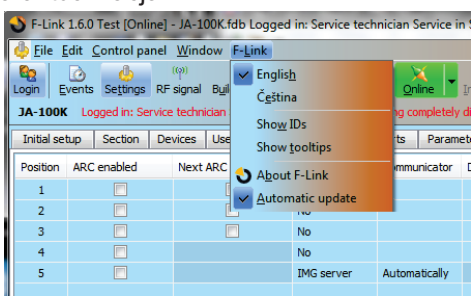
# 13 Aktualizacje firmware

*Centrale alarmowe i niektóre inne urządzenia w systemie JABLOTRON 100 umożliwiają zmianę firmware. Firmware zwykle zmienia się w celu rozbudowy przydatnych parametrów sprzętu i zapewnienia wsparcia produktów nowo wprowadzonych na rynek.*

## 13.1 Ogólne zasady aktualizacji firmware (FW)

1. Aktualizację firmware można przeprowadzić wyłącznie za pomocą komputera z zainstalowanym oprogramowaniem **F-Link**, korzystając z dostępu lokalnego przez przewód USB lub zdalnego, gdzie możliwość zmiany firmware ogranicza się do urządzeń MAGISTRALI oraz do dwukierunkowych urządzeń bezprzewodowych.
2. Firmware (FW) może zmienić użytkownik z upoważnieniem serwisowym.
3. Uprawnieni serwisanci mają dostęp do najnowszej wersji programu F-Link po zalogowaniu w aplikacji MyCOMPANY
   (program F-Link zawiera także pakiet FW). Jeśli program F-Link jest już zainstalowany, a komputer posiada dostęp do internetu, program F-Link po uruchomieniu automatycznie sprawdza obecność dostępnych aktualizacji, a jeśli znajdzie nowszą wersję, zaproponuje jej pobranie wraz z najnowszym pakietem FW.
4. Podłączyć komputer do centrali alarmowej przewodem USB.
5. Uruchomić program **F-Link** z podłączoną centralą alarmową.
6. Przełączyć centralę alarmową w tryb **Serwis**.
7. Uruchomić **Centrala alarmowa/aktualizacja firmware**
   Jeśli w **menu F-Link** jest dostępna **automatyczna aktualizacja** (ustawienie domyślne), wyświetli się lista urządzeń z możliwością aktualizacji. Ten plik wchodzi w skład F-Link w katalogu **F-Link x.x.x/Firmware** i jego aktualność gwarantowana jest jedynie w czasie pobierania programu F-Link.

Lokalizacja parametru Automatyczna aktualizacja:






JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

## 13.2 Aktualizacje FW dla centrali alarmowej i urządzeń połączonych z MAGISTRALĄ.

1. W oknie wyboru Aktualizacja firmware wyświetlają się urządzenia MAGISTRALI i dwukierunkowe urządzenia bezprzewodowe z możliwością aktualizacji. F-Link automatycznie wybiera urządzenia, dla których konieczna jest aktualizacja (ich oprogramowanie jest starsze od oprogramowania FW w pakiecie).
2. F-Link wyświetla także urządzenia bezprzewodowe, które można aktualizować bezprzewodowo (patrz 13.3 FW updates for wireless devices) lub indywidualnie za pomocą dodatkowego przewodu USB podłączonego do komputera.
3. Bardziej szczegółowe informacje na temat istniejących i nowych wersji poszczególnych urządzeń wyświetlają się w dymku pomocniczym po najechaniu kursorem myszy na poszczególne urządzenia.
4. W polach wyboru zaznacza się urządzenia, dla których firmware nigdy nie jest dostępne. Zalecamy ich stałe zaznaczenie. Niektóre pozycje mogą być obowiązkowe, a tym samym niedostępne (wyszarzone) do anulowania aktualizacji.
5. Jeżeli zaznaczona jest aktualizacja centrali alarmowej, wyświetla się możliwość zachowania zmodyfikowanego menu głosowego użytkownika (jeżeli jest nieaktywna, zostanie przywrócona domyślna rejestracja menu głosowego).
6. Kliknąć OK, aby rozpocząć aktualizację firmware dla wszystkich zaznaczonych urządzeń. Wszystkie zmiany zostaną zrealizowane w ciągu kilku minut (zależnie od liczby urządzeń). Na koniec centrala alarmowa uruchomi system ponownie.
7. Po zmianie firmware może dojść do zmiany części kodu rejestracji. Jego zmiana nie wpłynie na możliwość dostępu zdalnego (przy użyciu F-Link) ani na możliwą komunikację centrali alarmowej z usługą JABLOTRON w chmurze, a także serwerem img.jablotron.com.
8. Jeżeli podczas aktualizacji centrali alarmowej F-Link znajdzie uszkodzone pliki na karcie SD, sformatuje ją i po zakończeniu aktualizacji zaproponuje możliwość ponownego importu ustawień oryginalnych.
9. Przeprowadzić kontrolę zgodnie z opisem w rozdziale 13.4 Check after a FW check.

