Centrale alarmowe JA-107K i JA-103K systemu bezpieczeństwa JABLOTRON 100+

Centrala alarmowa stanowi podstawowy element systemu alarmowego serii JABLOTRON 100+ i jest przeznaczona do ochrony małych, średnich i dużych obiektów. Spełnia wymogi klasy ochronności 2. Jest zgodna z urządzeniami MAGISTRALI i/lub urządzeniami bezprzewodowymi (jeżeli system wyposażono w moduł radiowy). Zaleca się, by z systemem używać wyłącznie urządzeń JABLOTRON 100+. W przypadku korzystania z urządzeń innych producentów nie gwarantujemy poprawności działania.

Przestroga: System bezpieczeństwa JABLOTRON 100+ może instalować wyłącznie przeszkolony serwisant, posiadający ważny certyfikat wydany przez autoryzowanego dystrybutora.

Instrukcja przeznaczona jest dla przeszkolonych serwisantów.

Niektóre funkcje opisane w niniejszej instrukcji wymagają instalacji dodatkowych komunikatorów:

- ***menu głosowe do zdalnego sterowania, sterowanie dźwiękowe, raporty głosowe, raporty przez połączenie telefoniczne, raporty specjalne, raporty SMS, sterowanie SMS, komunikacja GDPS — komunikator GSM JA-19xY.***

Spis treści

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

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 ładowania 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.).

Moduł dostępowy (klawiatura) — jest podstawowym elementem modułowym klawiatury sterującej, a jego zadaniem jest identyfikacja użytkowników. Najprostsza wersja zawiera jedynie czytnik bezstykowych breloków/kart RFID. Dostępna jest także wersja z klawiaturą i wyświetlaczem LCD. Moduły dostępowe produkowane są w wersji dla MAGISTRALI i bezprzewodowej. Każdy moduł dostępowy zawiera jeden segment kontrolny (z możliwością rozszerzenia do 20 segmentów na urządzenie). Nasz portfel produktów obejmuje także czytnik kart RFID i klawiaturę z wbudowanym czytnikiem kart RFID do użytku na zewnątrz.

Segment kontrolny — jest elementem modułowym klawiatury sterującej do użytku w pomieszczeniach. Segment jest wyposażony w 2 przyciski (lewy = WYŁ., prawy = WŁ.). Instalując żądaną liczbę segmentów w module dostępowym, można utworzyć klawiaturę spełniającą wszystkie żądane funkcje. Segmenty wyraźnie wskazują stan systemu i umożliwiają jego intuicyjną obsługę. Zainstalowane segmenty przejrzyście pokazują użytkownikowi, jakie funkcje zapewnia system (nie są one ukryte wyłącznie w menu) i jakie przypisane prawa posiada użytkownik.

Klawiatura sterująca — składa się z modułu dostępowego oraz segmentów kontrolnych.

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, dotykanie strzeżonego obiektu, wysoka temperatura, ryzyko zamarzania itp.). Aby ograniczyć występowanie fałszywych alarmów, reakcję czujek można ustawić tak, by ich aktywacja wymagała potwierdzenia (konieczna jest ponowna aktywacja tej samej czujki lub potwierdzenie przez inną czujkę).

Weryfikacja wizualna alarmu — urządzenia do weryfikacji zdjęciowej (czujki z kamerą, kamery do weryfikacji zdjęć) są w stanie automatycznie robić i wysyłać zdjęcia lub sekwencje filmowe odpowiadające wydarzeniom w systemie.

Ochrona osób — w przypadku kradzieży, problemu zdrowotnego lub pożaru użytkownik może wezwać pomoc (naciśnięcie przycisku na klawiaturze, wpisanie kodu panika, aktywacja przycisku panika lub użycie bezprzewodowego manipulatora zdalnego).

Antynapadowa kontrola dostępu — służy do aktywacji cichego alarmu wyłącznie w drodze uwierzytelnienia lub sterowania systemem (uzbrajanie, rozbrajanie, sterowanie PG itp.), kiedy użytkownik będzie zagrożony (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 alarm można anulować. Ta funkcja jest przeznaczona dla użytkowników, którzy obawiają się otworzyć drzwi nieznanej osobie mogącej 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 (segment klawiatury, przycisk panika itp.).

Raportowanie zdarzeń — raportowanie wszystkich zdarzeń do centrum odbioru alarmów (SMA) może zapewnić terminową interwencję profesjonalistów. Raporty do SMA wysyłane są przez wbudowany komunikator LAN. Po zamontowaniu komunikatora GSM raporty można także wysyłać bezpośrednio do użytkowników za pomocą wiadomości SMS lub połączeń głosowych.

Raporty specjalne — to wiadomości SMS lub połączenia głosowe. Ich znaczenie można przesłać niezależnie od innych funkcji. Wysłanie raportu może być powiązane z aktywacją urządzenia. W ten sposób można monitorować stan innych urządzeń lub technologii wykazujących błąd itp.

Zdalne sterowanie — upoważnieni użytkownicy mogą wykonać połączenie telefoniczne do systemu i użyć menu głosowego do sterowania stanem uzbrojenia lub jego sprawdzenia. Stanami poszczególnych stref można sterować zdalnie za pomocą określonych poleceń SMS. Polecenia SMS można wykorzystać także do włączania i wyłączania programowalnych wyjść PG. Można je aktywować również przez wykonanie połączenia głosowego (bez nawiązania rozmowy) z uprawnionych numerów telefonu. Istnieje oprogramowanie F-link, za którego pomocą serwisanci mogą zdalnie zarządzać systemem. Istnieje także oprogramowanie o ograniczonych funkcjach, zwane J-Link, przeznaczone dla administratora systemu. Systemem można zdalnie sterować za pośrednictwem serwisu sieciowego pod adresem www.myjablotron.com lub aplikacji mobilnej.

MyJABLOTRON — wyjątkowy serwis zapewniający dostęp online do urządzeń JABLOTRON. Jest przeznaczony zarówno dla użytkowników końcowych, jak i instalatorów. W celu korzystania z serwisu MyJABLOTRON konieczna jest **karta SIM JABLOTRON Security**. Aby uzyskać bardziej szczegółowe informacje na temat rejestracji centrali alarmowych i dostępności serwisu w swoim kraju, prosimy o kontakt z dystrybutorem.

Prawa dostępowe użytkowników — określają poziom dostępu dla upoważnień użytkowników. Można modyfikować prawa dostępowe użytkowników w odniesieniu do części chronionego obiektu i programowalnych wyjść PG, którymi użytkownik może sterować. Użytkownicy potwierdzają swą tożsamość za pomocą breloka RFID lub wprowadzenia kodu z klawiatury. System umożliwia indywidualne ustawienie ograniczenia czasowego, by uniemożliwić dostęp wybranych użytkowników do strzeżonych stref.

Administrator — w systemie można określić (główną) żądaną liczbę administratorów, którzy będą mogli przypisać prawa dostępu zwykłym użytkownikom. Różne strefy budynku mogą mieć różnych użytkowników. W ustawieniu domyślnym w systemie jest tylko jeden administrator główny (nadrzędny), zawsze upoważniony do ustawiania praw dostępowych dla wszystkich użytkowników (kod domyślny 1234).

Serwisant — zawsze może być więcej niż jeden upoważniony serwisant zarządzający systemem (kod domyślny 1010). Za pomocą tego kodu serwisant ma prawo dostosować wszystkie parametry systemu. Dostęp serwisanta może zależeć od zatwierdzenia przez administratora. Specjalnym przypadkiem upoważnienia serwisowego jest serwisant SMA. Taki serwisant może używać swojego kodu do uzyskiwania dostępu do ustawień parametrów komunikacji z Centrum odbioru alarmów (SMA).

F-Link (J-Link) — do programowania systemu niezbędny jest komputer z systemem operacyjnym Windows. Z centralą alarmową można się połączyć z komputera lokalnie za pomocą przewodu USB lub zdalnie z komputera podłączonego do internetu. 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. W tym celu opracowano uproszczoną wersję tego oprogramowania (J-Link), która daje administratorom systemu dostęp do niektórych ustawień (zarządzanie użytkownikami, diagnostyka, ustawienia wydarzeń kalendarzowych, odczyt historii wydarzeń).

Tryb serwisowy — to tryb, w którym można zmienić całą konfigurację systemu. W tryb serwisowy systemu może wejść wyłącznie serwisant (lub serwisant SMA). Można tego dokonać przy użyciu oprogramowania F-Link przy lokalnym lub zdalnym połączeniu centrali alarmowej z komputerem (za pomocą przewodu USB lub internetu). W trybie SERWISOWYM system jest całkowicie nieczynny, wyjścia PG są wyłączone (nie zapewnia strzeżenia ani nie realizuje innych funkcji użytkownika, np. sterowania programowalnymi wyjściami PG). Tryb SERWISOWY sygnalizuje kontrolka systemu klawiatury migająca na żółto (2 x co 2 sekundy).

Tryb konserwacji — jest trybem przeznaczonym przede wszystkim dla Administratora. Umożliwia przeprowadzenie konserwacji (np. wymianę baterii) w strefie (strefach) zgodnie z prawami dostępowymi Administratora. Administrator może przełączyć system w tryb konserwacji za pomocą klawiatury lub oprogramowania J-Link (serwisant może wejść w tryb konserwacji za pomocą oprogramowania F-Link). Tryb konserwacji w jednej strefie nie wpływa na stan ani funkcjonalność innych stref ani stan programowalnych wyjść PG. Serwisant może ograniczyć dostęp Administratora do trybu konserwacji w zakładce Parametry w programie F-Link. Tryb KONSERWACJA sygnalizuje kontrolka systemu klawiatury migająca na zielono (2 x co 2 sekundy) i zgaśnięcie przycisków segmentu w konkretnej strefie.

Tryb dzienny/nocny — centrala alarmowa pozwala ustawić różne zachowanie na czas dnia i nocy. Na przykład różną intensywność podświetlenia klawiatury, aktywację wyjść PG zależnie od dnia/nocy (blokowanie świateł w ciągu dnia) itp. Tryb dzienny/nocny może włączać wybrane urządzenie (np. włącznik zmierzchowy) lub czas wschodu i zachodu słońca zgodnie z kalendarzem astronomicznym. W odniesieniu do tej opcji należy ustawić współrzędne lokalizacji, w której zainstalowano system.

Sterowanie urządzeniami — system ma programowalne wyjścia PG, za których pomocą można WŁĄCZAĆ i WYŁĄCZAĆ różne urządzenia. Wyjścia PG odzwierciedlają logikę zaprogramowaną w systemie, sterującą wymaganymi modułami wyjściowymi (urządzeniami systemu). Wyjściem można sterować za pomocą segmentów klawiatury, aktywacji czujek, manipulatorów zdalnych, wydarzenia w systemie (np. uzbrajanie strefy, aktywacja alarmu itp.), czynności z kalendarza, używając polecenia SMS, połączenia wykonanego przez upoważnionego użytkownika lub aplikacji MyJABLOTRON. Aktywację wyjścia PG można także zablokować stanem strefy, czujką bądź innym wyjściem PG. Aktywację lub dezaktywację wyjścia można zgłosić użytkownikom za pomocą wiadomości SMS lub do serwisu MyJABLOTRON w drodze przesyłu danych (powiadomienia push).

Sterowanie blokadą drzwi — elektryczną blokadę drzwi (połączoną z wyjściem PG) można otworzyć przez przyłożenie breloka lub wprowadzenie kodu z klawiatury. Każdego użytkownika można przypisać do drzwi, do których otwarcia jest uprawniony. 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.

Kalendarz — za pomocą kalendarza można zaprogramować automatyczne czynności z kalendarza, np. strzeżenie (uzbrojenie / uzbrojenie częściowe / rozbrojenie) stref i sterowanie programowalnymi wyjściami PG (aktywacja/dezaktywacja, blokowanie/odblokowanie). Każdą czynność można ustawić na dzień i miesiąc, w którym będzie realizowana. Mogą to być najwyżej 4 razy lub powtarzanie w ustalonych odstępach czasu dla wybranego dnia. W harmonogramie rocznym można ustanowić odstępstwa od harmonogramu tygodniowego (np. święta państwowe, wakacje).

Urządzenia MAGISTRALI — są podłączone do systemu za pomocą przewodu MAGISTRALI (4-żyłowego). 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 się podłącza i które działają bez przypisywania do pozycji (niektóre moduły wyjść PG, kontrolki stanu, izolatory MAGISTRALI itp.).

Urządzenia bezprzewodowe — w celu zapewnienia komunikacji centrala alarmowa musi być wyposażona w moduł radiowy, a urządzenia bezprzewodowe (czujki, klawiatury, syreny itp.) muszą być przypisane do pozycji (adres) w systemie. 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 pokryć obszar większego obiektu, 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. Czujki ustawia się na żądaną reakcję na ich uruchomienie (aktywację). Określa ona, w jaki sposób czujka ma zareagować na aktywację. Czujki pożaru, gazu, zalania lub panika nie należą do grupy czujek włamania.

Komunikator GSM — można go zainstalować w centrali alarmowej w charakterze modułu uzupełniającego, zapewnia połączenie z komórkową siecią telefoniczną i internetem. Dzięki temu system może przekazywać dane do centrum odbioru alarmów (SMA). Komunikator zapewnia zdalny dostęp do centrali alarmowej przy użyciu oprogramowania F-Link (J-Link), raportując zdarzenia użytkownikom i pozwalając na zdalne sterowanie systemem.

Komunikator LAN — wchodzi w skład centrali alarmowej i zapewnia połączenie z internetem. Umożliwia szybki dostęp zdalny za pośrednictwem oprogramowania F-Link i J-Link. Może także przesyłać dane do centrum odbioru alarmów (SMA), wyposażonego w technologię odbierania dla protokołu JABLOTRON. W ustawieniach centrali alarmowej można wybrać, który typ komunikacji będzie podstawowy, a który pomocniczy.

Strefa — system można podzielić na części (strefy), 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, że jest chroniona własną centralą alarmową (prawa dostępowe, raporty, wyświetlanie elementów na klawiaturze, sygnalizacja dźwiękowa, usługa MyJABLOTRON itp.).

Strefa wspólna — to odrębna strefa stanowiąca strefę nadrzędną dla wybranej grupy stref. Po uzbrojeniu ostatniej podstrefy następuje automatyczne uzbrojenie strefy wspólnej. W przypadku rozbrajania pierwszej podstrefy strefa wspólna również zostaje rozbrojona. Ma to na celu zabezpieczenie takich obszarów, jak korytarze, toalety, kuchnie w firmach itp. Nie zalecamy bezpośredniego sterowania strefą wspólną.

Segment wspólny — to funkcja segmentu klawiatury, która pozwala jednocześnie sterować wieloma strefami za pomocą tylko jednego segmentu. Te strefy należy ustawić na odrębne segmenty na konkretnej klawiaturze. Każda klawiatura może mieć najwyżej dwa segmenty o funkcji segmentu wspólnego, a tym samym pozwala sterować dwiema różnymi grupami stref.

Uzbrojenie częściowe — umożliwia regulację 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 stan urządzeń lub usterkę obecną w systemie potwierdza się podczas uzbrajania systemu. Stan 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 błędów systemu użytkownik potwierdza, że zostały one rozpoznane, ale nie zmienia stanu (błąd jest w dalszym ciągu obecny w systemie). Funkcja zależy od opcji umożliwionej parametrem Sposoby uzbrajania.

Blokowanie — blokuje aktywne wejście urządzenia w celu aktywacji wyjścia PG lub aktywacji dowolnej reakcji. Realizuje blokowanie ręczne za pomocą klawiatury LCD, J-Link lub F-Link bądź aplikacji MyJABLOTRON. W

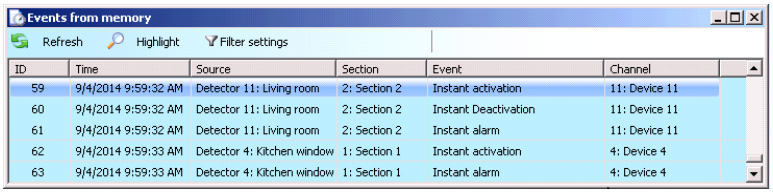
ten sposób można zablokować wejście urządzenia w dowolnej chwili, nie tylko podczas uzbrajania. Funkcja zależy od opcji umożliwionej parametrem Sposoby uzbrajania.

Auto-pominięcie — automatyczne pominięcie reakcji systemu na urządzenie zależnie od opcji. Aktywacja wejścia po 3 aktywacjach lub 3 alarmach (opcjonalnie). Błędy po aktywacji 3. usterki.

Dezaktywacja — ta opcja służy do czasowej, ręcznej dezaktywacji wybranych stref, urządzeń, użytkowników, wyjść programowalnych (PG) lub czynności z kalendarza. Strefy, do której przypisano centralę alarmową, nie można dezaktywować. Dotyczy to kodu serwisowego w pozycji 0 oraz kodu Administratora w pozycji 1. W przypadku urządzeń wyróżniamy Blokowanie (dotyczy tylko aktywacji wejścia) i Dezaktywację, patrz rozdział Dezaktywacja i blokowanie opcji.

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 9.11 Przeszkody uniemożliwiające uzbrojenie systemu.

Historia zdarzeń — system rejestruje w pamięci występujące zdarzenia. Zawartość pamięci można sprawdzić za pomocą oprogramowania F-Link (J-Link), klawiatury LCD lub aplikacji MyJABLOTRON. Początek zdarzenia zwykle rejestruje się jako Aktywacja (status urządzenia, usterka, sabotaż itp.), a koniec zdarzenia jako Dezaktywacja. Stany stref rejestruje się jako Uzbrojone/Rozbrojone, stany alarmów jako Alarm / Wygaśnięcie alarmu, Alarm wyciszony lub Anulowanie alarmu.



Aktywacja i dezaktywacja magnesu

Rozpoczęcie i zakończenie alarmu

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

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 do 4GB (SD / SD-HC). Przed rozpoczęciem użytkowania nowej karty SD należy zresetować centralę alarmową do ustawień domyślnych, patrz rozdział 12Reset of the control panel. Następnie należy przeprowadzić aktualizację oprogramowania, 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. Ten dysk zawiera także katalog J-Link z oprogramowaniem J-Link.exe, które może uruchamiać i wykorzystywać Administrator systemu.

FLEXI_LOG — zawiera 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 zdjęć, wysłanych do centrali alarmowej z urządzeń kamery (np. z czujek ruchu z kamerą). Oba rodzaje plików (txt i jpg) są przechowywane w formie szyfrowanej, a ich treści zwykle nie można wyświetlić za pomocą programów do wyświetlania tekstu i obrazów. Zawartość ZDJĘĆ można wyświetlić jedynie, gdy na komputerze jednocześnie działa także program F-Link (J-Link), a poziom uprawnień Serwis lub Administrator 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. Centrale alarmowe JA-103/107K można ustawić na zachowanie zgodne z zadanym **Profilem systemu**, aby zapewnić zgodność z wszystkimi poniższymi warunkami (profilami):

1. Zadany — 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. Parametrów nie można zmienić.

3. INCERT, klasa 2 — profil zadaje niektóre szczególne parametry systemu (dotyczące centrali alarmowej, klawiatur, syren itp.) zgodnie z wymogami podanej normy dla klasy ochronności 2. Parametrów nie można zmienić.

W odniesieniu do raportowania alarmów, dla klasy bezpieczeństwa 2, centralę alarmową można instalować co najmniej zgodnie z jedną z poniższych konfiguracji:

- minimum jedna syrena z baterią awaryjną (np. JA-111A lub JA-163A) i komunikator LAN* lub komunikator GSM.
- Dwa niezależne komunikatory, na przykład komunikatory LAN* + GSM.