## 13.3 Aktualizacje FW dla urządzeń bezprzewodowych

Najwygodniejszy sposób aktualizacji FW dla wybranych urządzeń bezprzewodowych zakłada wykorzystanie sieci radiowej systemu bez potrzeby złącza kablowego. Jeżeli bezprzewodowa aktualizacja któregokolwiek urządzenia nie jest możliwa (np. ze względu aktualnych, lokalnych warunków radiowych), można tego dokonać przy użyciu przewodu USB.

**Aktualizacja bezprzewodowa przy pomocy modułu radiowego:**

1. Uruchomić F-Link z podłączoną centralą alarmową
2. Otworzyć menu w programie **F-Link: Centrala alarmowa → Aktualizacja firmware**
3. Program oferuje tabelę zawierającą przypisane urządzenia do aktualizacji. Należy sprawdzić, czy wszystkie żądane urządzenia bezprzewodowe są zaznaczone (aktualizacja urządzeń wyszarzonych może być obowiązkowa i wybrana automatycznie w celu zachowania kompatybilności).
4. Bardziej szczegółowe informacje na temat istniejącej i nowych wersji poszczególnych urządzeń wyświetlają się w dymku pomocy po najechaniu kursorem myszy na każde z oferowanych urządzeń.
5. Naciśnięcie przycisku OK powoduje aktualizację wszystkich zaznaczonych urządzeń.
6. Po ukończeniu aktualizacji przeprowadzić kontrolę zgodnie z opisem w rozdziale 13.4 Check after a FW check.

**Aktualizacja przy pomocy przewodu USB:**

1. Otworzyć urządzenie bezprzewodowe do aktualizacji (niepowiązane z AC-160xx).
2. Jeżeli zawiera ono baterie, wyjąć je, jeśli zaś urządzenie jest zasilane przez adapter zewnętrzny, odłączyć go (tylko AC-160xx).
3. Uruchomić program F-Link, otworzyć bazę danych i podłączyć przewód USB do komputer (miniUSB lub microUSB zależnie od używanego urządzenia).
   ***Ostrzeżenie**: Przewody USB nie są dołączane do poszczególnych urządzeń. Zalecamy korzystanie z bezpośredniego połączenia USB z komputerem, ponieważ złącze z HUBEM USB może zmniejszyć niezawodność.*
4. Aktualizacje FW w urządzeniach bezprzewodowych należy realizować kolejno. Nie można tego zrobić jednocześnie przy użyciu kilku przewodów USB.
5. W urządzeniu bezprzewodowym do aktualizacji wejść w tryb do wczytywania nowego firmware. Przestrzegać instrukcji w odpowiednich instrukcjach obsługi.
6. Następnie postępować tak samo, jak w przypadku aktualizacji systemu za pomocą programu **F-Link: Centrala alarmowa → Aktualizacja firmware.**