Przestroga: *Należy zagwarantować zasilanie awaryjne dla wszystkich urządzeń sieci LAN zapewniających połączenie z internetem!*

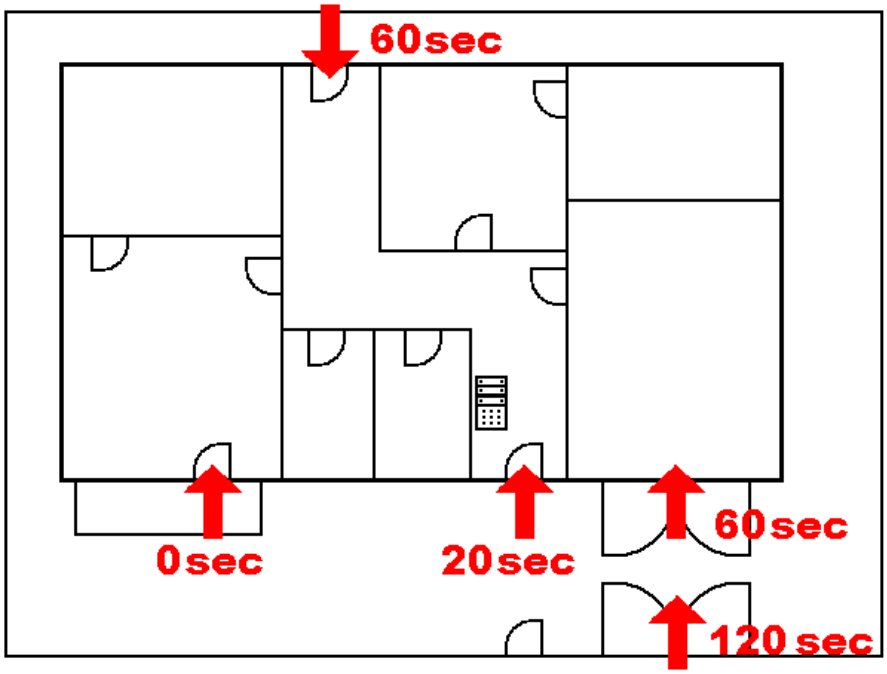
Podczas projektowania systemu należy uwzględnić podział na strefy i zadany czas na wejście, aby można było ustawić definicję stref alarmu opóźnionego. Mogą występować 3 rodzaje stref alarmu opóźnionego (Opóźnienie A, Opóźnienie B i Opóźnienie C), z których każda ma własny zegar odliczający zadany czas na wejście i wyjście.

Przykład: Typowy dom jednorodzinny z garażem o terenie chronionym przez czujki zewnętrzne:

Brama główna lub brama wejściowa, a także drzwi główne są chronione stykiem magnetycznym. Tak samo jest w przypadku bramy garażowej i drzwi tylnych. Cały budynek wraz z terenem i garażem jest chroniony tylko jedną strefą, a klawiatura systemu znajduje się w holu wejściowym*.

*Zaleca się używanie kilku klawiatur, zawsze w pobliżu drzwi wejściowych do chronionego obiektu, oraz zapewnienie, że stanu systemu ani wprowadzonego kodu nie może rozpoznać potencjalny włamywacz.

Pozycja i nazwa czujki	Reakcja	Czas na wejście	Czas na wyjście
1. Styk magnetyczny — Brama główna na zewnątrz	Opóźnienie C	120 sekund	360 sekund
2. Czujka ruchu — Ruch na zewnątrz	Opóźnienie C	120 sekund	360 sekund
3. Styk magnetyczny — Brama garażowa	Opóźnienie B	60 sekund	120 sekund
4. Styk magnetyczny — Drzwi tylne	Opóźnienie B	60 sekund	120 sekund
5. Czujka ruchu — PIR garaż	Następne opóźnienie (Opóźnienie B)	60 sekund	120 sekund
6. Styk magnetyczny — Drzwi główne	Opóźnienie A	20 sekund	60 sekund
7. Czujka ruchu — PIR hol	Następne opóźnienie (Opóźnienie A)	20 sekund	60 sekund
9. Styk magnetyczny — Drzwi balkonowe	Natychmiastowa	0 sekund	0 sekund
9. Czujka ruchu — PIR pokój	Natychmiastowa	0 sekund	0 sekund



Wariant 1:

- Wejście do chronionego obiektu (system jest UZBROJONY) przez drzwi główne uruchamia Opóźnienie A (**20 sekund**), a system zaczyna odliczać czas do rozbrojenia systemu (opóźnienie na wejście).
- Wprowadzenie prawidłowego kodu z klawiatury i naciśnięcie zielonego przycisku na segmencie klawiatury stanowi rozbrojenie systemu. W przypadku braku uwierzytelnienia i rozbrojenia systemu podczas opóźnienia na wejście aktywuje się alarm ze strefy opóźnionej (Opóźnienie A).

Wariant 2:

- Wejście do chronionego obiektu (system jest UZBROJONY) przez drzwi tylne lub bramę garażową uruchamia Opóźnienie B (**60 sekund**), a system zaczyna odliczać czas do rozbrojenia systemu (opóźnienie na wejście).
- Następnie ruch wykryty przez czujki z reakcją Opóźnienie A skraca opóźnienie na wejście zgodnie z Opóźnieniem A (20 sekund) w przypadku, gdy opóźnienie jest krótsze niż Opóźnienie B.
- Wprowadzenie prawidłowego kodu z klawiatury i naciśnięcie zielonego przycisku na segmencie klawiatury stanowi rozbrojenie systemu. W przypadku braku uwierzytelnienia i rozbrojenia systemu podczas opóźnienia na wejście aktywuje się alarm ze strefy opóźnionej, tj. ze strefy, w której czas wygaśnie jako pierwszy (Opóźnienie A, Opóźnienie B).

Wariant 3:

- Wejście do chronionego obiektu (system jest UZBROJONY) przez aktywację czujek zewnętrznych (otwarcie Bramy głównej, bramy wejściowej lub aktywacja zewnętrznego PIR) uruchamia czas na wejście strefy z Opóźnieniem C (**120 sekund**), a system zaczyna odliczać czas do rozbrojenia systemu (opóźnienie na wejście).
- W chwili otwarcia bramy garażowej i aktywacji czujki magnetycznej system zaczyna odliczać czas Opóźnienia B (60 sekund) i skraca czas Opóźnienia C dla strefy już aktywowanej (jeżeli opóźnienie C nie jest krótsze niż Opóźnienie B).
- Przejście przez drzwi główne aktywuje czas Opóźnienia A (20 sekund) i skraca czas na wejście (jeżeli opóźnienie B lub opóźnienie C nie jest krótsze od opóźnienia A).
- Wprowadzenie prawidłowego kodu z klawiatury i naciśnięcie zielonego przycisku na segmencie klawiatury stanowi rozbrojenie systemu. W przypadku braku uwierzytelnienia i rozbrojenia systemu podczas opóźnienia na wejście aktywuje się alarm ze strefy opóźnionej, tj. ze strefy, w której czas wygaśnie jako pierwszy (opóźnienie A, opóźnienie B, opóźnienie C).

1.2 Kody dostępu i ich ustawienia domyślne

Aby można obsługiwać system (uzbrajanie, rozbrajanie lub sprawdzanie stanu wybranej strefy lub urządzenia), konieczne jest uwierzytelnienie przy pomocy prawidłowego kodu (4, 6 lub 8 cyfr) lub przyłożenia 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.

Upoważnienie do sterowania systemem za pomocą klawiatury lub do korzystania z oprogramowania F-Link (J-Link), aplikacji MyJABLOTRON lub menu głosowego należy potwierdzić przez wprowadzenie kodu numerycznego. Kod można wprowadzić z prefiksem lub bez prefiksu (ustawienie domyślne).

Wprowadzić kod bez prefiksu w poniższym formacie:

CCCC

gdzie: **cccc** jest kodem 4-, 6- lub 8-cyfrowym, dopuszczone są kody 0000 to 99999999

Centralę alarmową dostarczamy z dwoma kodami domyślnymi:

Kody domyślne bez prefiksu	4-cyfrowy	6-cyfrowy	8-cyfrowy
Serwis	**1010**	**101010**	**10101010**
Administrator	**1234**	**123456**	**12345678**

*Domyślne kody zostają wprowadzone automatycznie przez program F-Link, dzięki czemu program nie żąda go od chwili pierwszej aktywacji do zmiany kodu. Jednakże ze względów bezpieczeństwa tuż po zakończeniu instalacji należy zmienić wszystkie kody domyślne. Jeżeli oba kody nie zostaną zmienione, po opuszczeniu trybu serwisowego zostanie wysłana wiadomość SMS na numer telefonu serwisowego ze zgłoszeniem **„Ostrzeżenie, kody domyślne, Strefa 1”** (można to anulować w zakładce Parametry „Ostrzeżenie o kodach domyślnych”).*

W przypadku systemów z większą liczbą użytkowników prefiks może być aktywny. Przy aktywnym prefiksie użytkownicy mogą samodzielnie zmienić kody za pomocą klawiatury LCD. Prefiks można aktywować w zakładce Konfiguracja początkowa w programie F-Link.

Wprowadzić kod z prefiksem w poniższym formacie:

ppp*cccc

gdzie: **ppp** to numer sekwencyjny (pozycja **0 do 600**) użytkownika (zwany prefiksem)

***** to separator (klawisz *)

cccc jest kodem 4-, 6- lub 8-cyfrowym, dopuszczone są kody 0000 to 99999999

W takim przypadku kody serwisowe lub Administratora ustawia się następująco:

Kody domyślne z prefiksem	4-cyfrowy	6-cyfrowy	8-cyfrowy
Serwis	**0*1010**	**0*101010**	**0*10101010**
Administrator	**1*1234**	**1*123456**	**1*12345678**

Przestroga: ***Kod serwisowy*** *zawsze musi się zaczynać od prefiksu* ***0****.*
Kod administratora *zawsze musi się zaczynać od prefiksu* ***1.***

Ostrzeżenie: *Kiedy prefiks jest nieaktywny, kody zawsze ulegną zmianie na wartości domyślne, a wszystkie inne kody zostaną wykasowane (pozostaną wszystkie karty / breloki RFID zapewniające dostęp). Kiedy prefiks jest aktywny, wszystkie kody i karty/breloki pozostaną uzbrojone, a dodane zostaną tylko prefiksy.*

1.2.1 Zmiana kodów dostępu

Kiedy opcja „Kod z prefiksem" jest aktywna, centrala alarmowa umożliwia dowolną kombinację cyfr w kodzie 4–8-cyfrowym dla każdego użytkownika (może być ten sam kod o odmiennym prefiksie). Każdy użytkownik z uprawnieniem „Użytkownik" i zaznaczonym parametrem „Dopuszczona zmiana kodu" posiada opcję edycji własnego kodu.

Kody dostępu można zmienić za pomocą:

- klawiatury LCD (komputer musi być odłączony od centrali alarmowej, bez połączenia zdalnego lub lokalnego);
- oprogramowania J-Link (dla użytkownika) w module dysku centrali alarmowej (który pojawia się po podłączeniu przewodu USB) lub oprogramowania F-Link (dla serwisanta) do pobrania z MyCOMPANY;
- aplikacji mobilnej MyJABLOTRON (od wersji 3.5).

Kiedy opcja „Kod z prefiksem" jest nieaktywna, centrala alarmowa umożliwia kombinację kodu 4–8-cyfrowego dla każdego użytkownika, ale ogranicza wykorzystanie kodu o tej samej wartości, którą już wykorzystano w systemie, dla innego użytkownika. Wyłącznie Administratorzy systemu ponoszą pełną odpowiedzialność za edycję istniejących kodów użytkownika i przypisywanie nowych kodów.

Kody dostępu może zmienić jedynie Administrator za pomocą:

- klawiatury LCD (komputer musi być odłączony od centrali alarmowej, bez połączenia zdalnego lub lokalnego);
- oprogramowania J-Link (administrator) dostępnego w module dysku centrali alarmowej (pojawia się po podłączeniu przewodu USB) lub oprogramowania F-Link (serwisant), które można pobrać z MyCOMPANY;
- aplikacji mobilnej MyJABLOTRON (wersja 3.5 i wyższa).

1.2.2 Zabezpieczające kody dostępu i urządzenia RFID

Centrala alarmowa pozwala przypisać każdemu użytkownikowi jeden kod 4-, 6- lub 8-cyfrowy i do dwóch breloków RFID w celu uwierzytelnienia. Uwierzytelnienie jest konieczne w przypadku obsługi systemu za pomocą klawiatury, menu głosowego, komputera, aplikacji sieciowej lub mobilnej. Poziom bezpieczeństwa jest odpowiedni i mogą go reprezentować liczby.

Obliczenie kombinacji kodu dla 1 użytkownika podano na poniższych przykładach:

Parametry centrali alarmowej	4-cyfrowy	6-cyfrowy	8-cyfrowy
„Kod z prefiksem" aktywny	**= 10^4 =** (10 000)	**= 10^6 =** (1 000 000)	**= 10^8 =** (100 000 000)
„**Kod z prefiksem**" oraz „**Antynapadowa kontrola dostępu**" wyłączone	**= 10^4** – (liczba użytkowników w systemie – 1)	**= 10^6** – (liczba użytkowników w systemie – 1)	**= 10^8** – (liczba użytkowników w systemie – 1)

„**Kod z prefiksem**" wyłączony, „**Antynapadowa kontrola dostępu**" włączona	≤10^4 - ((liczba użytkowników w systemie – 1) * 3)	≤10^6 - ((liczba użytkowników w systemie – 1) * 3)	≤10^8 - ((liczba użytkowników w systemie – 1) * 3)
Używanie **karty RFID** tylko o 14 znakach (6 stałych + 8 zmiennych)	= 10^8 = (100 000 000)	= 10^8 = (100 000 000)	= 10^8 = (100 000 000)
„**Kod z prefiksem**" i „**Potwierdzenie karty kodem**" włączone	= (10^8 * 10^4) = 10^{12} = (1 000 000 000 000)	= (10^8 * 10^6) = 10^{14} = (100 000 000 000 000)	= (10^8 * 10^8) = 10^{16} = (1 000 000 000 000 000)
„**Kod z prefiksem**" wyłączone i „**Potwierdzenie karty kodem**" włączone	= 10^8 * (10^4 – (liczba użytkowników w systemie – 1))	= 10^8 * (10^6 – (liczba użytkowników w systemie – 1))	= 10^8 * (10^8 – (liczba użytkowników w systemie – 1))

Przykład: W przypadku standardowego 4-cyfrowego kodu dostępu z włączoną funkcją „Kody z prefiksem" liczba kombinacji kodu dla każdego użytkownika sięga 10^4 (10 000). Liczbę kombinacji zmniejsza się przez wyłączenie prefiksów i zwiększenie liczby użytkowników. Zależy także od parametru „Antynapadowa kontrola dostępu", ponieważ dla każdego użytkownika dodaje jeszcze jeden kod.

Rozwiązanie pozwalające zmniejszyć ryzyko złamania kodu może być następujące:
- wykorzystanie kodu 6- lub 8-cyfrowego;
- wybór wyższego poziomu uwierzytelniania, jak „Potwierdzenie karty kodem" lub „Podwójne uwierzytelnianie";
- wykorzystanie bezstykowych kart/breloków RFID (JA-19xJ).

Centrala alarmowa liczy próby wprowadzenia nieprawidłowego kodu, a po **10. próbie** system uruchomi zdarzenie sabotażu „Próba złamania kodu" 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.

1.2.3 Regularna kontrola systemu (konserwacja)

Cały system bezpieczeństwa 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 błędy do centrali alarmowej, która powiadomi o takim stanie w zależności od wprowadzonych ustawień. 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 każdym okresowym teście transmisji. System zgłasza niski poziom baterii z każdego przypisanego urządzenia od chwili jego pojawienia się do czasu wymiany na klawiaturze LCD, ewentualnie również za pomocą zadanego raportu SMS. Wymiany baterii może dokonać serwisant w trybie serwisowym lub administrator w trybie konserwacji. Po wyjęciu baterii należy odczekać kilka chwil (co najmniej 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	Raz w roku
	Sprawdzenie baterii (urządzenia MAGISTRALI i urządzenia 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	Raz w roku
	Sprawdzić każdy przycisk, segmenty 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
	Sprawdzić baterie i baterie awaryjne, pomiar, stan fizyczny, pomiar napięcia każdej baterii itp.	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

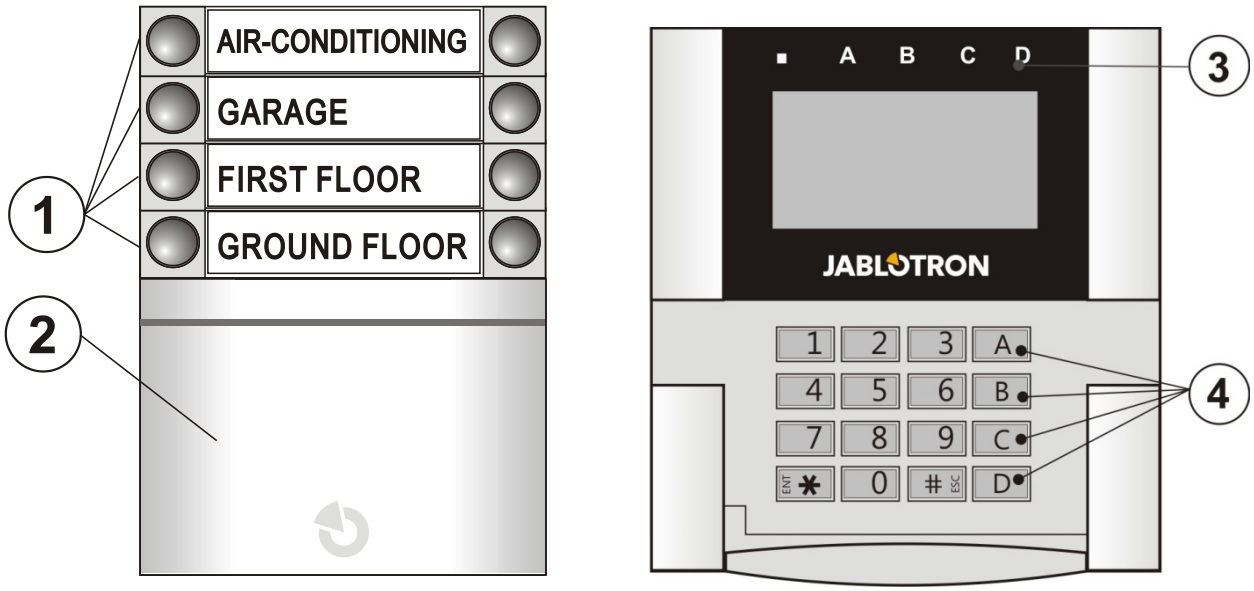
Wszystkie czynności są zalecane przez producenta, ale nie mają pierwszeństwa przed przepisami lokalnymi.

2 Rozmiar systemu

Zasięg systemu można ustawić zależnie od rozmiaru obiektu i potrzeb użytkownika.

2.1 Rozmiar zewnętrzny

Rozmiar zewnętrzny systemu, postrzegany przez użytkowników, można określić za pomocą zespołu modułu dostępowego (klawiatury segmentowej). Klawiatury JA-110E/JA-150E mają 4 przyciski funkcji i nie można tego zmienić. Można je ustawić na sterowanie strefami i wyjściami PG.



1 – Segmenty kontrolne; 2 – Moduł dostępowy; 3 – Kontrolki stref; 4 – Przyciski funkcji

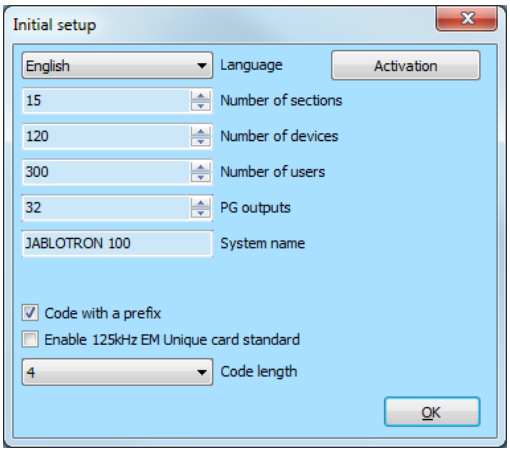
Klawiatura może mieć najwyżej 20 **segmentów kontrolnych**. Każdy segment ma dwa przyciski (WYŁ. z lewej i WŁ. z prawej). Segment służy do sterowania strefą (Uzbrojenie/Rozbrojenie) bądź urządzeniami lub wzywania pomocy. Segmentu można używać także do sygnalizacji stanu strefy lub wyjścia PG (może sygnalizować stan aktywny zarówno standardowo za pomocą czerwonej diody, jak i zielonej diody — funkcja segmentu „Sygnalizacja odwrócona"). Na przykład na klawiaturze można monitorować i sygnalizować aktywację/dezaktywację segmentu czujki magnetycznej zamontowanej na drzwiach w przypadku ich otwarcia lub zamknięcia. Można go ustawić jako „Segment wspólny" do jednoczesnego sterowania większą liczbą stref.

Moduł dostępowy weryfikuje uwierzytelnianie użytkowników. Sposób uwierzytelniania określa się przez wybór modułu (czytnik kart/breloków RFID, klawiatura + czytnik RFID, klawiatura z wyświetlaczem LCD + czytnik RFID). Moduł umożliwia także otwarcie zamka w drzwiach przez przyłożenie karty/breloka (wprowadzenie kodu). Moduły są dostępne w wersji bezprzewodowej i MAGISTRALI. Funkcje odnoszą się do obu rodzajów.

Konfigurację klawiatury sterowania opisano w rozdziale 10.5.1 Keypad configuration.

2.2 Rozmiar wewnętrzny (zasięg systemu)

Centralę alarmową można podzielić na 15 stref (części z możliwością niezależnej regulacji). Każde urządzenie ma własny adres (klawiatury, czujki, syreny) i wymaga przypisania do strefy. Każdy użytkownik może posiadać przypisane uprawnienie do uzyskiwania dostępu wyłącznie do wymaganych stref. Liczbę stref ustawia się przy pomocy oprogramowania F-Link, zakładka Konfiguracja wstępna. Zapewnia to lepszą organizację programowania. Ich ilość można zwiększyć lub zmniejszyć (jeżeli nie wykonano połączeń mogących uniemożliwić obniżenie liczby stref).

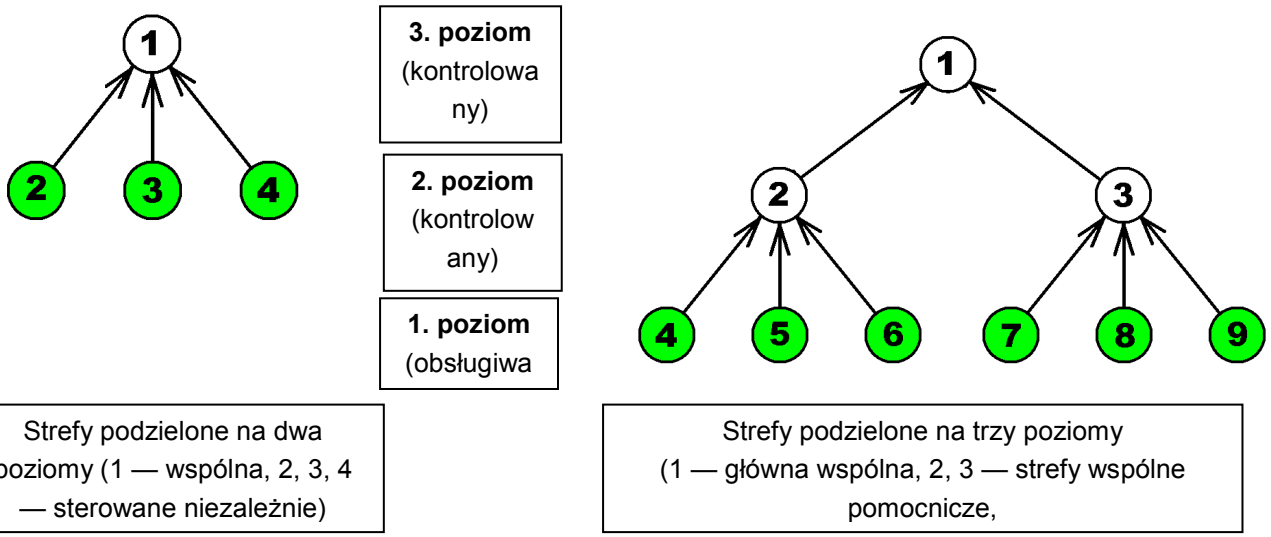


Liczbę urządzeń, stref, użytkowników i wyjść programowalnych ustawia się przy pomocy oprogramowania F-Link. Można utworzyć system zarówno dla małego mieszkania o jednej strefie i z kilkoma urządzeniami, jak i dużego budynku, korzystając z wszystkich funkcji systemu JABLOTRON 100+ dla stref mających niezależne sterowanie. Strefę można powiązać z innymi strefami, aby móc jednocześnie sterować nimi i ich stanami.

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

2.2.1 Konfiguracja i podział

Centrala alarmowa systemu bezpieczeństwa JA-103K jest przeznaczona do ochrony niewielkich obiektów. W przypadku obiektów średniej wielkości i dużych lepiej sprawdzi się system JA-107K. Dzięki swemu zasięgowi, wymiarom i liczbie stref oferuje dużą zmienność, dopasowując się do danej instalacji. Strefa jest częścią systemu, do którego przypisano urządzenia powiązane z chronionym obszarem. Niewielkie obiekty charakteryzują się jedną strefę podstawową (mieszkanie, mały dom jednorodzinny) i w takim przypadku wszystkie urządzenia przypisuje się do tej samej strefy. Systemy średniej wielkości mogą składać się z kilku stref (na przykład mieszkania w blokach, obiekty firmowe), a także własną strefę wspólną 2. poziomu (wspólny hol, piwnice itp.). Większe obiekty mogą obejmować znacznie więcej stref (biura), strefy wspólne 2. poziomu (na przykład w budynkach wielopiętrowych) i powierzchnie wspólne, jak recepcja lub hol wejściowy w charakterze strefy wspólnej 3. poziomu (patrz zdjęcie). Dla eksploatacji takich systemów szczególnie ważna jest konfiguracja uwierzytelniania użytkowników na najniższy poziom sterowania strefami, do których ich przypisano. Nie dla poziomu 2. i 3. stref wspólnych. Kiedy wszystkie strefy przypisane do 2. lub 3. poziomu strefy wspólnej są uzbrojone, każda strefa wspólna jest uzbrajana i rozbrajana automatycznie, jeżeli rozbrojono co najmniej jedną ze stref podstawowych. Użytkownicy mogą sterować wyłącznie strefami 1. poziomu. Patrz poniższy rysunek:



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

Strefy podzielone na trzy poziomy (1 — główna wspólna, 2, 3 — strefy wspólne pomocnicze,

W odniesieniu do wyższych poziomów powierzchni wspólnych (poziom 2. i 3.) zaleca się stosowanie klawiatur o konkretnej liczbie segmentów równej liczbie stosowanych stref celem określenia, która strefa jest uzbrojona/rozbrojona po wejściu do chronionych miejsc.

W przypadku klawiatur poziomu 1. całkowicie wystarczy zapewnienie segmentów kontrolnych przypisanych do konkretnych stref.

3 Rodzaje centrali alarmowych, parametry użytkowe

Funkcja/Typ	JA-103K	JA-107K	Uwaga
Maksymalna liczba urządzeń	50	230	JA-107K Maks. 120 urządzeń bezprzewodowych w pozycjach 1–120, maks. 60 urządzeń na 1 zacisk MAGISTRALI
Maksymalna liczba użytkowników	50	600	
Maksymalna liczba niezależnych stref (części)	8	15	
Maksymalna liczba wyjść programowalnych	32	128	W odniesieniu do transmisji bezprzewodowej można wykorzystać tylko PG 1–32.
Komunikator GSM/GPRS	Nie	Nie	Uzupełniający moduł GSM JA-19xY
Komunikator IP LAN (Ethernet)	Tak	Tak	
Maksymalna liczba modułów radiowych	3	3	
Raporty SMS	Do 8 użytkowników	Do 50 użytkowników	5 raportów na 1 zdarzenie
Raporty głosowe	Do 8 użytkowników	Do 15 użytkowników	5 raportów na 1 zdarzenie
Zalecana bateria awaryjna 12 V	2,6 Ah	7–18 Ah	
Maksymalne możliwe krótkoterminowe zużycie energii	1000 mA	2000 mA stałe 3000 mA przez 60 min (maks. 2000 mA dla jednej MAGISTRALI)	
Maksymalne ciągłe zużycie energii dla zasilania awaryjnego 12 godzin	JA-103K — bateria 2,6 Ah		JA-107K — bateria 18 Ah	
	Bez komunikatora GSM	LAN — WYŁ. — 115 mA LAN — WŁ. — 88 mA	Bez komunikatora GSM	LAN — WYŁ. — 1135 mA LAN — WŁ. — 1107 mA
	Z komunikatorem GSM	LAN — WYŁ. — 80 mA LAN — WŁ. — 53 mA	Z komunikatorem GSM	LAN — WYŁ. — 1100 mA LAN — WŁ. — 1072 mA
Zaciski końcowe MAGISTRALI	MAGISTRALA 1 + złącze 4-pinowe (I-BUS) dla modułu radiowego	MAGISTRALA 1, MAGISTRALA 2 + złącze 4-pinowe (MAGISTRALA 3) dla modułu radiowego lub rozdzielacz JA-110Z-D	Zaciski JA-107K są izolowane, tj. zwarcie jednego odgałęzienia nie wpływa na drugie odgałęzienie.
Maksymalna długość przewodu MAGISTRALI	500 m	3 x 500 m	Można przedłużyć za pomocą modułów JA-110T lub JA-120Z.

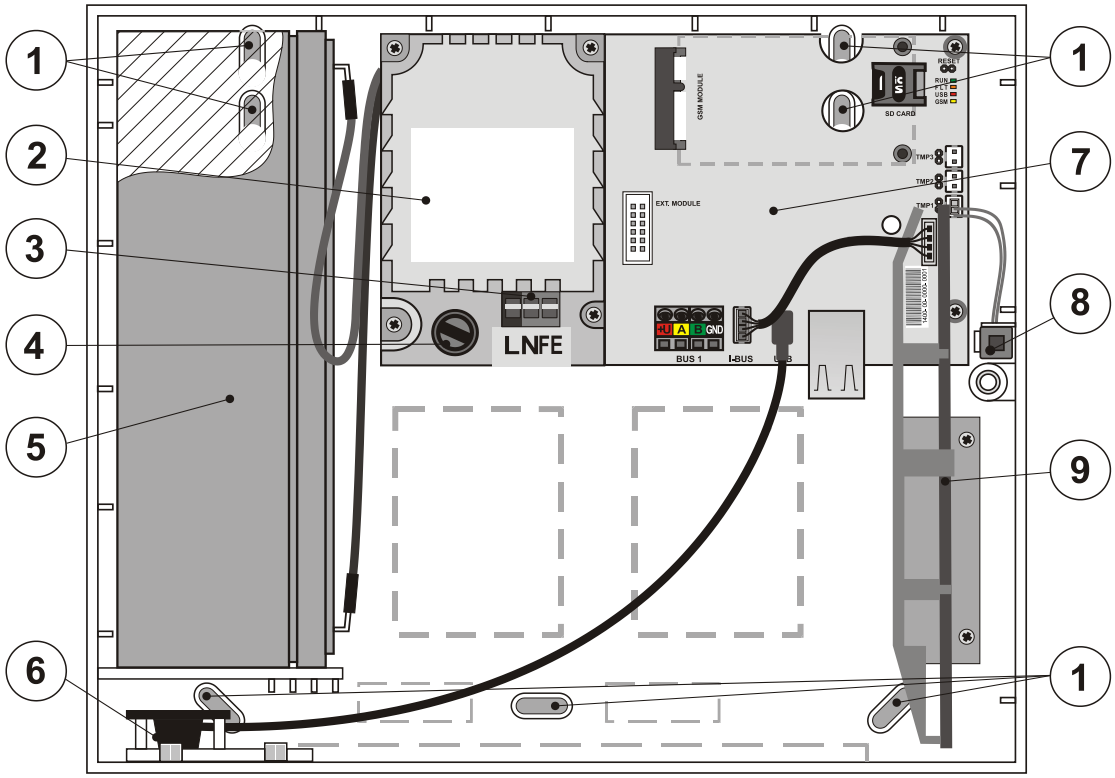
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

3.1 Opis centrali alarmowej JA-103K

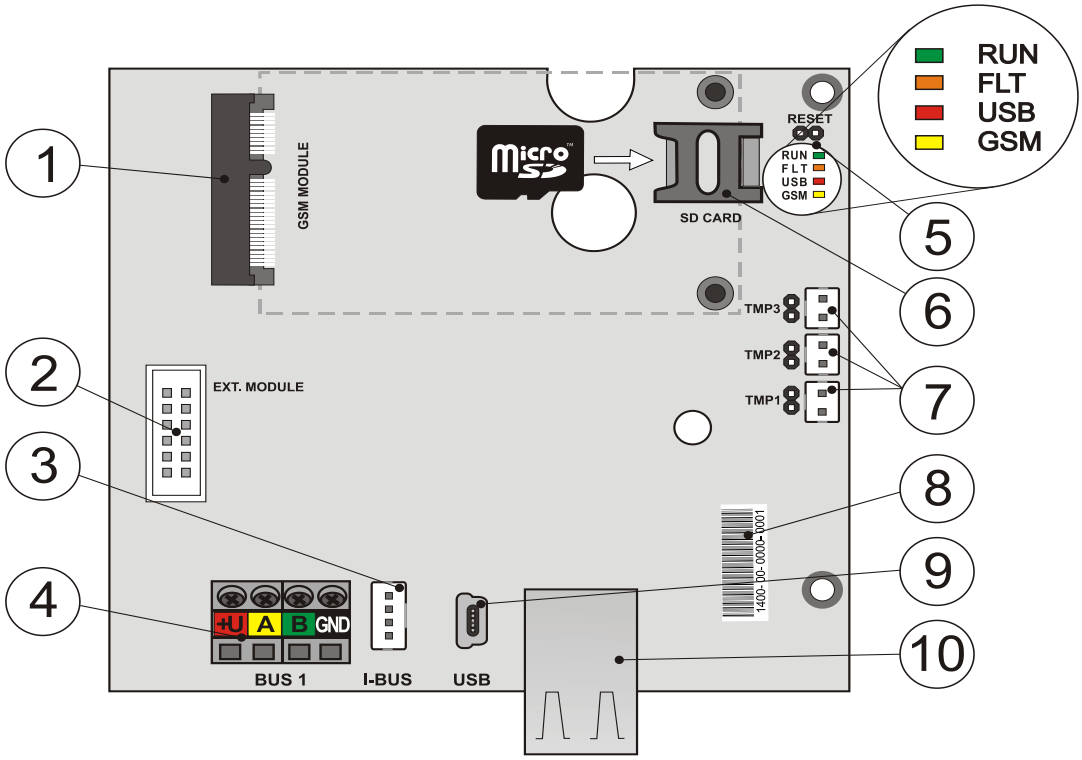
Centrala alarmowa JA-103K jest przeznaczona do małych **systemów MAGISTRALI** (ograniczonych przez moc zasilania) oraz **średnich systemów** z komunikacją bezprzewodową. Centralę alarmową wyposażono w komunikator LAN, który można połączyć z internetem, i który umożliwia wysyłanie danych do serwerów (zdjęcia wykonane przez urządzenia do weryfikacji zdjęciowej), usług JABLOTRON w chmurze lub do serwera agencji ochrony po otrzymaniu wyposażenia technicznego na potrzeby takich danych. Po połączeniu z internetem za pośrednictwem komunikatora LAN dostęp zdalny jest możliwy także przy użyciu oprogramowania F-Link (J-Link).

Centralę alarmową można rozbudować o dodatkowy komunikator:

JA-19xY — komunikator GSM do komunikacji GSM/GPRS. Umożliwia taki sam sposób komunikacji i usługi jak komunikator LAN.



1 — Otwory do montażu na ścianie; 2 — Moduł zasilający; 3 — Zaciski do zasilania sieciowego; 4 — Bezpiecznik do zasilania sieciowego; 5 — Bateria awaryjna; 6 — Złączka USB do podłączenia do komputera; 7 — Płytka drukowana centrali alarmowej; 8 — Styk sabotażu w obudowie; 9 — Uchwyt modułu radiowego JA-11xR



1 — Złączka komunikatora GSM; 2 — Złączka do dodatkowych modułów; 3 — Listwa zaciskowa MAGISTRALI do wewnętrznego modułu radiowego JA-11xR; 4 — Zaciski MAGISTRALI; 5 — Kontrolki i kabel złączowy RESETOWANIA; 6 — Uchwyt karty MicroSD; 7 — Złączki styków sabotażu w obudowie, 8 — Kod produktu; 9 — Złączka MiniUSB; 10 — Złączka LAN

Części centrali alarmowej JA-103K (wymienne) są następujące:

- Karta MicroSD

W celu poszerzenia opcji centrali alarmowej należy wykorzystać:

- Moduł radiowy JA-11xR
- Komunikator GSM JA-19xY

Do elementów wyposażenia dodatkowego centrali alarmowej należą:

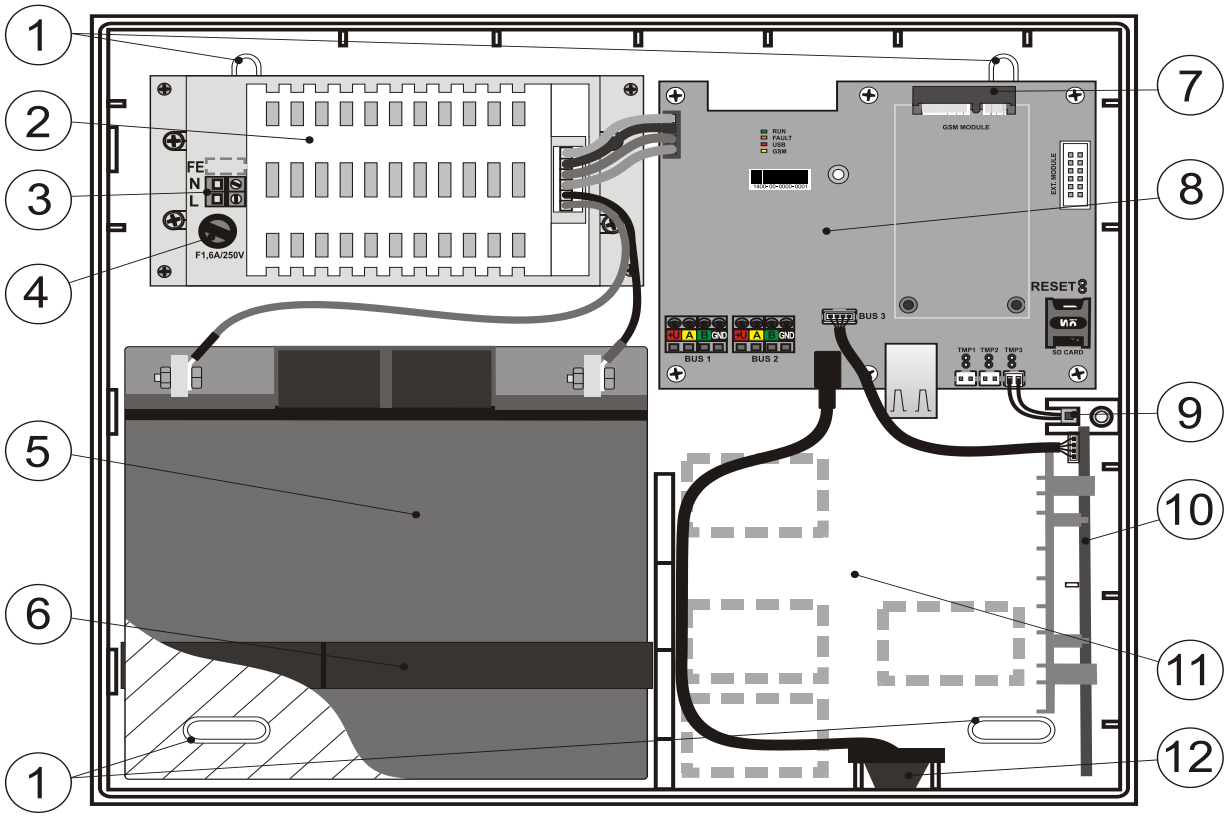
- 1 szt. przewód USB (180 cm)
- 1 szt. przewód łączący do modułu radiowego JA-11xR
- 1 szt. przedłużacz USB (20 cm) zainstalowany w centrali alarmowej
- 1 szt. bezpiecznik T1,6 A, 250 V
- 4 szt. złącza (do podłączania wtyków złącza)
- 6 szt. naklejki ostrzegawcze
- 4 szt. elementy mocujące 8 mm
- 4 szt. wkręty 40 mm
- 3 szt. opaski 100 mm
- Szablon do nawiercania A4
- Instrukcja instalacji CZ/EN (wersja skrócona)