7. W tabeli wyboru urządzeń wybrać pozycję USB (zwykle w pozycji pierwszej).
8. Bardziej szczegółowe informacje na temat istniejących i nowych wersji poszczególnych urządzeń wyświetlają się w dymku pomocniczym po najechaniu kursorem myszy na poszczególne urządzenia.
9. Naciśnięcie przycisku OK pozwoli zaktualizować wszystkie urządzenia.
10. Po ukończeniu aktualizacji odłączyć przewód USB, ponownie włożyć baterie lub podłączyć zasilanie i złożyć moduł.
11. Przeprowadzić kontrolę zgodnie z opisem w rozdziale 13.4 Check after a FW check.
12. Przejść do aktualizacji kolejnego urządzenia bezprzewodowego.

## 13.4 Kontrola po kontroli FW

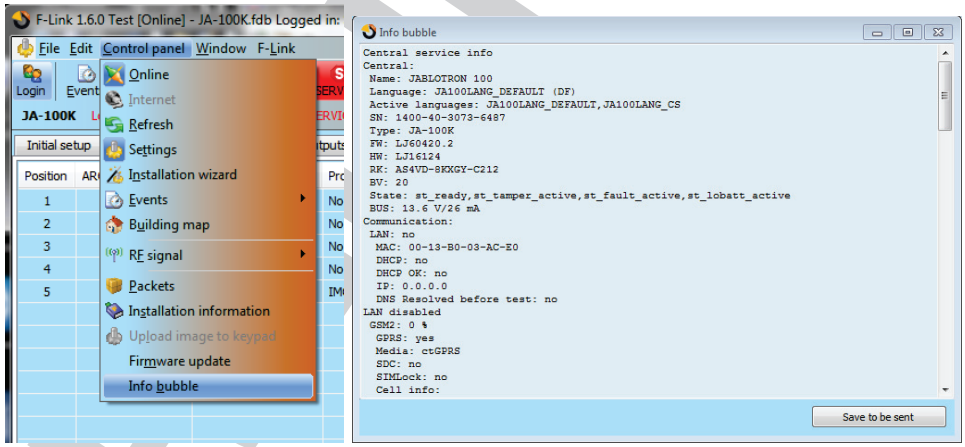
1. Sprawdzić ustawienia wszystkich zmienionych urządzeń i centrali alarmowej w **F-Link, Urządzenia / Ustawienia wewnętrzne**. Zależnie od zakresu zmian wprowadzonych podczas aktualizacji można zachować poprzednie ustawienie lub zresetować je do domyślnych wartości fabrycznych. Po przeprowadzeniu resetu do wartości domyślnych można wybrać spośród poprzednich ustawień za pomocą przycisku Importuj w ustawieniach wewnętrznych poszczególnych urządzeń.
2. Jeżeli w ramach aktualizacji dodano nowe pozycje, będą one posiada ustawienia domyślne. Sprawdzić je i dostosować ustawienia do potrzeb instalacji
3. Sprawdzić ustawienia i sprawdzić działanie zaktualizowanych urządzeń.

## 13.5 Okno Informacji

Otwiera się je z menu głównego **Centrala alarmowa / Okno informacji**, podczas generowania Okna informacji centrala alarmowa kontaktuje się z wszystkimi podłączonymi urządzeniami i urządzeniami bezprzewodowymi, prosząc o aktualne informacje.

Okno informacje oferuje ogólny przegląd danych technicznych całego systemu, w tym centrali alarmowej (numer seryjny, kod rejestracji, wersja FW i sprzętu, napięcie i natężenie MAGISTRALI, zakres ustawień: urządzeń, stref, wyjść PG), używanego komunikatora (GSM: numer telefonu, numer BTS sygnału lub PSTN: status linii telefonicznej), LAN: status, MAC, IP, a także wszystkich urządzeń MAGISTRALI i bezprzewodowych (jedno- i dwukierunkowych): typ urządzeń, identyfikacja wersji FW / sprzętu poszczególnych urządzeń i ich status. Jest dostępne we wszystkich statusach systemu (uzbrojony / rozbrojony / serwis).