3.2 Opis centrali alarmowej JA-107K

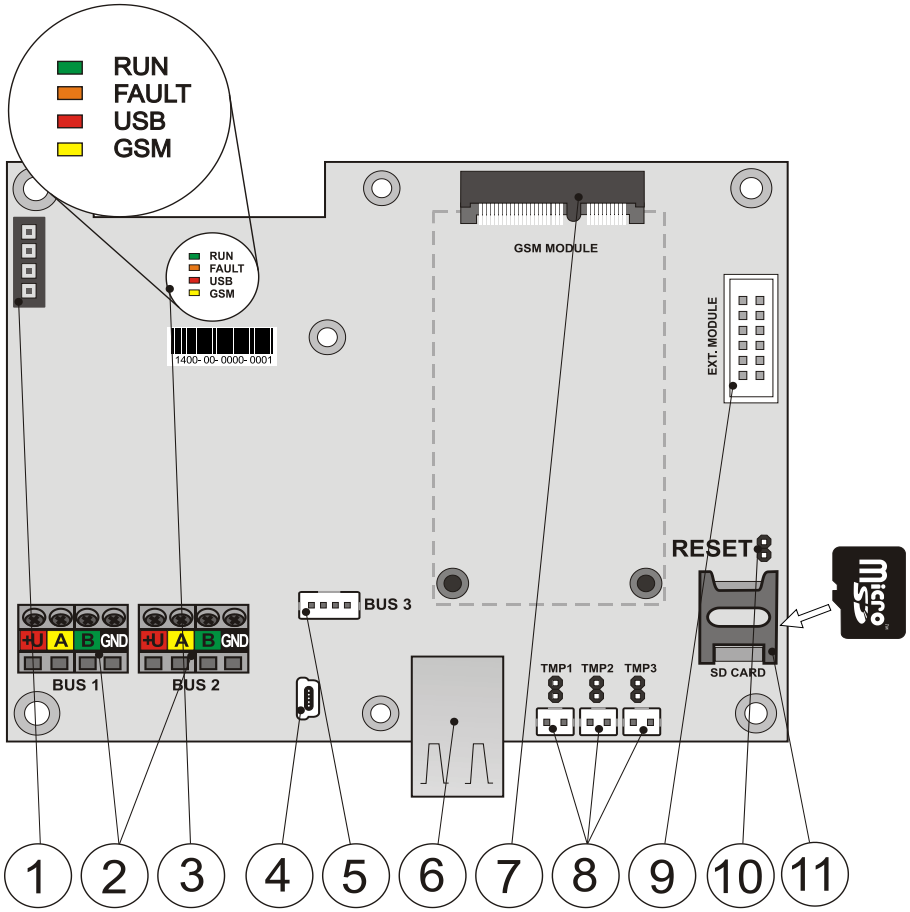
Centrala alarmowa JA-107K jest przeznaczona do **instalacji średnich i dużych w systemach MAGISTRALI i bezprzewodowych.** Centralę alarmową wyposażono w komunikator LAN, który można połączyć z internetem i który umożliwia wysyłanie danych do serwerów (zdjęcia wykonane przez urządzenia do weryfikacji zdjęciowej) lub do serwera agencji ochrony po otrzymaniu wyposażenia technicznego na potrzeby takich danych. Po połączeniu z internetem za pośrednictwem komunikatora LAN dostęp zdalny jest możliwy także przy użyciu oprogramowania F-Link (J-Link).

Centralę alarmową można rozbudować o dodatkowy komunikator:

JA-19xY — komunikator GSM do komunikacji GSM/GPRS. Umożliwia taki sam sposób komunikacji i usługi jak komunikator LAN.



1 — Otwory do montażu na ścianie; 2 — Zasilacz centrali alarmowej; 3 — Zaciski zasilania sieciowego; 4 — Bezpiecznik główny; 5 — Bateria awaryjna; 6 — Pasek do mocowania baterii awaryjnej; 7 — Złącze komunikatora GSM; 8 — Płytka drukowana centrali alarmowej; 9 — Styk sabotażu w obudowie; 10 — Uchwyt modułu radiowego JA-11xR; 11 — Schowek na przewód; 12 — Złączka USB do podłączenia do komputera)



1 — Zacisk zasilania; 2 — Niezależne zaciski MAGISTRALI; 3 — Kontrolki; 4 — Złączka MiniUSB; 5 — Zacisk MAGISTRALI dla modułu radiowego lub 3. zacisku MAGISTRALI; 6 — Złączka LAN; 7 — Złączka komunikatora GSM; 8 — Złączki do styków sabotażu w obudowie; 9 — Złączka do dodatkowych modułów; 10 — Kabel złączowy RESETOWANIA; 11 — Uchwyt karty MicroSD

Części centrali alarmowej JA-107K (wymienne) są następujące:

- Karta MicroSD

W celu poszerzenia opcji centrali alarmowej należy wykorzystać:

- Moduł radiowy JA-11xR
- Komunikator GSM JA-19xY

Do elementów wyposażenia dodatkowego centrali alarmowej należą:

- 1 szt. przewód USB (180 cm)
- 1 szt. przewód łączący do modułu radiowego JA-11xR
- 1 szt. przedłużacz USB (20 cm) zainstalowany w centrali alarmowej
- 1 szt. bezpiecznik T1,6 A, 250 V
- 4 szt. złącza (do podłączania wtyków złącza)
- 6 szt. naklejki ostrzegawcze
- 4 szt. elementy mocujące 8 mm
- 4 szt. wkręty 40 mm
- 2 szt. opaski 150 mm
- Szablon do nawiercania A3
- 2 szt. wkręty 3 x 8 mm
- 2 szt. redukcja do podłączania zacisków FASTON do baterii
- Instrukcja instalacji CZ/EN (wersja skrócona)

3.3 Kontrolki na płytce centrali alarmowej

Wszystkie wersje centrali alarmowych są wyposażone w poniższe kontrolki na płycie głównej:

Opis	Kolor	Znaczenie
AKTYWNA	zielony	Miganie podczas pracy MAGISTRALI komunikacji wskazuje poprawne działanie
BŁĄD	żółty	Nieprzerwane świecenie sygnalizuje ogólny błąd systemu (więcej informacji w programie F-Link lub na klawiaturze z wyświetlaczem).
USB	żółty	Sygnalizacja połączenia USB z komputerem.
GSM	czerwony	Jeżeli zainstalowano komunikację GSM: – świeci nieprzerwanie po podłączeniu zasilania podczas wyszukiwania sieci GSM (najwyżej przez 1 min). – WYŁ. sygnalizuje GSM OK i brak komunikacji. – Miganie w odstępach 1s/1s WŁ/WYŁ sygnalizuje brak dostępnej sieci GSM. *Uwaga*: *Szybkie, wielokrotne miganie podczas komunikacji sygnalizuje ustawienie parametru: komunikator GSM WYŁ.*

3.4 Dodatkowe złącza na płytce drukowanej centrali alarmowej

Wszystkie centrale alarmowe mają 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.

Płytka drukowana centrali alarmowej zawiera płaską złączkę na potrzeby komunikatora GSM JA-19xY oraz złączkę 10-pinową na potrzeby dodatkowego modułu.

Istnieje także złączka 4-pinowa:

- JA-103K — I-BUS — przeznaczona wyłącznie do podłączania modułu radiowego JA-11xR, umieszczonego
  w obudowie centrali alarmowej. Do tej złączki nie można podłączyć żadnego innego urządzenia.
- JA-107K — jest to 3. MAGISTRALA o takich samych parametrach jak MAGISTRALA 1 i 2. Umożliwia podłączenie
  modułu radiowego JA-11xR lub rozbudowę systemu na potrzeby 3. MAGISTRALI przez podłączenie rozdzielacza MAGISTRALI JA-110Z-D.

Istnieją 3 złączki na potrzeby specjalnego styku sabotażu na płytce drukowanej centrali alarmowej (styk sabotażu pokrywy przedniej, tylny styk sabotażu i jeden uzupełniający styk sabotażu, zwiększający poziom

ochrony). Obok każdej złączki znajduje się kabel złączowy. Jego usunięcie powoduje WŁĄCZENIE styku sabotażu. W przypadku braku wykorzystywania któregokolwiek ze styków kabel złączowy musi być podłączony.

3.5 Zaciski łączące na płytce drukowanej centrali alarmowej

Centrala alarmowa systemu bezpieczeństwa posiada wymóg stałego podłączenia do zasilania sieciowego ~110–230 V. Zasilanie sieciowe podłącza się za pomocą zacisków z wymiennym bezpiecznikiem. Centrala alarmowa jest urządzeniem o 2. klasie ochronności z podwójną izolacją. Dlatego właśnie wystarczy kabel dwużyłowy (przewód pod napięciem i neutralny). Przewód uziemiający (jeżeli istnieje) można podłączyć do zacisku FE (w przypadku JA-107K należy usunąć zaślepkę). Komunikacja wewnętrzna między centralą alarmową a podłączonymi urządzeniami odbywa się za pośrednictwem MAGISTRALI. Centrala alarmowa JA-103K realizuje ją za pomocą pojedynczego zacisku o czterech kolorach (czerwony, żółty, zielony i czarny), a w przypadku centrali JA-107K istnieją dwa takie zaciski MAGISTRALI.

Wbudowana złączka USB znajduje się na płytce drukowanej centrali alarmowej, podłączonej do złączki USB na obudowie centrali alarmowej. Pozwala to ustanowić połączenie z komputerem za pomocą przewodu USB bez otwierania centrali alarmowej.

4 Przed instalacją systemu

Na centralę alarmową należy wybrać osłonięte miejsce (w chronionym obszarze), w którym dostępne jest zasilanie sieciowe. Zalecamy ochronę pomieszczenia z centralą alarmową za pomocą czujki o reakcji natychmiastowej. Jeżeli centrala alarmowa jest wyposażona w komunikator GSM, w danej lokalizacji musi być dobry odbiór sygnału GSM (sprawdzić telefonem). Przestroga: Jeżeli ewentualny intruz zna położenie centrali alarmowej, istnieje ryzyko uszkodzenia systemu bez wysłania informacji o włamaniu.

Zasilanie sieciowe centrali alarmowej może instalować jedynie osoba posiadająca wymagane kwalifikacje w zakresie elektryki. Zasilanie centrali alarmowej ma podwójne rozdzielenie obwodów ze względów bezpieczeństwa. Podczas instalacji i podłączania elementów MAGISTRALI należących do centrali alarmowej całe zasilanie centrali alarmowej musi być całkowicie odłączone lub CENTRALA alarmowa musi być wyłączona w oprogramowaniu F-Link.

Centrala alarmowa zapewnia opcję podłączenia zasilania w zakresie ~110–230 V / 50–60 Hz.

1. Najpierw należy rozważyć układ i docelowe ustawienie systemu. Ustalić z klientem żądaną metodę sterowania. W przypadku bardziej złożonego systemu zaleca się przygotowanie dokumentacji projektowej.
2. Podczas konfiguracji urządzeń należy przestrzegać ich instrukcji obsługi, ogólnych zasad budowy systemu sygnalizacji pożaru i instrukcji przekazanych przez producenta podczas szkolenia certyfikacyjnego. W przypadku jakichkolwiek niejasności należy telefonicznie skontaktować się z konsultantem firmy Jablotron. **Producent nie ponosi odpowiedzialności za jakiekolwiek szkody w przypadku nieprawidłowej instalacji lub konfiguracji systemu.**
3. Należy przygotować zasilanie centrali alarmowej, wykorzystując odpowiedni przewód z podwójną izolacją o przekroju 0,75–1,5 mm². Zaleca się ochronę przepięciową na zasilaniu sieciowym centrali alarmowej. Zaleca się także wykorzystanie pojedynczego przewodu z wyłącznikiem automatycznym (2–6 A), który pełni również funkcję wyłącznika głównego.
   Ostrzeżenie: *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.*
4. Centralę alarmową należy przymocować bezpośrednio do ściany lub innej niepalnej powierzchni. Sprawdzić, czy w pobliżu centrali alarmowej nie ma metalowych konstrukcji (np. szyb windy), mogących negatywnie oddziaływać na transmisję lub odbiór sygnałów radiowych (moduł radiowy i komunikator GSM). Do przygotowania otworów na elementy mocujące należy użyć dołączonego szablonu. Przełożyć dostarczone wkręty przez górne otwory w plastikowej obudowie, aby utrzymać ją w odległości 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

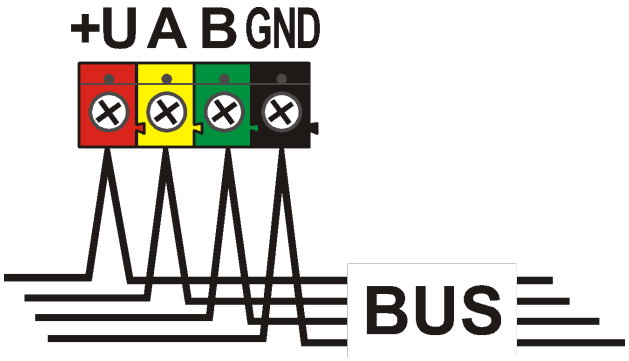
Do systemu podłączyć wyłącznie urządzenia MAGISTRALI serii JA-1xx JABLOTRON. Należy postępować w następujący sposób:

1. Podczas podłączania jakichkolwiek modułów MAGISTRALI zasilanie centrali alarmowej musi być całkowicie wyłączone lub MAGISTRALA musi być wyłączona w oprogramowaniu F-Link.
2. Należy przestrzegać instrukcji instalacji poszczególnych urządzeń.
3. Przewód MAGISTRALI należy zamontować wewnątrz obszaru chronionego przez system. Jeżeli przewód znajduje się poza obszarem chronionym, tę część należy oddzielić separatorem MAGISTRALI JA-110T.
4. Do rozgałęziania instalacji należy wykorzystać rozdzielacz MAGISTRALI JA-110Z (i JA-110Z-B, JA-110Z-C, JA-110Z-D).
5. Podczas podłączania urządzeń MAGISTRALI należy zwracać uwagę na kolor żył (czerwona, żółta, zielona, czarna).

Urządzenia podmiotów zewnętrznych lub urządzenie innego producenta można podłączyć za pośrednictwem odpowiedniego modułu (JA-111H, JA-116H, JA-114HN, JA-110M, JA-118M itp.). W przypadku wykorzystania takiego urządzenia producent (JABLOTRON) nie może zagwarantować odpowiedniego działania podłączonego urządzenia ani klasy bezpieczeństwa systemu.

5.1 MAGISTRALA JABLOTRON 100+

MAGISTRALA systemu JABLOTRON 100+ ma 4 żyły (4-żyłowa). MAGISTRALA jest przeznaczona wyłącznie do systemu JABLOTRON 100+ i nie można jej dzielić z innym systemem ani za jej pomocą zasilać innych urządzeń. Do zasilania innych systemów za pomocą MAGISTRALI (automatyka inteligentnego domu) należy wykorzystać interfejs JA-121T lub separator magistrali JA-110T BUS.



Listwa zaciskowa MAGISTRALI

Zacisk	Kolor	Uwaga
+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-03	opór pary na 1 m	0,0705 Ω
	opór pary na 10 m	0,705 Ω
	opór pary na 100 m	7,05 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

Podłączyć urządzenia MAGISTRALI za pomocą przewodu JABLOTRON CC-01, CC-02, CC-03 lub CC-11.

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

Przewód CC-01 JABLOTRON jest przewidziany do głównej linii MAGISTRALI lub łączenia elementów o wysokim zużyciu (syrena) lub elementów zdalnych. Przewód ma 4 żyły (kolory odpowiadające kolorowi MAGISTRALI). Żyły zasilające (czarna i czerwona) cechują się większym przekrojem rdzenia (0,5 mm^2) w porównaniu z przewodami do komunikacji (0,2 mm^2). Kabel dostarczamy w opakowaniach po 300 m.

Przewód CC-02 JABLOTRON 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.

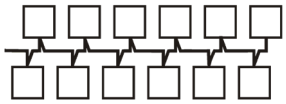
Przewód CC-03 JABLOTRON jest przewidziany do głównej linii MAGISTRALI lub łączenia elementów o wysokim zużyciu (syrena) lub elementów zdalnych. Przewód ma 8 żył (8-żyłowy) podzielonych w następujący sposób: Żyły zasilające (czerwona i czarna) mają większy przekrój, tj. 0,7 mm^2, żyły komunikacji (zielona i żółta) dla MAGISTRALI systemu oraz żyły pomocnicze (brązowa i szara, biała i niebieska) mają przekrój 0,3 mm^2. Żyły pomocnicze można wykorzystać jako pętle do czujek magnetycznych lub styków sabotażu. Kabel dostarczamy w opakowaniach po 250 m.

Przewód CC-11 JABLOTRON jest przewidziany do głównej linii MAGISTRALI lub łączenia elementów o wysokim zużyciu (syrena) lub elementów zdalnych. Kabel ma izolację zewnętrzną w kolorze pomarańczowym i 4 żyły (w kolorach odpowiadających kolorowi MAGISTRALI). Żyły zasilające (czarna i czerwona) charakteryzują się większym przekrojem rdzenia (0,5 mm^2) w porównaniu z przewodami do komunikacji (0,2 mm^2). Kabel dostarczamy w opakowaniach po 200 m. Ma on atest zwiększonej ochrony przeciwpożarowej B2CA.

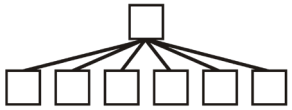
5.3 Układ MAGISTRALI

Podłączając poszczególne części systemu, tj. czujki, klawiatury, syreny, moduły wyjść itp., kabel MAGISTRALI można poprowadzić najkrótszą możliwą drogą niezależnie od części systemu, do której należą wykorzystane elementy. MAGISTRALA może mieć wymaganą liczbę odgałęzień. Może cechować się strukturą liniową (łańcucha), gwiazdy lub drzewa (łańcucha i gwiazdy). W faktycznych instalacjach połączenie tych trzech opcji jest zwykle najbardziej dogodnym wyborem.

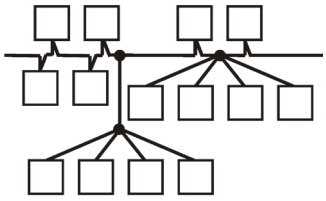
Przykłady możliwych układów okablowania MAGISTRALI:



Łańcuch (liniowa struktura MAGISTRALI)



Gwiaździsta struktura MAGISTRALI



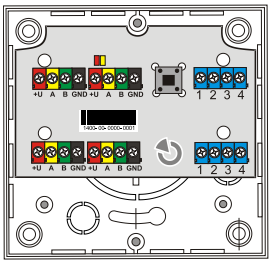
Łańcuch i gwiazda (drzewiasta struktura MAGISTRALI)

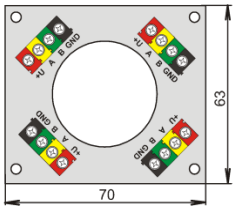
Kabla MAGISTRALI **nie wolno** podłączać w sposób tworzący **zamkniętą pętlę** jakiegokolwiek przewodu (końców poszczególnych odgałęzień nie wolno łączyć ze sobą, nie wolno także łączyć wspólnego przewodu GND).

5.4 Rozgałęzianie i dzielenie MAGISTRALI

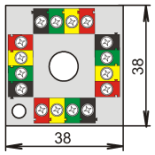
W celu wygodnego rozgałęziania i dzielenia MAGISTRALI można wykorzystać **rozgałęziacz MAGISTRALI JA-110Z**. Produkuje się go w czterech wariantach: JA-110Z, JA110Z-B, JA110Z-C i JA110Z-D. JA-110Z dostarcza się w puszce montażowej przeznaczonej do montażu natynkowo, wyposażonej w przedni i tylny styk sabotażu w celu wykrywania niepożądanej manipulacji. Zajmuje jedną pozycję w systemie. Wszystkie zaciski tego samego koloru są połączone ze sobą na płytce drukowanej rozdzielacza. Wariant B ma wymiary umożliwiające montaż w wielofunkcyjnej puszce montażowej JA-190PL. Wariant C ma wymiary umożliwiające montaż w standardowej elektrycznej puszce montażowej KU-68.

Warianty listw zaciskowych do łączenia wzajemnego:





JA-110Z-B



JA-110Z-C

5.5 Długość MAGISTRALI i liczby podłączonych urządzeń

Maksymalna długość MAGISTRALI bez wzmacniania (separacji) wynosi 500 m. Długość oblicza się jako sumę długości wszystkich przewodów między wszystkimi połączonymi urządzeniami. Centrale alarmowe JA-107K mogą mieć do 3 odrębnych odgałęzień MAGISTRALI, tj. całkowita długość obu linii MAGISTRALI może wynosić 3 x 500 m. Zalecamy, aby adresowane urządzenia MAGISTRALI równo rozdzielić między obie linie MAGISTRALI, tj. maksymalnie 60 urządzeń na każdą MAGISTRALĘ.

Liczbę podłączonych urządzeń MAGISTRALI ogranicza pojemność baterii awaryjnej centrali alarmowej. Aby spełnić normę dla poziomu bezpieczeństwa 2, w przypadku awarii zasilania sieciowego 230 V system musi działać niezawodnie przez co najmniej 12 godzin przy zasilaniu z awaryjnego źródła zasilania. Tym samym całkowite zużycie dla wszystkich urządzeń MAGISTRALI nie może przekraczać maksymalnego ciągłego zużycia prądu z centrali alarmowej, patrz rozdział 5.8 Example of calculation of BUS consumption to back-up the system. Aby obliczyć całkowite ciągłe zużycie podłączonych elementów, należy zsumować ich **zużycie awaryjne** (określone w instrukcji).

Kolejnym parametrem ograniczającym całkowitą długość MAGISTRALI może być strata napięcia na linii (wyraźnie wskazana przez Diagnostykę systemu w oprogramowaniu F-Link).

5.6 Obliczanie strat na linii

Straty napięcia na linii zależą od oporu linii, który wynika z użytego przewodu (kabla) i zużytego prądu. Wartości zużycia prądu urządzeń można znaleźć w poszczególnych instrukcjach obsługi. Te wartości można wykorzystać do obliczenia straty napięcia linii w celu stwierdzenia, czy będzie wystarczające napięcie dla ostatniego zainstalowanego urządzenia. Obliczenie opiera się na prawie Ohma **U = I * R.**

Kabel CC-01 (para zasilająca)		**Kabel CC-02**		**Kabel CC-03 (para zasilająca)**		**Kabel CC-11 (para zasilająca)**	
Natężenie całkowite	Maks. długość	Natężenie całkowite	Maks. długość	Natężenie całkowite	Maks. długość	Natężenie całkowite	Maks. długość
50 mA	400 m	25 mA	200 m	70 mA	400 m	50 mA	400 m
100 mA	300 m	50 mA	150 m	140 mA	300 m	100 mA	300 m
200 mA	150 m	100 mA	100 m	280 mA	150 m	200 mA	150 m
300 mA	100 m	200 mA	50 m	420 mA	100 m	300 mA	100 m
500 mA	50 m	300 mA	30 m	800 mA	50 m	500 mA	50 m
Dane w tabeli zakładają najgorszy możliwy scenariusz, tj. że całkowite zużycie występuje na końcu kabla.							

W zwykłym stanie eksploatacji napięcie zacisków +U i GND wynosi niemal 14 V. Do obliczeń należy przyjąć sytuację, w której centrala alarmowa jest zasilana wyłącznie baterią, a napięcie sięga około 12 V. Dla wszystkich urządzeń musi być dostępne napięcie wyższe od minimalnego dozwolonego o wartości 10 V. W celu prawidłowego funkcjonowania podłączonych urządzeń **maksymalna dozwolona strata napięcia wynosi 2,0 V.**

Nieoczekiwaną stratę napięcia mogą powodować złącza zacisków o słabym styku (opory przejściowe).

Straty napięcia poszczególnych urządzeń można zweryfikować w przybliżeniu przy pomocy oprogramowania F-Link w karcie Diagnostyka dla urządzeń adresowanych. Urządzenia nieadresowane (np. moduły wyjściowe) nie dają takiej możliwości. Należy je sprawdzać przy pomocy urządzenia pomiarowego.

W rzeczywistych instalacjach zawsze zalecamy weryfikację obliczeń i połączenia przez pomiar zacisku. W przypadku urządzeń o wysokim zużyciu (syrena, klawiatura, wyjście przekaźnika) taki pomiar należy przeprowadzić w okresach o wyższym zużyciu (aktywna syrena, podświetlona klawiatura, włączony przekaźnik).

Obowiązują ogólne ograniczenia określone w tabeli.

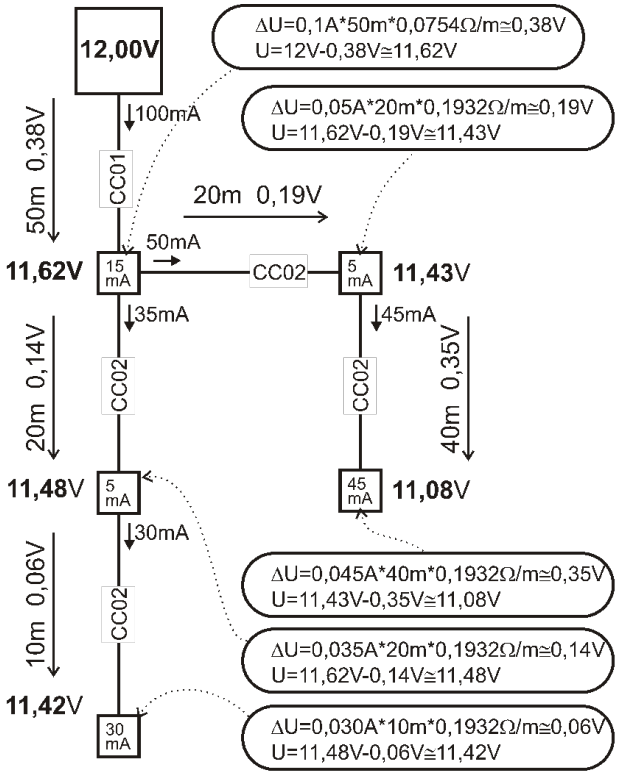
W celu obliczenia całkowitego obciążenia kabla należy obliczyć **zużycie dla dobranych przewodów** (podano je w instrukcjach urządzeń).

5.7 Przykład obliczania straty napięcia

1. Znaleźć parametry zużycia prądu dla poszczególnych urządzeń (w parametrach technicznych produktów — Zużycie prądu dla wybranych przewodów).
2. Uzyskać informacje o długościach przewodów. Trzeba znać jak najdokładniejszą wartość długości przewodu od węzła do węzła.
3. Narysować plan przedstawiający długość przewodów i zużycie poszczególnych odgałęzień.
4. Obliczyć natężenie prądu przepływającego przez poszczególne odgałęzienia.

5. Aby porównać odpowiedniość wyboru kabli, wykorzystać przyjętą długość linii i szacunkowe wartości natężenia poszczególnych odgałęzień zgodnie z powyższą zakładką.

Odliczyć poszczególne straty od napięcia zasilania, aby określić napięcie na końcu linii. Należy zawsze uwzględnić napięcie 12 V z centrali alarmowej podczas działania przy awarii zasilania sieciowego.



5.8 Przykładowe obliczenie zużycia MAGISTRALI dla systemu awaryjnego

W tabeli podano przykład małego systemu. Całkowite zużycie w trybie jałowym w trybie awaryjnym wynosi 78 mA. Dzięki temu można wykorzystać centralę alarmową JA-103K z komunikatorem GSM oraz wyłączonym komunikatorem LAN, co umożliwia maksymalne stałe obciążenie na poziomie 80 mA.

Urządzenie	Opis	Liczba sztuk	Zużycie w awaryjnym trybie zasilania
JA-11xR	moduł do komunikacji radiowej	1	25 mA
JA-114E	centrala alarmowa 15 mA + 3 x segmenty 1 mA	1	18 mA
JA-110M	moduł do czujników magnetycznych 5 mA	1	5 mA
JA-110P	czujka ruchu PIR 5 mA	2	10 mA
JA-110ST	czujka pożarowa 5 mA	2	10 mA
JA-110A	syrena wewnętrzna 5 mA	1	5 mA
JA-111A	syrena zewnętrzna z zasilaniem awaryjnym 5 mA	1	5 mA
		RAZEM	**78 mA**

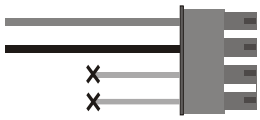
Typ JA-103 bardziej nadaje się do systemów bezprzewodowych, gdzie urządzenia są zasilane bateriami. Podczas planowania konfiguracji bezprzewodowej centrali alarmowej nie należy zapominać o wliczeniu modułów radiowych do zużycia.

W przypadku większych systemów MAGISTRALI należy używać centrali alarmowej JA-107K.

5.9 Wymogi dotyczące zasilania

Centrala alarmowa wymaga stałego zasilania z zabezpieczonego źródła AC o napięciu w zakresie 110–230 V, patrz Specyfikacja techniczna. Centrala alarmowa jest urządzeniem o podwójnej izolacji, w związku z czym podłącza się ją zwykle kablem o podwójnej izolacji i przekroju 0,75–1,5 mm². Centrala alarmowa ma zabezpieczenie w formie małego bezpiecznika ze szkła. Wchodzi w skład zacisków zasilania sieciowego. Urządzenia JA-103K nie można zasilać ze źródeł alternatywnych, jak baterie o dużej pojemności ładowane panelami słonecznymi itp.

Urządzenie JA-107K można zasilać ze źródeł alternatywnych. Napięcie zasilania dla centrali alarmowej musi mieć wartość 10–15 V. Należy zapewnić źródło zasilania awaryjnego. Podłączyć zewnętrzne źródło zasilania do zacisku zasilania. Do podłączenia zasilania z zewnętrznego źródła zasilania należy wykorzystać żyłę czerwoną i czarną. Przeciąć i zaizolować białe żyły do komunikacji. Producent nie ponosi jakiejkolwiek odpowiedzialności za szkody spowodowane używaniem alternatywnego źródła energii.



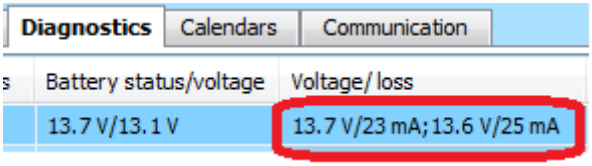
5.10 Wymagania dotyczące zasilania awaryjnego

System bezpieczeństwa, który musi spełniać wymogi dla klasy ochronności 2, wymaga zasilania awaryjnego przez 12 godzin podczas awarii zasilania sieciowego. Musi być także w pełni naładowany 72 godziny po przywróceniu zasilania i gotowy do ponownego awaryjnego zasilania systemu. Aby spełnić ten wymóg, nie wolno przekraczać maksymalnego zużycia prądu z MAGISTRALI.

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

	JA-103K bateria 2,6 Ah		**JA-107K bateria 18 Ah**	
Maksymalne ciągłe zużycie mocy z MAGISTRALI	MAGISTRALA 1 — 1000 mA I-BUS — 200 mA		2000 mA stałe 3000 mA przez 60 min (maks. 2000 mA dla jednej MAGISTRALI)	
Maksymalne ciągłe zużycie energii dla zasilania awaryjnego 12 godzin	Bez komunikatora GSM	LAN — WYŁ. — 115 mA LAN — WŁ. — 88 mA	Bez komunikatora GSM	LAN — WYŁ. — 1135 mA LAN — WŁ. — 1107 mA
	Z komunikatorem GSM	LAN — WYŁ. — 80 mA LAN — WŁ. — 53 mA	Z komunikatorem GSM	LAN — WYŁ. — 1100 mA LAN — WŁ. — 1072 mA

Natężenie pobrane z każdego zacisku wyjściowego MAGISTRALI przedstawia program F-Link w zakładce Diagnostyka w wierszu 0, gdzie znajduje się centrala alarmowa. W przypadku centrali alarmowej JA-107K należy zsumować wartość wszystkich wyjść MAGISTRALI. Natężenie porównuje się z natężeniem podanym w powyższej tabeli. W ten sposób można sprawdzić, czy pojemność baterii awaryjnej spełnia wymogi norm dla czasu zasilania awaryjnego systemu. Jeżeli zmierzone natężenie jest wyższe od podanego w tabeli, należy rozwiązać zasilanie systemu, np. dodając moduł wzmacniacza JA-120Z.



5.11 Izolacja MAGISTRALI

Części MAGISTRALI prowadzone w obszarach pozbawionych ochrony wymagają zabezpieczenia na wypadek ewentualnego zwarcia lub innej próby dezaktywacji systemu w formie izolacji przy użyciu izolatora MAGISTRALI JA110T. Moduł można wpiąć w wielofunkcyjną puszkę instalacyjną JA-190PL. Izolator poprawia także jakość sygnału MAGISTRALI. Jest podłączony do MAGISTRALI i przez nią zasilany, nie zajmuje pozycji

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

w systemie i umożliwia przedłużenie MAGISTRALI o kolejne 500 m. Na jednym odgałęzieniu MAGISTRALI nie należy stosować 2 lub większej liczby izolatorów MAGISTRALI — urządzenia nie mogą się komunikować za pośrednictwem 2 ani większej liczby izolatorów.

Przykładem zastosowania może być marszrutowanie do modułów przekaźnika sterujących na przykład roletami lub syreną, do których MAGISTRALA ma marszrutę umożliwiającą potencjalny atak lub dezaktywację z zewnątrz. Bardziej szczegółowe informacje znajdują się w instrukcji JA-110T.

MAGISTRAL
A z centrali

Ewentualne uszkodzenie MAGISTRALI za modułem, spowodowane na przykład zwarciem, nie wpływa na

5.12 W przypadku remontów wykorzystać istniejące kable.

- W celu instalacji nowych linii lepiej używać przewodów CC-01, CC-02, CC-03 oraz CC-11.
- W przypadku podłączenia do kabli typu SYKFY 3 x 2 x 0,5 żyły danych MAGISTRALI (A, B) należy podłączyć do jednej wybranej skrętki dwużyłowej. W odniesieniu do zasilania (+U12, GND) można podłączyć odpowiednie żyły razem w pozostałych dwóch parach (dublowanie w obrębie pary).
- W przypadku podłączenia do przewodów UTP żyły danych MAGISTRALI (A, B) należy podłączyć do jednej wybranej skrętki dwużyłowej. W przypadku zasilania (+U, GND) należy połączyć razem (zdublować) odpowiednie żyły pozostałych skrętek dwużyłowych.

W przypadku wykorzystania kabla ekranowanego nie podłączać ekranu do zacisków MAGISTRALI! Zalecamy połączenie wszystkich ekranów (cynowania) w centrali alarmowej do zacisku pomocniczego, a nie w jakimkolwiek innym miejscu. Drugi koniec ekranu od strony urządzenia powinien pozostać wolny.

6 Wykorzystanie urządzeń bezprzewodowych

W systemie JABLOTRON 100+ można użyć urządzenia bezprzewodowego serii JA-15x, JA-16x i JA-18x. Do komunikacji z urządzeniami bezprzewodowymi należy wykorzystać moduł radiowy JA-11xR. W systemie mogą być najwyżej 3 moduły radiowe.

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

Przestroga: *Do centrali alarmowej JA-107K można przypisać najwyżej 120 urządzeń bezprzewodowych, wyłącznie w pozycjach 1 do 120. Pozycje 121 do 230 są przeznaczone wyłącznie dla urządzeń MAGISTRALI. Jeżeli moduł radiowy JA-11xR zainstalowano za modułem wzmacniacza MAGISTRALI JA-120Z, należy go przypisać w zakresie pozycji 1–120.*

6.1 Instalacja modułu radiowego JA-11xR

1. Moduł radiowy JA-11xR można umieścić w uchwycie w prawym dolnym rogu centrali alarmowej.
2. W przypadku instalacji centrali alarmowej JA-103/107K w miejscu o słabym odbiorze sygnału GSM moduł GSM zwiększa moc transmisji, co może niekorzystnie wpływać na zasięg komunikacji modułu radiowego w systemie. W takim przypadku zaleca się umieszczenie modułu radiowego poza centralą alarmową, w odległości co najmniej 2 m od niej, w miejscu, gdzie nie będzie podlegać niekorzystnemu wpływowi i gdzie będzie mieć wyższej jakości odbiór radiowy z urządzeń, co umożliwi większy zasięg, a tym samym dłuższe odległości instalacji.

   Uwaga: *Urządzenie JA-111R wyjęte z centrali alarmowej należy umieścić w plastikowej obudowie PLV-111R (sprzedawanej oddzielnie).*

   Złączka modułu radiowego na płytce drukowanej centrali alarmowej JA-103K
   jest przeznaczona wyłącznie do podłączania jednego modułu radiowego zainstalowanego w obudowie centrali alarmowej.

3. Sygnałem radiowym można objąć większy obszar, instalując najwyżej 3 moduły radiowe w różnych miejscach (np. każdy na innym piętrze). Sygnały z urządzenia bezprzewodowego (dalej urządzenie) może odbierać jednocześnie większa liczba modułów radiowych. 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. Później nie otrzyma tej samej informacji z innych modułów radiowych, nawet jeśli odebrały ją przy silniejszym sygnale. W odniesieniu do urządzeń dwukierunkowych centrala alarmowa „rezerwuje" raz używany kanał (komunikacja z pierwszym modułem radiowym), a później komunikuje się z danym urządzeniem wyłącznie za pośrednictwem tego modułu radiowego (jak pokazano w zakładce Diagnostyka, kolumna Kanał) do chwili, gdy urządzenie przestanie reagować. 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). Można wybrać moduł radiowy, dla którego należy sprawdzić komunikację oraz urządzenia aktywne 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.).
5. Po włączeniu systemu **należy najpierw przypisać moduły radiowe.** Dopiero wówczas można przypisać urządzenia bezprzewodowe.

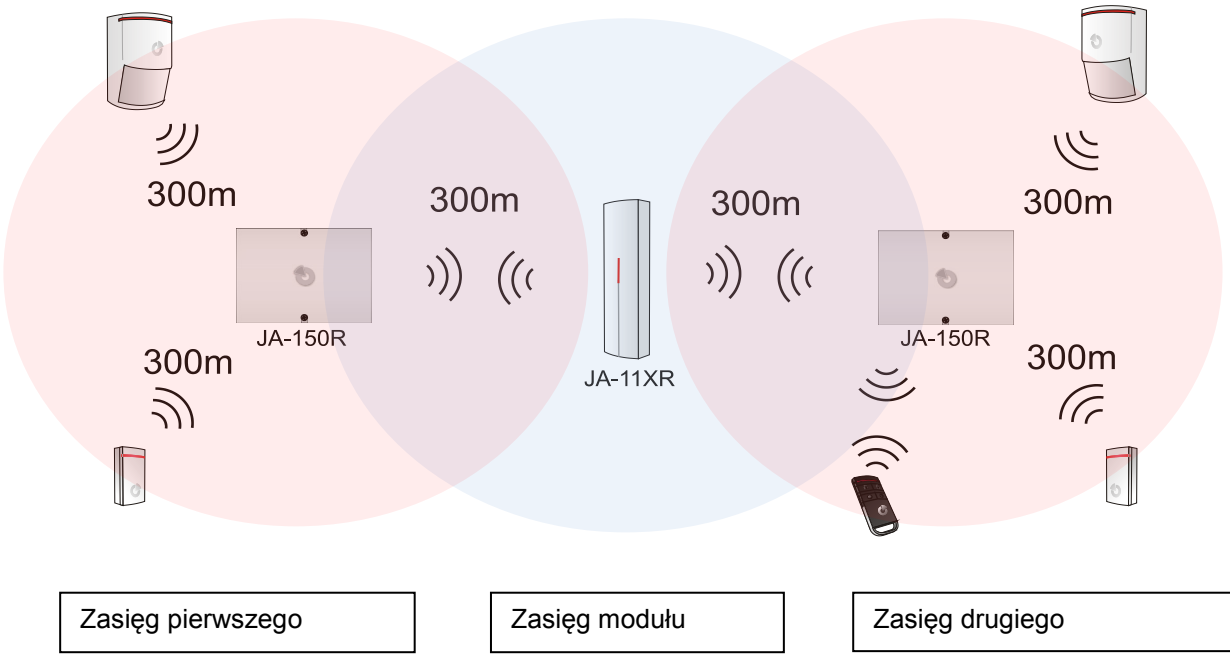
Zalecenie: Zaleca się przypisywanie urządzeń bezprzewodowych po ich instalacji w ostatecznym położeniu w pomieszczeniu. Choć w ten sposób procedura instalacji jest mniej wygodna, oferuje zaletę bardziej niezawodnego połączenia urządzeń bezprzewodowych z modułem radiowym po uruchomieniu systemu alarmowego. Moduł radiowy realizuje mechanizm pomiaru sygnału RF w trybie serwisowym. Ten mechanizm zapewnia margines bezpieczeństwa na wypadek pogorszenia warunków transmisji radiowej podczas pełnej eksploatacji systemu. Więcej informacji podano w normie EN 50131-5-3.