Te dane są niezbędne np. do komunikacji z konsultantem technicznym, do czego przeznaczony jest przycisk „Zapisz do wysłania" w prawym dolnym rogu. Plik ma postać pliku spakowanego ZIP i zawiera dane instalacji, w tym część historii zdarzeń (100 kB), ale nie zawiera danych wrażliwych, jak numery telefonów użytkowników ani ich kody dostępu bądź inne dane poufne.





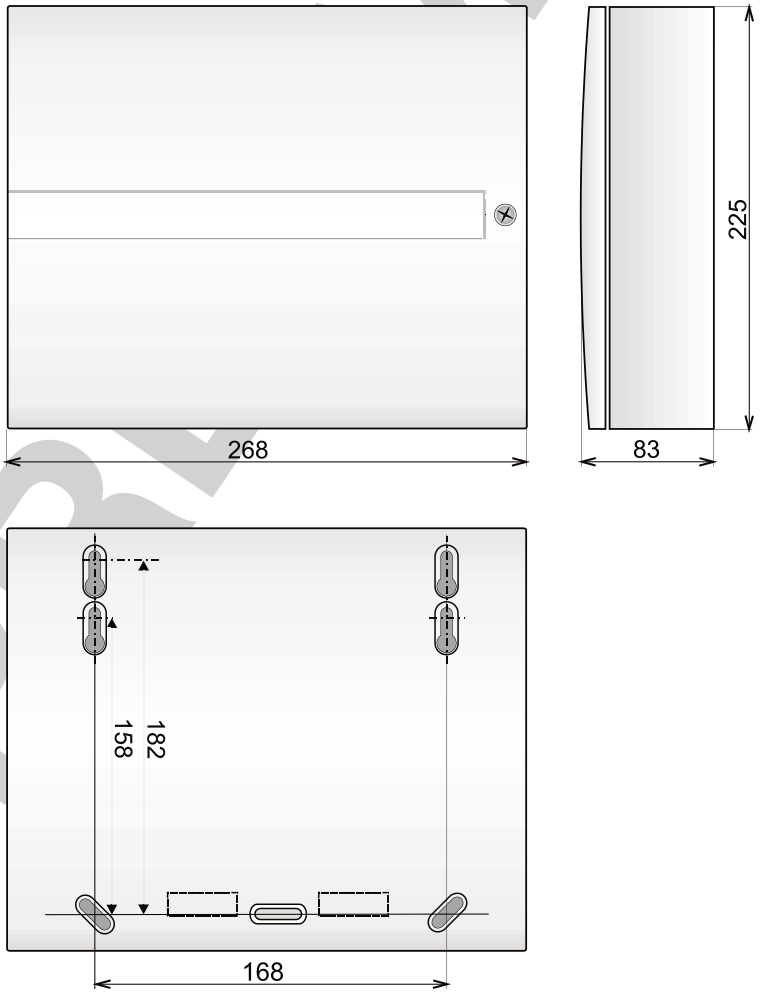

JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

# 14 Informacje uzupełniające

## 14.1 Zestawienie tabelaryczne aktualnego zużycia urządzeń MAGISTRALI

| Urządzenie | Zużycie w trybie awaryjnym (mA) | Zużycie dla wybranych przewodów | Uwaga |
|---|---|---|---|
| **JA-110E** Klawiatura LCD z czytnikiem LCD | 15 | 110 | |
| **JA-11xR** Moduł radiowy do łączenia bezprzewodowego | 25 | 25 | |
| **JA-110A** Syrena wewnętrzna | 5 | 30 | 30 mA podczas alarmu |
| **JA-111A** Syrena zewnętrzna | 5 | 50 | W przypadku awarii zasilania sieciowego bez ładowania baterii, w przeciwnym razie 550 mA zależnie od poziomu naładowania baterii |
| **JA-190X** Moduł komunikacji telefonicznej | 15 | 30 | |
| **JA-190Y** Komunikator GSM | 25 | 220 | Maksymalne natężenie do komunikacji z dostawcą |