6.2 Instalacja urządzeń bezprzewodowych — tryb przypisywania

Urządzenia bezprzewodowe można przypisać do systemu na przykład za pomocą kodu produktu. Procedurę przypisywania można przeprowadzić w trybie przypisywania za pomocą komputera z zainstalowanym programem F-Link, patrz rozdział 8.4.1 Enrolling and erasing devices.

6.3 Zwiększanie zasięgu urządzeń bezprzewodowych

Jeżeli standardowy zasięg modułu radiowego nie jest wystarczający lub jeśli nie można skrócić odległości między modułem radiowym a urządzeniami bezprzewodowymi, sygnały jednokierunkowych urządzeń bezprzewodowych (czujek, manipulatorów zdalnych, modułu PG) można wzmocnić za pomocą wzmacniacza sygnału radiowego JA-150R, którego instalacja wymaga jedynie stałego zasilania. Lokalizację wzmacniacza sygnału JA-150R wybiera się tak, by zarówno centrala alarmowa (moduł radiowy), jak i urządzenia bezprzewodowe znajdowały się w jego zasięgu, patrz poniższy rysunek.



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 przy pomocy 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 -).
   a. Włączyć zasilanie sieciowe i sprawdzić kontrolki na centrali alarmowej:
   b. Zielona dioda zaczyna migać (funkcja MAGISTRALI).
   c. Miga czerwona dioda — logowanie do sieci GSM.
   d. Czerwona dioda GSM gaśnie — centrala alarmowa ustanowiła połączenie z siecią mobilną.
   e. Czerwona dioda świeci — centrala alarmowa nie zalogowała się do sieci .
   (punkty c, d, e odnoszą się wyłącznie do urządzeń z zainstalowanym komunikatorem GSM).
6. Kiedy podłączone urządzenia MAGISTRALI zaczną migać na żółto, należy je przypisać do systemu, patrz rozdział 8.4.1 Enrolling and erasing devices.
7. Należy przeprowadzić konfigurację klawiatur, patrz rozdział 10.5.1 Keypad configuration.
8. Skonfigurować niezbędne funkcje i sprawdzić system, patrz rozdział 10.9 Parameters tab.
9. Aby spełnić wymogi normy EN50131-1 lub INCERT, klasa 2, odłączyć przedłużacz USB od płytki drukowanej centrali alarmowej.

8 Konfiguracja systemu

System bezpieczeństwa (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 3 zegary.

Ochrona obiektu zapewnia bezpieczeństwo sejfów i kosztowności, ale także wykrywanie włamania 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 zwykle mają regulowaną reakcję, trwale niezależną od stanu systemu lub po prostu reakcję 24 h.

8.1 Profile systemu

Gama profili systemu umożliwia globalną konfigurację następujących parametrów systemu 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 i wdrożenie usługi SMA.*

Przegląd parametrów systemu po ustawieniu „DOMYŚLNEGO" profilu systemu (ustawień domyślnych):

Urządzenie	Parametr	Opcja	Blokowanie (ograniczenie)
Centrala alarmowa	Kody z prefiksem	NIE	NIE
Centrala alarmowa	Aktywować standard karty 125 kHz EM UNIQUE	TAK	NIE
Centrala alarmowa	Długość kodu	4	NIE
Centrala alarmowa	Automatycznie sprawdzić czas w podłączonym komputerze	TAK	NIE
Centrala alarmowa	Syrena przy uzbrojeniu częściowym	NIE	NIE
Centrala alarmowa	Syreny aktywne	TAK	NIE
Centrala alarmowa	Ostrzeżenie o kodach domyślnych	TAK	NIE
Centrala alarmowa	Administrator — ograniczone prawa serwisowe / SMA	NIE	NIE
Centrala alarmowa	Serwis i SMA steruje systemem	TAK	NIE
Centrala alarmowa	Działanie próbne	NIE	NIE
Centrala alarmowa	Wymóg serwisu	NIE	NIE
Centrala alarmowa	Aktywować tryb konserwacji	TAK	NIE
Centrala alarmowa	Antynapadowa kontrola dostępu	TAK	NIE
Centrala alarmowa	Potwierdzenie alarmu w jednej strefie	NIE	NIE
Centrala alarmowa	Syrena (wyjście IW) przy aktywacji sabotażu	NIE	NIE

Centrala alarmowa	Sygnalizacja alarmu sabotażu resetowana przez Serwis	NIE	NIE
Centrala alarmowa	Reset aktywny	TAK	NIE
Centrala alarmowa	Dobowe resetowanie auto-pominięcia urządzenia	TAK	NIE
Centrala alarmowa	Blokowanie podczas uzbrajania	NIE	NIE
Centrala alarmowa	Rozbrojenie anuluje alarm	NIE	NIE
Centrala alarmowa	Niepowodzenie uzbrojenia	NIE	NIE
Centrala alarmowa	Auto-pominięcie z powodu problemu z urządzeniem	TAK	TAK
Centrala alarmowa	Opóźniony raport do SMA	NIE	NIE
Centrala alarmowa	Sposoby uzbrajania	Uzbrój z ostrzeżeniem	NIE
Centrala alarmowa	Typ uwierzytelniania	Standardowy	NIE
Centrala alarmowa	Blokowanie systemu przez alarm	NIE	NIE
Centrala alarmowa	Utrata modułu MAGISTRALI	Błąd	NIE
Centrala alarmowa	Auto-pominięcie usterki	3. aktywacja	TAK
Centrala alarmowa	Długość alarmu	260 sek.	90…1200 sek.
Centrala alarmowa	Opóźnienie na wejście	30 sek.	5…120 sek.
Centrala alarmowa	Opóźnienie na wyjście	30 sek.	5..120 sek.
Moduł radiowy	Wykrywanie zagłuszania RF	Nieaktywna	NIE
Klawiatura	Ustawienia sygnalizacji optycznej	1. Stała (MAGISTRALA) lub 4. Zmiana stanu segmentu (RF)	NIE
Klawiatura	Sygnalizuje stan ROZBROJONY	TAK	NIE
Klawiatura	Sygnalizuje stan UZBROJONY	TAK	NIE
Klawiatura	Sygnalizacja dźwiękowa alarmu	TAK	NIE
Klawiatura	Sygnalizacja dźwiękowa opóźnienia na wejście	TAK	NIE
Klawiatura	Sygnalizacja dźwiękowa opóźnienia na wyjście	TAK	NIE

Ustawienie „Domyślnego” profilu systemu przywraca wszystkie powyższe parametry do zadanych ustawień fabrycznych i zapewnia dostęp do wszystkich niedostępnych parametrów w celu wprowadzenia zmian. System alarmowy nie spełnia wówczas wymogów klasy ochronności 2, co może naruszać również wymogi ustanowione przez firmę ubezpieczeniową lub przepisy lokalne. W przypadku szkody firma ubezpieczeniowa nie musi wypłacać odszkodowania z powodu braku przestrzegania przepisów oraz nieprawidłowego programowania systemu przez firmę instalującą.

Przegląd parametrów systemu po ustawieniu „EN50131-1, klasa 2” lub „INCERT”:

Urządzenie	Parametr	Opcja	Blokowanie (ograniczenie)
Centrala alarmowa	Kody z prefiksem	TAK	TAK
Centrala alarmowa	Aktywować standard karty 125 kHz EM UNIQUE	TAK	NIE
Centrala alarmowa	Długość kodu	4 (INCERT 6)	NIE, (INCERT TAK)
Centrala alarmowa	Automatycznie sprawdzić czas w podłączonym komputerze	TAK	NIE
Centrala alarmowa	Syrena przy uzbrojeniu częściowym	NIE	NIE
Centrala alarmowa	Syreny aktywne	TAK	TAK
Centrala alarmowa	Ostrzeżenie o kodach domyślnych	TAK	TAK
Centrala alarmowa	Administrator — ograniczone prawa serwisowe / SMA	TAK	TAK
Centrala alarmowa	Serwis i SMA steruje systemem	NIE	TAK

Centrala alarmowa	Działanie próbne	NIE	NIE
Centrala alarmowa	Wymóg serwisu	NIE	NIE
Centrala alarmowa	Antynapadowa kontrola dostępu	TAK	NIE
Centrala alarmowa	Potwierdzenie alarmu w jednej strefie	NIE	NIE
Centrala alarmowa	Syrena (wyjście IW) przy aktywacji sabotażu	TAK	TAK
Centrala alarmowa	Sygnalizacja alarmu sabotażu resetowana przez Serwis	TAK	TAK
Centrala alarmowa	Reset aktywny	NIE	TAK
Centrala alarmowa	Dobowe resetowanie auto-pominięcia urządzenia	NIE	TAK
Centrala alarmowa	Blokowanie podczas uzbrajania	TAK	TAK
Centrala alarmowa	Rozbrojenie anuluje alarm	TAK	TAK
Centrala alarmowa	Niepowodzenie uzbrojenia	TAK	TAK
Centrala alarmowa	Dezaktywować auto-pominięcie z powodu problemu z urządzeniem	NIE	NIE
Centrala alarmowa	Opóźniony raport do SMA	TAK	NIE
Centrala alarmowa	Sposoby uzbrajania	Zgodnie z profilem systemu	TAK
Centrala alarmowa	Typ uwierzytelniania	Standardowy	NIE
Centrala alarmowa	Blokowanie systemu przez alarm	Nie	NIE
Centrala alarmowa	Utrata modułu MAGISTRALI	Sabotaż zawsze	NIE
Centrala alarmowa	Auto-pominięcie urządzenia	3. aktywacja	NIE
Centrala alarmowa	Długość alarmu	260	90…900 sek.
Centrala alarmowa	Opóźnienie na wejście	30	5…30 sek.
Centrala alarmowa	Opóźnienie na wyjście	30	5..60 sek.
Moduł radiowy	Wykrywanie zagłuszania RF	NISKIE	NIE
Klawiatura	Ustawienia sygnalizacji optycznej	2. Zmiana stanu strefy (MAGISTRALA) lub 4. Zmiana stanu segmentu (RF)	TAK
Klawiatura	Sygnalizuje stan ROZBROJONY	NIE	NIE
Klawiatura	Sygnalizuje stan UZBROJONY	NIE	NIE
Klawiatura	Sygnalizacja dźwiękowa alarmu	TAK	TAK
Klawiatura	Sygnalizacja dźwiękowa opóźnienia na wejście	TAK	TAK
Klawiatura	Sygnalizacja dźwiękowa opóźnienia na wyjście	TAK	TAK
Manipulatory zdalne	Ograniczenie funkcji sterowania	NIE	TAK
Kalendarz	Ograniczenia funkcji sterowania	NIE	TAK

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

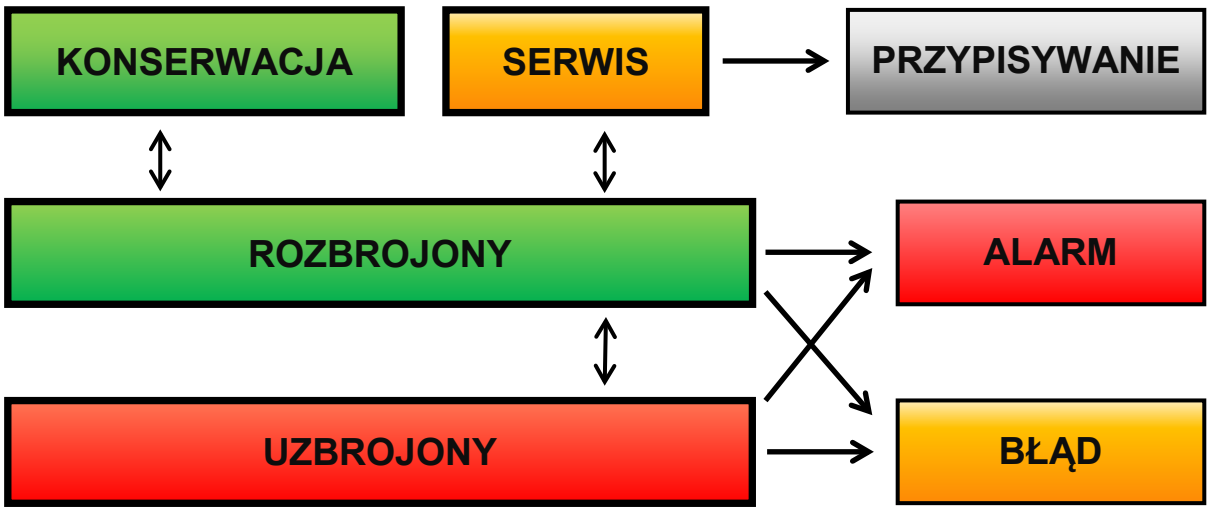
Globalny przegląd przyczyn uniemożliwiających konfigurację zgodnie z zadanym profilem systemu:

Profil / Zdarzenie	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			☑			☑
Urządzenie RF nie reaguje przez 20			☑		☑	
Błąd syreny				☑		☑
Błąd	☑		☑			☑
Utrata urządzenia	☑		☑			☑
Zablokowane czujki						
Niski poziom baterii w	☑		☑			☑
Niski poziom baterii w centrali	☑		☑			☑
Awaria baterii w centrali	☑			☑		☑
Awaria prądu stałego			☑		☑	
Awaria prądu stałego przez 30	☑		☑			☑
System w trakcie konfiguracji				☑		☑
Błąd GSM	☑		☑			☑
Błąd LAN	☑		☑			☑
Błąd PSTN	☑		☑			☑
Błąd we wszystkich SMA				☑		☑

8.2 Tryby pracy centrali alarmowej

System bezpieczeństwa posiada kilka trybów pracy. Przełączanie między trybami zależy od poziomów upoważnienia użytkowników.

Tryb	Opis
Serwis (+ 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). Segmenty na klawiaturach są wyłączone, a tryb sygnalizuje miganie żółtej diody przycisku podświetlanego (2 mignięcia co 2 sekundy). Sygnały z manipulatorów zdalnych i innych urządzeń są ignorowane. W tryb serwisowy można wejść lub go opuścić za pomocą klawiatury LCD lub programu F-Link na komputerze. W przypadku komputera połączonego z internetem nie można wejść w tryb serwisowy ani go opuścić za pomocą klawiatury.
Tryb konserwacji	Tryb przeznaczony przede wszystkim dla Administratora. Umożliwia przeprowadzenie konserwacji w strefie/strefach zgodnie z prawami dostępowymi Administratora (np. wymiana baterii w czujkach). Administrator może przełączyć system w tryb konserwacji za pomocą klawiatury lub oprogramowania J-Link. Tryb konserwacji w jednej strefie nie wpływa na stan ani funkcjonalność innych stref ani stan programowalnych wyjść PG. Tryb konserwacji sygnalizuje migający na zielono podświetlony przycisk (2 mignięcia co 2 sekundy) i zgaśnięcie przycisków segmentu w konkretnej strefie. W tryb serwisowy można wejść lub go opuścić za pomocą klawiatury LCD lub programu F-Link (J-Link) na komputerze.
Rozbrój	Zwykły tryb, w którym czujki włamania nie zapewniają ochrony. Można się swobodnie poruszać po obiekcie, otwierać okna i drzwi. Czujki dymu/temperatury, czujki wycieku gazu, czujki zalania lub przyciski panika cały czas mogą uruchomić alarm. Również styki sabotażu wszystkich urządzeń zapewniają ochronę, a w przypadku ich aktywacji system uruchamia alarm sabotażu. Tryb rozbrojenia sygnalizuje zielona kontrolka w konkretnym segmencie klawiatury.
Uzbrój (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 czerwona kontrolka (żółta kontrolka w przypadku uzbrojenia częściowego) na konkretnym segmencie.
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 przycisku podświetlonego na czerwono. Opis różnic między zachowaniem wyjścia EW i IW znajduje się w rozdziale 8.5 Rodzaje alarmów.
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.



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

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. Pozostali użytkownicy, których można dodać lub usunąć, posiadają upoważnienie z możliwością dostosowania.

Uwierzytelnienie użytkowników może mieć następującą formę:

Uwierzytelnianie kodem	Opis typu
Kod SMA	Ten kod ma najwyższy poziom uprawnień do konfiguracji zachowania systemu i jako jedyny umożliwia odblokowanie systemu po uruchomieniu 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 większą liczbę Administratorów i innych użytkowników o niższym poziomie uprawnień, a także przypisywać im kody, breloki oraz karty RFID. Pozwala on także na dostęp do kasowania alarmu i pamięci alarmów sabotażowych. Liczbę kodów SMA ogranicza wyłącznie wolne miejsce w centrali alarmowej.
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 / prawo SMA" pozostaje niezaznaczony, kod serwisowy może sterować wszystkimi strefami i wyjściami PG używanymi w systemie. Może tworzyć użytkownika o pozwoleniu SMA, innych serwisantów, Administratorów i innych użytkowników o niższym poziomie uprawnień, a także przypisywać im kody, breloki oraz karty RFID. Liczbę kodów serwisowych ogranicza wyłącznie wolne miejsce w centrali alarmowej. Domyślnie kod ma postać 1010 i nie można go skasować.
Administrator (Główny)	Może wejść w tryb konserwacji. Ten kod zawsze umożliwia pełen dostęp do wszystkich stref i ma prawo sterować wszystkimi wyjściami PG. Administrator może utworzyć innego Administratora oraz inne kody o niższym poziomie uprawnień i przypisać im dostęp do stref i wyjść PG, kody dostępu, chipy i 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. Domyślny kod fabryczny to 1234.
Administrator (Inny)	Może wejść w tryb konserwacji w przypisanych strefach. Ten kod 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 i 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 przypisanymi 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. Użytkownicy mogą zmieniać własne kody pod warunkiem, że system używa kodów z prefiksami. Wybrani użytkownicy mogą mieć dostęp do stref ograniczonych harmonogramem. Liczbę kodów użytkownika ogranicza wyłącznie wolne miejsce w centrali alarmowej. Nie ma kodu ustawionego fabrycznie.
Uzbrój	Ten kod umożliwia wyłącznie uzbrajanie wyznaczonej strefy. Użytkownicy o tym poziomie uprawnień 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 uprawnień 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 w 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 uprawnień umożliwia uzbrajanie całego systemu. Kod ochrony może rozbroić cały system wyłącznie podczas alarmu lub po jego zakończeniu, o ile 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 lub J-Link.

8.4 Opcjonalne parametry systemu

Kod z prefiksem — ta funkcja określa sposób wprowadzania wszystkich kodów dostępu podczas uwierzytelniania użytkownika. W przypadku jego aktywacji system wymaga wprowadzenia prefiksu 1- lub 3-cyfrowego, po którym następuje *. Dopiero wówczas można wprowadzić poprawny 4-, 6- lub 8-cyfrowy kod dostępu (na przykład 12*3456). W takim przypadku użytkownicy mogą wpisywać własne kody 4-cyfrowe z klawiatury LCD i dowolnie je edytować. Dezaktywacja tej funkcji powoduje, że system nie wymaga wprowadzenia prefiksu, a wyłącznie poprawnego kodu dostępu. W takim przypadku kody wszystkich użytkowników może dodawać i edytować jedynie administrator systemu. Administrator musi unikać sytuacji powielania kodu (2 użytkowników nie powinno mieć tego samego kodu).

Przestroga: *Dezaktywacja tego parametru powoduje nieodwołalne kasowanie wszystkich kodów użytkownika oraz zadanych kodów serwisowych i administratora do wartości domyślnych. Uwierzytelnianie użytkownika oraz karty i breloki RFID już skonfigurowanych użytkowników pozostają niezmienione.*

Długość kodu — aby zwiększyć poziom bezpieczeństwa systemu alarmowego podczas uwierzytelniania, można ustawić **długość kodu użytkownika** niezależnie od funkcji prefiksu. Kody mogą mieć długość 4, 6 lub 8 cyfr. Po zmianie długości kodu kody serwisowy i Administratora wracają do ustawień domyślnych (1010 i 1234), a wszystkie inne kody zostają skasowane. Kody domyślne są następujące:

Kody domyślne bez prefiksu	4-cyfrowy	6-cyfrowy	8-cyfrowy
Serwisowy:	**1010**	**101010**	**10101010**
Administrator:	**1234**	**123456**	**12345678**

Kody domyślne z prefiksem	4-cyfrowy	6-cyfrowy	8-cyfrowy
Serwisowy:	**0*1010**	**0*101010**	**0*10101010**
Administrator:	**1*1234**	**1*123456**	**1*12345678**

Aktywować standard karty 125 kHz EM UNIQUE — jeżeli nieaktywny, można używać wyłącznie kart/breloków RFID służących do identyfikacji (JA-190J, JA-191J, JA-192J, JA-194J), zalecanych przez producenta. Jeżeli aktywny, dopuszczone są także karty innych producentów, działające z powyższą częstotliwością.

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.

Ostrzeżenie o kodach domyślnych — po opuszczeniu trybu serwisowego system wysyła wiadomość SMS (pozycja 0) do serwisanta, informując, że pozostałe kody w dalszym ciągu mają ustawienie domyślne.

Usługa ograniczona do Administratora / prawa SMA — uwierzytelnienie administratora jest niezbędne, by serwisant SMA lub serwisant uzyskał dostęp do systemu. W przypadku dostępu zdalnego serwisanta do systemu za pośrednictwem programu F-Link administrator może dokonać uwierzytelnienia przy użyciu klawiatury w budynku. W przypadku połączenia lokalnego serwisanta z centralą alarmową za pomocą przewodu USB administrator może dokonać uwierzytelnienia zdalnego za pośrednictwem menu głosowego.

Serwis i SMA steruje systemem — pozwala serwisantom i serwisantom SMA sterować (Uzbrojenie / Rozbrojenie) wszystkimi strefami i wyjściami PG (WŁ./WYŁ.) wymagającymi uwierzytelnienia.

Działanie próbne — tryb specjalny używany po instalacji systemu, kiedy, niezależnie od faktycznego ustawienia długości alarmu, skraca go do 60 sekund, a wszystkie zdarzenia alarmowe są zgłaszane za pomocą wiadomości SMS określonym użytkownikom i serwisantowi (pozycja 0) pomimo, że nie aktywowano dla nich raportów alarmu. Działanie próbne automatycznie kończy się po upływie 7 dni od opuszczenia trybu serwisowego.

Wymóg serwisu — jeżeli jest aktywny, 12 miesięcy od opuszczenia trybu serwisowego na klawiaturze LCD pojawi się komunikat „Wymóg sprawdzenia systemu", a po naciśnięciu przycisku „I" wyświetli się komunikat „wezwij serwisanta" wraz z numerem telefonu (jeżeli ustawiono). Komunikat na ekranie LCD zgaśnie automatycznie, gdy serwisant uzyska zdalny dostęp do systemu. Licznik sprawdzania rocznego wyzeruje się. Wymóg serwisu można ustawić także na dokładną datę jako czynność kalendarzową w zakładce Kalendarz *(funkcję „Wymóg serwisu" Kalendarza można połączyć z automatycznym „Wymogiem serwisu" w ciągu roku po opuszczeniu trybu serwisowego).*

Antynapadowa kontrola dostępu — ta funkcja służy do aktywacji cichego alarmu panika wyłącznie przez uwierzytelnienie lub podczas sterowania systemem (uzbrajanie, rozbrajanie, PG), kiedy użytkownik jest zagrożony przez włamywacza. Alarm panika można uruchomić podczas sterowania systemem przez dodanie „1" do ostatniej cyfry kodu. Obsługuje go także kod z prefiksem lub bez niego. 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 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 — syreny z reakcją IW sygnalizują dźwiękowo alarm sabotażu w przypadku strefy rozbrojonej lub częściowo uzbrojonej. Syreny zawsze sygnalizują przy całkowitym uzbrojeniu systemu (strefy).

Sygnalizacja alarmu sabotażu resetowana przez Serwis — sygnalizację pamięci sabotażu może zresetować wyłącznie serwisant lub serwisant SMA. Jeżeli ta opcja nie jest zaznaczona, sygnalizację może zresetować także Administrator (ale nie Użytkownik).

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

Dobowe resetowanie auto-pominięcia urządzenia — opcja odnosi się wyłącznie do wejść aktywacji (nie do wejść sabotażu ani błędu). Jeżeli ta opcja jest aktywna, system automatycznie zresetuje urządzenia pominięte automatycznie, tj. codziennie o godzinie 12:00. Jeżeli ta opcja nie jest aktywna, auto-pominięcie urządzenia zostanie zresetowane wyłącznie za pomocą zmiany stanu w strefie. To zaznaczenie nadaje się np. do czujek z reakcją 24 h lub czujek zalania znajdujących się w strefie, gdzie uzbrajanie/rozbrajanie nie jest konieczne.

Blokowanie podczas uzbrajania — jeżeli jest aktywne, nastąpi blokowanie wszystkich aktywnych wejść podczas uzbrajania strefy, w okresie takiej ochrony nie mogą aktywować alarmu. Jeżeli nie jest aktywne, nastąpi czasowe pominięcie wszystkich aktywnych wejść (auto-pominięcie) do chwili ich przejścia w stan czuwania, gdy czujki wznowią ochronę (ryzyko aktywacji fałszywego alarmu, np. nieprawidłowo zamknięte okno).

Rozbrojenie anuluje alarm — funkcja, która określa, czy anulowanie alarmu nastąpi wyłącznie poprawnym kodem czy też przez rozbrojenie strefy, gdzie wystąpił alarm. Jeżeli jest aktywne, alarm można anulować przez rozbrojenie strefy, w której aktywowano alarm lub z menu klawiatury LCD przyciskiem „Anuluj ostrzeżenie".

Niepowodzenie uzbrojenia —funkcja przetwarzana podczas każdego uzbrajania. W przypadku aktywacji alarmu natychmiastowego w czasie opóźnienia na wyjście lub ciągłego otwarcia strefy z opóźnieniem po wygaśnięciu czasu na wyjście nie nastąpi uzbrojenie systemu i aktywuje się zdarzenie „Niepowodzenie uzbrajania", które zostanie zarejestrowane w historii. Informację o tym otrzyma zadany użytkownik w formie wiadomości SMS pod warunkiem, że aktywowano wysyłanie zdarzenia „SMS o niepowodzeniu uzbrajania". Sygnalizują je klawiatury oraz syrena zewnętrzna. Aby anulować sygnalizację niepowodzenia uzbrojenia, należy nacisnąć „Anuluj ostrzeżenie" w menu klawiatury LCD.

Auto-pominięcie błędu — jest dostępne jedynie, gdy wybrano jeden z profili systemu, tj. „EN50131-1" lub „INCERT". Służy do dezaktywacji ograniczonej liczby aktywowanych błędów od 3 do nieograniczonej liczby.

Sposoby uzbrajania — wybór sposobu, w jaki system realizuje uzbrajanie systemu z aktywnym urządzeniem lub błędem w systemie. Od najniższego poziomu, gdy system zawsze uzbraja się niezależnie od aktywnych urządzeń lub błędów do najwyższego poziomu, gdy 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.

Blokowanie systemu przez alarm — parametry umożliwiają blokowanie systemu po pierwszej aktywacji alarmu (włamanie lub sabotaż) w celu uniknięcia kolejnych alarmów. Odblokowanie można wykonać specjalnym kodem do Odblokowania lub za pomocą uprawnionego dostępu z SMA (dla Wielkiej Brytanii). Odblokowanie po aktywacji alarmu sabotażu może przeprowadzić także użytkownik o uprawnieniach serwisowych (dla krajów Beneluksu).

Utrata urządzenia MAGISTRALI — centrala alarmowa przetwarza utratę urządzenia lub zwarcie w MAGISTRALI systemu. Zależnie od wybranej opcji będzie reagować przez aktywację Błędu lub alarmu sabotażu dla każdego utraconego urządzenia lub ewentualnie przez aktywację alarmu sabotażu po potwierdzeniu utraty innego urządzenia.

Auto-pominięcie urządzenia — opcja odnosi się wyłącznie do wejść aktywacji, nie do wejść sabotażu ani błędu. Jeżeli funkcja jest aktywna i ustawiona na „3. aktywację", centrala alarmowa dopuszcza 3 aktywacje urządzenia w jednym okresie alarmowym. Drugą opcją jest „3. alarm", co oznacza, że obejście konkretnego urządzenia następuje dopiero po 3 okresach alarmowych, tj. urządzenie może ulegać aktywacji najwyżej 9 razy w jednym okresie strzeżenia.

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. **Naciśnięcie przycisku sabotażu urządzenia MAGISTRALI = zamknięcie pokrywy** (niektóre urządzenia można przypisać naciśnięciem przycisku, 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). Manipulatory zdalne typu JA-154Jx i JA-16xJ można przypisać naciśnięciem dowolnego przycisku. Bezprzewodowe moduły dostępowe (klawiatury) można przypisać przez naciśnięcie podświetlonego przycisku aktywacji.
   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 za pomocą optycznego czytnika 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 **Enroll not enrolled** (Przypisz nieprzypisane), co umożliwi przypisywanie urządzenia MAGISTRALI. W celu przypisania urządzenia należy dwukrotnie kliknąć wybraną pozycję.
   e. **Łączne ładowanie nieprzypisanych urządzeń MAGISTRALI** — w przypadku braku przypisania co najmniej jednego urządzenia, które jest jednak podłączone do MAGISTRALI, po naciśnięciu przycisku **Scan/add new BUS devices** (Skanuj/dodaj nowe urządzenia MAGISTRALI) nastąpi łączne przypisanie wszystkich urządzeń MAGISTRALI. Ta procedura nie pozwala określić kolejnych pozycji dla poszczególnych urządzeń.
3. Urządzenie można usunąć, usuwając jego kod produktu (zostanie usunięte całe urządzenie) lub wybierając właściwy wiersz w zakładce Urządzenia i opcję Delete (Usuń) w menu lub prawym klawiszem myszy, lub przez naciśnięcie przycisku Delete (Usuń), co usunie cały wiersz urządzenia (wraz z ustawieniami 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.

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 mają 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 nastąpi przeniesienie do tej pozycji.
- Jeżeli urządzenie zajmuje więcej niż jedną pozycję, podczas jednego przypisywania będzie automatycznie zajmować odpowiednią liczbę kolejnych pozycji (np. moduł JA-110M z dwoma wejściami alarmowymi będzie zajmować dwie pozycje). 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 znajdują się domyślnie w strefie 1. Wybór strefy można zmienić później.
- W przypadku urządzeń o wielu pozycjach, jak JA-116H, JA-118M czy JA-150M itp. można ograniczyć liczbę zajmowanych pozycji przez kasowanie odpowiednich wierszy podczas przypisywania modułu. W celu wykasowania należy kliknąć w konkretnym wierszu na żądaną pozycję (a nie przycisk w kolumnie Typ!) i nacisnąć przycisk Delete na klawiaturze komputera.

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. syrena zewnętrzna).

Natychmiastowa	Natychmiastowy alarm włamania, jeżeli uzbrojona. Jeżeli uzbrojono opóźnienie 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).
Opóźniony A	Alarm włamania z opóźnieniem na wejście/wyjście, zegar A.
Opóźniony B	Alarm włamania z opóźnieniem na wejście/wyjście, zegar B.
Opóźniony C	Alarm włamania z opóźnieniem na wejście/wyjście, zegar C. Ustawianie zegarów A, B, C — patrz zakładka Parametry. W zakładce Parametry można ustawić dla tej reakcji przedłużenie opóźnienia na wyjście przez aktywną czujkę z opóźnieniem C (np. na czas otwierania bramy garażu).
Następna opóźniona	Alarm włamania. Czujka zapewnia taki sam czas 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.
Skrócone wyjście A	Alarm włamania z opóźnieniem na wejście/wyjście, zegar A. Czas opóźnienia na wyjście skraca się do 5 sekund po wejściu aktywnej czujki w tryb czuwania.
Skrócone wyjście B	Alarm włamania z opóźnieniem na wejście/wyjście, zegar B. Czas opóźnienia na wyjście skraca się do 5 sekund po wejściu aktywnej czujki w tryb czuwania.
Skrócone wyjście C	Alarm włamania z opóźnieniem na wejście/wyjście, zegar C. Czas opóźnienia na wyjście skraca się do 5 sekund po wejściu aktywnej czujki w tryb czuwania.
Zawsze natychmiastowa	Natychmiastowy alarm włamania w przypadku uzbrojenia. Ostrzeżenia o alarmie EW i IW aktywują się jednocześnie i bezzwłocznie również podczas opóźnienia na wyjście.
Natychmiastowy/Opóźniony A	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 — patrz8.4.3 Reakcja na potwierdzone włamanie poniżej.
Opóźniony A potwierdzony	Alarm włamania z opóźnieniem na wejście i wyjście, zegar A — patrz 8.4.3Reakcja na potwierdzone włamanie poniżej.
Powtórzony natychmiastowy	Natychmiastowy alarm włamania — patrz 8.4.3 Reakcja powtórzona poniżej.
Powtórzony opóźniony A	Alarm włamania z opóźnieniem na wejście i wyjście, zegar A — patrz 8.4.3 Reakcja powtórzona poniżej.
Sabotaż	Alarm sabotażowy w dowolnym czasie (strefa nie wymaga uzbrojenia).
24 godziny	Natychmiastowy alarm włamania (strefa nie wymaga uzbrojenia).
Cicha panika	Alarm Cicha panika: 1) EW i IW nieaktywne (patrz rozdział 8.5 Types of alarms); 2) klawiatura nie wydaje sygnałów dźwiękowych, choć jest ustawiona w ten sposób; 3) jeżeli system potrafi rozpoznać, kto uruchomił Alarm panika (np. za pomocą breloka z przypisaną tożsamością użytkownika lub kodu panika 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 Rodzaje alarmów).
Alarm pożarowy	Alarm pożarowy w dowolnym czasie (strefa nie wymaga uzbrojenia).
Potwierdzenie pożaru	Alarm pożarowy w dowolnym czasie (strefa nie wymaga uzbrojenia), patrz 8.4.3

	Potwierdzona reakcja pożarowa poniżej.
Pożar, natychmiastowa	Alarm pożarowy wyłącznie w przypadku uzbrojenia danej strefy.
Gaz	Wyciek gazu w dowolnym czasie (strefa nie wymaga uzbrojenia).
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.
Raport A / B / C / D	Wysyłany jest raport specjalny (raporty specjalne A, B, C i D ustawia się w zakładce Raporty do Użytkowników), czemu może towarzyszyć komunikat głosowy. Jeżeli aktywowano zapisywanie raportów specjalnych w historii wydarzeń, raporty wysyłane są także do SMA.
Szafka na klucze	Specjalna reakcja przeznaczona dla szafki na klucz w nagłym wypadku itp., której otwarcie wyśle raport do SMA bez aktywacji alarmu z syreną.
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 wyjście.
Brak	Bez wpływu na alarm włamania. Urządzenie można jednakże wykorzystać do aktywacji wyjść PG.
Brak bez sabotażu	System reaguje na aktywację czujki wyłącznie w drodze sterowania wyjściem PG. Brak aktywacji żadnego rodzaju 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 strefy uzbrojonej, 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 rozpoczyna jedynie 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). Ta reakcja jest dostępna wyłącznie w przypadku zastosowania „Domyślnego" profilu systemu.

Potwierdzona reakcja pożarowa — w przypadku aktywacji czujki pożarowej o tej reakcji, do SMA zgłoszony jest wyłącznie niepotwierdzony alarm pożarowy, a system czeka na potwierdzenie pożaru inną czujką 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. W przypadku 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.*

Reakcja powtórzona — w przypadku aktywacji czujki o tym rodzaju reakcji system czeka, czy nastąpi ponowna aktywacja tej samej czujki. W zakładce Parametry można ustawić czas, przez który system czeka na ponowną aktywację oraz czas, przez który czujka jest pomijana. Jeżeli nie nastąpi powtórzenie aktywacji czujki w zadanym czasie (regulowanym w zakresie od 6 do 120 sekund), system anuluje pierwszą aktywację. Reakcję powtórzoną wykorzystuje się w środowisku o podwyższonym ryzyku okazjonalnych fałszywych alarmów, np. wywołanych przez gryzonie, małe owady, przeciągi itp.

Funkcja 3 aktywacji (3x i STOP!) — wszystkie czujki z aktywną reakcją alarmową na włamanie i pożar mają najwyżej trzy możliwe aktywacje centrali alarmowej podczas jednego okresu monitorowania. Po trzech aktywacjach (przy czwartym włamaniu) dla danego wejścia alarmu aktywuje się obejście, a dany czujnik

wyłącza się z dalszego działania. 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.
Tę funkcję można poszerzyć o parametr „Auto-pominięcie urządzenia", znajdujący się w zakładce Parametry, oraz o zaznaczenie „3. alarmu". Teraz z każdego urządzenia mogą nastąpić najwyżej 3 aktywacje w całym okresie najwyżej 3 alarmów. Oznacza to możliwość wysłania najwyżej dziewięciu (3 x 3) komunikatów SMS. Obejście można anulować w drodze rozbrojenia i ponownego uzbrojenia strefy. Wówczas czujka powróci w tryb strzeżenia. Obejście dla reakcji na pożar i zalanie można anulować także automatycznie o godzinie 12:00 następnego dnia (zgodnie z parametrem „Dobowe resetowania auto-pominięcia urządzenia" w zakładce Parametry). Mechanizm pominięcia na zasadzie 3x i stop nie ma zastosowania w przypadku ustawienia reakcji Panika. Liczbę aktywnych usterek można ograniczyć w podobny sposób (patrz „Auto-pominięcie usterki" w zakładce Parametry).

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 agencji ochrony. W przypadku aktywacji alarm wewnętrzny (syreny, sygnalizacja klawiatury) uruchomi się po zakończeniu opóźnienia na wejście, ale system odczeka 15 sekund przed wysłaniem raportu do SMA. Użytkownik ma 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 bezpieczeństwa polega na raportowaniu zdarzeń do właściciela i użytkowników bądź do specjalistycznej agencji ochrony, by powiadomić o zagrożeniach. Może to być włamanie, ale także pewne oddziaływanie środowiskowe, jak dym, pożar, wyciek gazu, zalanie w chronionym obiekcie. Sygnalizacja każdego rodzaju alarmu może być odmienna, zależnie od jego przyczyny. W przypadku syren alarmy dzieli się na wewnętrzne (IW) i zewnętrzne (EW).

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

	Typ alarmu					Ustawienia systemu — Parametry		Aktywuje	
Stan strefy	**Włamanie**	**Sabotaż**	**sygnałem dźwiękowy**	**Pożar**	**24 h/ Zalanie**	**Syrena IW przy uzbrojeniu częściowym**	**Syrena IW w przypadku 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**

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 ma własne ustawienia, jak ograniczenie długości alarmu, dzięki czemu można zadać krótszy czas sygnalizacji alarmu przez syrenę zewnętrzną niż przez syrenę wewnętrzną. Każdy alarm (z wyjątkiem alarmu panika) ma początek i koniec (wygaśnięcie lub anulowanie przez użytkownika), a przyczynę zdarzenia rejestruje się w zdarzeniach ze znacznikiem godziny i daty.