## 14.2 Wymiary centrali alarmowej



# 15 Odbiór systemu przez użytkownika

Po zakończeniu instalacji systemu zabezpieczeń zaleca się opracowanie dokumentacji (raportu przekazania systemu, dziennika systemu zabezpieczeń itp.), gdzie znajdą się wszystkie informacje na temat liczby i lokalizacji takich urządzeń, jak czujki, syreny, klawiatury, ich przycisków funkcyjnych i sposobu konfiguracji. Użytkowników systemu należy przeszkolić w zakresie użytkowania systemu zgodnie z następującymi punktami:

1. Sterowanie z klawiatury systemu. Uzbrajanie i rozbrajanie stref (przy pomocy przycisków funkcji lub z menu klawiatury).
2. Należy zapewnić odpowiedni czas na wyjście / wejście, również dla bramy garażowej lub innych tras wejściowych.
3. Wyjaśnić, czym jest uwierzytelnienie, do czego służy, a także opcje jak kody, breloki RFID itp....
4. Częściowe uzbrojenie w domu. Różnice sygnalizacji uzbrojenia częściowego i pełnego.
5. Sterowanie automatyką domową przy pomocy przycisków funkcji i innych funkcji (Panika, Pożar, problemy zdrowotne).
6. Aktywacja alarmu po uzbrojeniu systemu, w tym syreny, test połączenia alarmowego.
7. Wyjaśnienie różnicy między anulowaniem alarmu przez uwierzytelnienie a rozbrojeniem strefy.
8. Sterowanie strefami (zdalnie za pomocą menu głosowego przy użyciu klawiatury telefonu komórkowego).
9. Sterowanie strefami i automatyka domowa (wyjścia PG) za pomocą SMS.
10. Sterowanie przy pomocy aplikacji sieciowej lub mobilnej z tabletów, smartfonów lub strony internetowej.

Należy pamiętać o oferowaniu klientom corocznych kontroli systemu. Dobrze jest okresowo sprawdzać funkcje systemu, nie tylko centrali alarmowej, ale także zainstalowanych urządzeń. Serwisant tworzy raport na temat wyników corocznej kontroli, który może się przydać firmie ubezpieczeniowej.

# 16 Specyfikacja techniczna

| Parametr | JA-100K |
|---|---|
| Typ instalacji | Instalacja stała |
| Znamionowe napięcie / częstotliwość / bezpiecznik centrali alarmowej | ~ 230 V / 50 Hz, bezpiecznik T200 mA 250 V 5 x 20 mm<br>~ 115 V / 60 Hz, bezpiecznik T400 mA 250 V 5 x 20 mm |
| Opcjonalny zakres napięcia prądu zmiennego | ~ 195 V ÷ 250 V<br>~ 110 V ÷ 120 V |
| Moc / natężenie prądu | Maks 23 VA / 0,1 A |
| Klasa ochronności | II. |
| Bateria awaryjna | 12 V; 2.6 Ah maks. (kwasowo-ołowiowa) |
| Niskie napięcie baterii (wskazanie błędu) | ≤11 V |
| Maksymalny czas ładowania baterii | 48 ÷ 72 godziny |
| Napięcie MAGISTRALI / maks. tętnienie napięcia (czerwono-czarne) | 12,0 ÷ 13,8 $V_{DC}$ / ± 100 mV |
| Maks. ciągłe zużycie z MAGISTRALI centrali alarmowej + RJ | 400 mA stale (1000 mA przez 5 minut) |
| @ wsparcie 12-godzinne (2,6 Ah) | LAN OFF (sieć LAN wył.): 125 mA — zużycie dla modułów JA-190X (Y)<br>LAN ON (sieć LAN wł.): 85 mA — zużycie dla modułów JA-190X (Y) |
| Maks. liczba stref | 4 |
| Maks. liczba urządzeń | 32 |
| Maks. liczba użytkowników | 33 |
| Maks. liczba wyjść PG | 4 |
| Złącze alarmowe | MAGISTRALA Jablotron — okablowanie dedykowane<br>Połączenie bezprzewodowe (z JA-111R) — nieokreślone połączenie bezprzewodowe, protokół bezprzewodowy Jablotron |



JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

| | |
|---|---|
| Klasyfikacja systemu alarmowego | Klasa ochronności 2 / klasa środowiskowa II |
| @ zgodnie z normami | EN 50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN50131-10, EN 50136-1, EN 50136-2 |
| @ środowisko | wewnętrzne, ogólne |
| @ temperatura / wilgotność pracy | -10°C do + 40°C, wilgotność względna 75% bez kondensacji |
| @ moc | Typ A — zasilanie podstawowe z naładowaną baterią awaryjną |
| @ historia zdarzeń | około 7 milionów najnowszych zdarzeń, z datą i godziną |
| @ reakcja systemu na utratę komunikacji | Błąd lub sabotaż — zależnie od zadanego profilu<br>@ MAGISTRALA do 10 sekund<br>@ komunikacja bezprzewodowa w ciągu 2 godzin (raport)<br>@ komunikacja bezprzewodowa w ciągu 20 minut, blokuje uzbrajany system |
| @ reakcja na wprowadzenie nieprawidłowego kodu | Po dziesięciu nieudanych próbach wprowadzenia kodu uruchomi się alarm sabotażu. Zgodnie z wybranym profilem zablokuje on wszystkie urządzenia sterowania na 10 minut. |
| @ Klasyfikacja ATS | Obsługiwane klasy ATS: SP2 – SP 5, DP2 – DP3<br>SPT: typ Z<br>Typ eksploatacji: Przekazująca<br>Wbudowana sieć LAN: SP2–SP5 (z protokołem IP)<br>JA-190Y SP2–SP5 (z protokołem IP)<br>JA-190X SP2 (z protokołem Contact ID)<br>LAN + JA-190Y DP2–DP3 (z protokołem IP)<br>LAN + JA-190X DP2 (z protokołem IP / CID) |
| @ Protokoły transmisji ATS | JABLO IP, SIA IP, Contact ID, JABLO SMS |
| @ ochrona ATC przed zastępowaniem i ochrona danych | Protokół JABLOTRON: Szyfrowanie zastrzeżone AES z kluczem min. 128-bitowym<br>Protokół ANSI SIA DC-09.2012 z szyfrowaniem AES 128-bitowym |
| Komunikator LAN | Interfejs ethernetowy CAT 5 (RJ-45) |
| Wymiary (mm) | 268 x 225 x 83 |
| Waga | 1450 g |
| Podstawowe parametry modułu JA-111R | 868,1 MHz, < 25 mW, GFSK < 80 kHz |
| Emisje radiowe | ETSI EN 300 220-2 (moduł R) |
| Kompatybilność elektromagnetyczna | EN 50130-4, EN 55022, ETSI EN 301 489-7, ETSI EN 301 489-3 |
| Bezpieczeństwo elektryczne | EN 60950-1 |
| Warunki pracy | ERC REC 70-03, ERC DEC (98) 20 |
| Organ certyfikujący | TREZOR TEST |



JABLOTRON ALARMS a.s. niniejszym oświadcza, że centrale alarmowe JA-100K spełniają podstawowe wymagania i inne istotne postanowienia dyrektyw nr 2014/53/UE, 2014/35/UE, 2014/30/UE oraz 2011/65/UE. Oryginał Deklaracji zgodności znajduje się na stronie www.jablotron.com.

Uwaga: Choć produkt nie zawiera szkodliwych surowców, nie należy go wrzucać do odpadów komunalnych, ale oddać do punktu odbioru odpadów elektronicznych. Bardziej szczegółowe informacje można uzyskać na stronie www.jablotron.com w sekcji Wsparcia technicznego.