Na wszystkich klawiaturach systemu wszystkie alarmy (z wyjątkiem alarmu panika) sygnalizuje migający na czerwono podświetlony przycisk sygnalizacji oraz ciągła sygnalizacja dźwiękowa.

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. Gdy alarm wygaśnie, ustaje sygnalizacja na klawiaturze i za pomocą syreny. Uwierzytelnienie użytkownika wycisza sygnalizację dźwiękową wszystkich syren i klawiatur, ale nie anuluje stanu alarmowego systemu i nie rozbraja. Należy je przeprowadzić jako poniższą czynność za pomocą segmentu kontrolnego lub menu klawiatury LCD.

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 sabotażu może powodować także utrata urządzeń MAGISTRALI (np. zwarcie) lub próba złamania kodu (10x) na klawiaturze, zdalnie lub za pośrednictwem połączenia głosowego przy pomocy DTMF, wiadomości SMS lub aplikacji MyJABLOTRON (sieciowa + mobilna).

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 lub wybuchowego gazu w celu 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 za pomocą konkretnego (ukrytego lub przenośnego) przycisku panika. Zwykle za pomocą przycisku przypisanego do cichego alarmu panika, połączenia przycisków na manipulatorze zdalnym, klawiatury ze specjalnym segmentem kontrolnym przypisanym do cichego alarmu panika (w takim przypadku alarm panika może być opóźniony przy pomocy opcjonalnego zegara), naciśnięcia przycisku na syrenie wewnętrznej, wejścia na module MAGISTRALI przeznaczonego do urządzeń przewodowych lub wprowadzenia specjalnego kodu do uruchamiania cichego alarmu panika.Cichy alarm panika można także uruchomić w trakcie Antynapadowej kontroli dostępu (patrz rozdział 9.10 Sterowanie systemem przez Antynapadową kontrolę dostępu), gdzie modyfikuje się standardowy kod użytkownika.
2. **Alarm panika z sygnałem dźwiękowym** — jest to zwykłe zdarzenie alarmowe, mające początek i koniec, sygnalizowane dźwiękowo syreną i przez klawiaturę. Można go używać do sterowania stanem wyjścia PG. Przede wszystkim służy 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, zadany klawisz na manipulatorze zdalnym, 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.

Przestroga: *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 niezależnie od stanu systemu (uzbrojony lub rozbrojony) mogą mieć 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. Zależnie od stanu systemu alarm sygnalizują także syreny wewnętrzne i zewnętrzne, jak wynika z powyższej tabeli. Alarm raportuje się w ten sam sposób jak inne alarmy.

8.5.6 Anulowanie alarmu

W przypadku aktywacji alarmu w systemie jego czas trwania odlicza zegar przewidziany do długości alarmu, patrz F-Link, zakładka Parametry. Jeżeli w chronionym obiekcie jest dostępny upoważniony użytkownik, alarm można anulować w dowolnej chwili. Anulowanie alarmu powoduje natychmiastowe wyciszenie wszystkich syren i kończy raportowanie głosowe alarmu na wszystkie zdane numery telefonów. Sposób anulowania alarmu zależy od parametru w zakładce Parametry:

Rozbrojenie anuluje alarm

- Jeżeli jest aktywne, aktualnie działający alarm zostaje anulowany przez rozbrojenie strefy, gdzie występuje alarm lub po uwierzytelnieniu na klawiaturze LCD i naciśnięciu opcji „Anuluj ostrzeżenie”.
- Jeżeli nie jest aktywne, aktualnie działający alarm anuluje jedynie prawidłowe uwierzytelnienie użytkownika, posiadającego prawa dostępu do danej strefy, bez wymogu rozbrojenia takiej strefy.

8.6 Błędy systemu

Błąd jest sygnałem ostrzegawczym, pochodzącym z systemu, który sygnalizuje jakąś nieprawidłowość centrali alarmowej, komunikacji lub urządzeń. Problem może się wiązać z komunikacją radiową, za pośrednictwem GSM i LAN, maskowaniem czujek (z funkcją antymaskowania), problemami z zasilaniem (zasilanie sieciowe lub z baterii) lub zasilaniem awaryjnym. Błędy sygnalizują klawiatury systemu przy użyciu podświetlonego przycisku sygnalizacji. Raporty dotyczące błędów pochodzą z każdego źródła, a przy 4. aktywacji błędu źródło błędu zostaje pominięte, co oznacza brak zgłoszenia 4. błędu. Takie automatyczne blokowanie błędu jest parametrem opcjonalnym, patrz zakładka Parametry. Jeżeli jest aktywne, nie następuje zliczanie błędów i nie ma ograniczeń ich raportowania. Parametr nie jest dostępny, gdy ustawiono „Domyślny” profil systemu.

W poniższej tabeli znajduje się zestawienie ogólnych błędów systemu:

<table>
<tr><th>Źródło błędu</th><th>Przyczyna</th></tr>
<tr><td rowspan="2">Centrala alarmowa</td><td>Zasilanie sieciowe odłączone przez ponad 30 minut</td></tr>
<tr><td>Wadliwa bateria awaryjna lub niski poziom energii w takiej baterii w centrali alarmowej</td></tr>
<tr><td rowspan="2">Komunikator</td><td>Utrata połączenia LAN, utrata sygnału GSM lub błąd linii PSTN na co najmniej 15 minut</td></tr>
<tr><td>Zdarzenia niedostarczone do SMA w zadanym czasie</td></tr>
<tr><td rowspan="2">Moduł radiowy</td><td>Tłumienie pasma radiowego 868 MHz</td></tr>
<tr><td>Utrata komunikacji MAGISTRALI</td></tr>
<tr><td>Klawiatury</td><td rowspan="4">Utrata komunikacji radiowej lub MAGISTRALI (patrz rozdział 8.7 Błąd spowodowany utratą urządzenia poniżej)</td></tr>
<tr><td>Syreny</td></tr>
<tr><td>Moduły</td></tr>
<tr><td rowspan="2">Czujki</td></tr>
<tr><td>Maskowanie czujek ruchu (antymaskowanie)
Błąd czujki wewnętrznej (czujka wycieku gazu)
Błąd wywołany zmniejszeniem intensywności promieni podczerwonych (bariera podczerwieni)</td></tr>
</table>

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) i utracie komunikacji z centralą alarmową (brak reakcji w zadanym czasie). Wówczas system aktywuje zdarzenie „Aktywacja błędu" i zależnie od „Utraty urządzenia MAGISTRALI" może po tym następować alarm sabotażu. Jest opcjonalny i może się aktywować, gdy moduł radiowy wykryje tłumienie RF lub jakiś rodzaj zakłóceń RF trwający co najmniej 30 sekund zgodnie z poziomem wykrywania ustawionym w module radiowym. 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. W przypadku urządzeń MAGISTRALI wynosi on 8 sek., a dla bezprzewodowych 120 minut od chwili ostatniej możliwości komunikacji.

Funkcja „**Nadzór**" jest opcjonalna dla niemal wszystkich urządzeń bezprzewodowych przeznaczonych do strzeżenia (czujki, syreny, klawiatury). W przypadku niektórych z nich jest całkowicie wyłączona (manipulatory zdalne i urządzenia automatyki), natomiast np. dla niektórych urządzeń MAGISTRALI jest zawsze aktywna i nie można jej wyłączyć.

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 zostanie usunięty, system skasuje także alarm sabotażu.
- **Sabotaż po potwierdzeniu** — centrala alarmowa przetwarza utratę pierwszego urządzenia jako błąd, a jeżeli w zadanym czasie, określonym parametrem „Okres oczekiwania na potwierdzenie alarmu", wystąpi utrata kolejnego urządzenia, system potwierdzi ją 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 kilka sposobów. Podstawowe opcje sterowania to opcje lokalne lub zdalne. Inne opcje wymieniono w poniższej tabeli:

Typ	Sposób/tryb	Urządzenie	Stan	Opis sterowania
Lokalne	Klawiatura z segmentem kontrolnym	JA-114E, JA-113E, JA-154E, JA-153E, JA-123E	Moduł radiowy JA-11xR do urządzeń bezprzewodowych	Czynność można wykonać po uwierzytelnieniu użytkownika i naciśnięciu odpowiedniego segmentu kontrolnego lub za pomocą menu klawiatury LCD.
	Klawiatura	JA-110E, JA-150E	Moduł radiowy JA-11xR do urządzeń bezprzewodowych	Czynność można wykonać po uwierzytelnieniu użytkownika i naciśnięciu odpowiedniego przycisku funkcji lub za pomocą menu klawiatury LCD.
	Czytnik RFID z segmentem kontrolnym	JA-112E, JA-152E; JA-122E (tylko sterowanie z komputera)	Moduł radiowy JA-11xR do urządzeń bezprzewodowych	Obsługa jest możliwa po uwierzytelnieniu użytkownika przy pomocy breloka RFID i naciśnięciu określonego segmentu kontrolnego.
	Manipulator zdalny	JA-15xJ, JA-16xJ, JA-18xJ	Moduł radiowy JA-11xR do urządzeń bezprzewodowych	Uzbrajanie i rozbrajanie przez naciśnięcie zadanego przycisku na manipulatorze zdalnym.
	Kalendarz	Do 64 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.
	Oprogramowanie J-Link (F-Link)	Komputer z systemem Windows	Przewód USB	Za pomocą wirtualnej klawiatury można sterować strefami oraz wyjściami PG po uwierzytelnieniu.
	Moduł sterujący	JA-111H-AD TRB i JA-121T	MAGISTRALA	Systemem można sterować za pomocą dowolnego urządzenia zewnętrznego (za pomocą aktywacji przewodowego wejścia modułu lub komunikacji danych).
Zdalne	Menu głosowe	Telefon	Komunikator GSM	Ustanowienie połączenia z numerem telefonu w systemie i systemem sterowania za pomocą tonów DTMF po uwierzytelnieniu.
	Komunikat SMS	Telefon komórkowy	Komunikator GSM	Uwierzytelnione polecenie do uzbrajania lub rozbrajania stref, a także sterowania wyjściami PG.
	Ustanowienie połączenia z uprawnionego numeru telefonu	Telefon (wyłącznie sterowanie PG)	Komunikator GSM	Dla każdego uprawnionego numeru telefonu można sterować jednym konkretnym wyjściem PG.
	Aplikacja sieciowa MyJABLOTRON	Komputer	Karta SIM JABLOTRON Security w komunikatorze GSM	Po uwierzytelnieniu można sterować strefami, przeszukiwać zdjęcia wykonane za pośrednictwem urządzeń do wykonywania zdjęć, sprawdzać termometry i liczniki energii elektrycznej.
	Aplikacja mobilna MyJABLOTRON	Smartfon lub tablet	Karta SIM JABLOTRON Security w komunikatorze GSM	Po uwierzytelnieniu można sterować strefami, przeszukiwać zdjęcia wykonane za pośrednictwem urządzeń do wykonywania zdjęć, sprawdzać termometry i liczniki energii elektrycznej.
	Oprogramowanie J-Link (F-Link)	Komputer z systemem Windows	Komunikator GSM lub LAN	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). Jedynymi wyjątkami są zewnętrzne czytniki RFIS JA-122E i nawiązywanie połączenia z uprawnionego numeru telefonu, który może sterować wyjściem PG.

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 sterować żądanymi strefami lub wyjściami PG, czy też może jedynie przeglądać stan systemu i dziennik historii przy użyciu menu klawiatury LCD. Każdy użytkownik może posiadać przypisane różne opcje uwierzytelniania:

- Kod dostępu (numer 4-, 6-, lub 8-cyfrowy z prefiksem lub bez niego).
- Karta/brelok RFID (do 2 pozycji na potrzeby elementów identyfikacji RFID).
- Numer telefonu do uwierzytelnienia podczas zdalnego dostępu przez połączenie telefoniczne lub SMS.

Aby dostosować poziom bezpieczeństwa, poziom uwierzytelniania można ustawić na 3 poniższych poziomach:

1. **Standardowy** — uwierzytelnianie odbywa się przez przyłożenie karty RFID lub wprowadzenie prawidłowego kodu dostępu.
2. **Potwierdzenie karty kodem** — konieczne jest zastosowanie potwierdzenia kodu użytkownika kartą RFID (kolejność nie ma znaczenia). Jeżeli użytkownicy posiadają karty lub kody, przeprowadzą uwierzytelnienie zgodnie z opcją standardową, dzięki czemu wystarczy uwierzytelnienie na jeden ze sposobów. W przypadku dostępu zdalnego najpierw weryfikowany jest numer telefonu, a w charakterze potwierdzenia należy wprowadzić prawidłowy kod dostępu. W takim przypadku dla niektórych użytkowników o wyższym poziomie nadzoru można zastosować podwójne uwierzytelnienie, natomiast dla innych konieczne będzie uwierzytelnienie standardowe.
3. **Podwójne uwierzytelnienie** — wprowadzenie kodu użytkownika i korzystanie z karty RFID zapewni poprawne uwierzytelnienie (niezależnie od kolejności uwierzytelniania). Podczas dostępu zdalnego zawsze następuje weryfikacja numeru telefonu oraz wprowadzenia poprawnego kodu. F-Link monitoruje, czy kod i karta zostały przypisane do użytkownika w zakładce Użytkownicy (w przeciwnym razie F-Link nie pozwoli na zapisanie konfiguracji).

Przestroga: *Potwierdzenie kodu użytkownika kartą RFID zmniejsza ryzyko nieuprawnionej obsługi lub obejścia systemu przez osobę trzecią.*

9.2 Sterowanie systemem z klawiatury

9.2.1 Sterowanie systemem z klawiatur segmentowych

Najlepszym sposobem sterowania systemem bezpieczeństwa i monitorowania go jest korzystanie z klawiatury systemu, gdzie dzięki kolorowej sygnalizacji głównego przycisku sterującego można sprawdzać błędy i alarmy, zaś przy pomocy innych segmentów kontrolnych można sterować strefami i wyjściami PG, a także kontrolować opcje systemu, jak sygnalizacja pamięci alarmów, aktywacja alarmu panika lub problemy zdrowotne. Przy pomocy klawiatury LCD można przeglądać menu wewnętrzne, aby uzyskać informacje na temat błędów, zdarzeń, czujek aktywnych lub pominiętych bądź czujek uniemożliwiających uzbrojenie systemu, zawsze po określonym uwierzytelnieniu. Brak uwierzytelnienia = brak dostępu do menu klawiatury, zależnie od ustawień danej klawiatury można wyłączyć widoczność konkretnych segmentów, co chroni system przed obsługą przez osoby nieuprawnione.

Najbardziej podstawową funkcją klawiatury systemu jest uzbrajanie i rozbrajanie stref. System można uzbroić całkowicie lub częściowo. Systemem można sterować z menu klawiatury LCD lub segmentów kontrolnych. Przy pomocy segmentów można przeprowadzić uzbrojenie zgodnie z ich ustawieniami: całkowicie lub częściowo i z uwierzytelnieniem (w historii zdarzeń rejestruje się, kto przeprowadził uzbrojenie konkretnej strefy) lub bez niego (brak wymaganego kodu, w historii zdarzeń nie określa się, kto uzbroił system). Do rozbrojenia systemu zawsze konieczne jest uwierzytelnienie w systemie, w związku z tym w historii zdarzeń rejestruje się, kto rozbroił system.

Procedurę uzbrajania można przeprowadzić na dwa poniższe sposoby:

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

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. Całkowicie uzbrojony system/strefę sygnalizuje podświetlony na czerwono segment kontrolny lub wypełniony kwadrat z numerem strefy na klawiaturze LCD.

2. Uzbrojenie częściowe, użytkownik pozostaje w obiekcie:

Kiedy system jest uzbrojony częściowo, użytkownik pozostaje w chronionym obiekcie, a strzeżenie obejmuje wyłącznie ochronę terenu (zapewnia swobodny ruch wewnątrz obiektu). 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 manipulatorem zdalnym, menu głosowym, wiadomością SMS lub za pomocą aplikacji MyJABLOTRON. W tym przypadku czujki mają zadaną reakcję natychmiastową / opóźnioną A.

Uzbrojenie częściowe sygnalizuje żółte podświetlenie segmentu lub kwadrat wokół cyfry na wyświetlaczu klawiatury LCD.

Sterowanie systemem z klawiatury — procedura:

System oferuje kilka profili systemu spełniających różne wymogi norm. Zmienia także zachowanie klawiatury oraz, rzecz jasna, sposób sterowania nią. Systemem można sterować na dwa sposoby:

1. Wariant 1 sterowania systemem (obowiązuje dla wszystkich profili)

Uzbrajanie systemu:

Używanie **wariantu 1 wymaga wcześniejszego uwierzytelnienia**, ponieważ nie wszystkie segmenty muszą pokazywać swój stan zależnie od swych ustawień bez uwierzytelnienia!

1. Przyłożenie karty/breloka RFID lub wprowadzenie kodu umożliwia uwierzytelnienie (w przypadku gdy wymagany jest zarówno kod, jak i karta ich kolejność nie ma znaczenia).
2. Strefę rozbrojoną sygnalizuje zielona kontrolka po lewej stronie segmentu.
3. Naciśnięcie czerwonego przycisku segmentu z prawej strony skutkuje żądaniem uzbrojenia systemu. Zależnie od liczby wykorzystanych segmentów można wybrać większą liczbę żądań.
4. Jeżeli po dokonaniu wyboru będzie migać czerwona lub żółta dioda (8 sekund), system wykrywa przeszkodę uniemożliwiającą uzbrojenie (patrz rozdział 9.11 Obstacles preventing setting the system).
5. Udane uzbrojenie lub uzbrojenie częściowe potwierdzają czerwone lub żółte kontrolki segmentu.

Rozbrajanie systemu:

W celu sterowania systemem z klawiatury dla **wariantu 1 konieczne jest uwierzytelnienie**!

1. Przyłożenie karty/breloka RFID lub wprowadzenie kodu umożliwia uwierzytelnienie (w przypadku gdy wymagany jest zarówno kod, jak i karta ich kolejność nie ma znaczenia).
2. Uzbrojoną strefę sygnalizuje czerwona lub żółta kontrolka z prawej strony segmentu. W przypadku wykrycia włamania do chronionego obiektu aktywuje opóźnienie na wejście sygnalizowane szybkim miganiem zielonej diody.
3. Naciśnięcie zielonego przycisku (lub kolejno kilku przycisków) z lewej strony przesyła żądanie rozbrojenia strefy.
4. Pomyślne rozbrojenie potwierdzają zielone kontrolki segmentu.
5. Jeżeli po rozbrojeniu strefy nie ustaje szybkie miganie kontrolki, sygnalizuje to pamięć alarmów w strefie. Tę sygnalizację można anulować kolejnym naciśnięciem zielonego przycisku w segmencie z uprawnieniem do anulowania takiej sygnalizacji lub wykorzystaniem menu klawiatury LCD i wyborem opcji „Anulowanie ostrzeżenia”.

2. Wariant 2 sterowania systemem (profil „Domyślny")

Uzbrajanie systemu:

Sposób sterowania opiera się na procedurze „wybierz żądane działanie i uwierzytelnij się".

1. Strefę rozbrojoną sygnalizuje zielona kontrolka po lewej stronie segmentu.
2. Naciśnięcie czerwonego przycisku segmentu z prawej strony skutkuje żądaniem uzbrojenia systemu. Zależnie od liczby wykorzystanych segmentów można wybrać większą liczbę żądań.
3. Jeżeli do uzbrojenia strefy konieczne jest uwierzytelnienie, powoli migająca czerwona (uzbrojenie całkowite) lub żółta (uzbrojenie częściowe) kontrolka 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 dokonaniu wyboru 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 uzbrojenie lub uzbrojenie częściowe potwierdzają czerwone lub żółte kontrolki segmentu.

Rozbrajanie systemu:

1. Uzbrojoną strefę sygnalizuje czerwona lub żółta kontrolka z prawej strony segmentu. W przypadku wykrycia włamania do chronionego obiektu aktywuje opóźnienie na wejście sygnalizowane szybkim miganiem odpowiedniej kontrolki.
2. Naciśnięcie zielonego przycisku (lub kolejno większej liczby przycisków) z lewej strony przekazuje żądanie rozbrojenia strefy, a segment powolnym miganiem sygnalizuje czas pozostały do uwierzytelnienia.
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. Pomyślne rozbrojenie potwierdzają zielone kontrolki segmentu.
5. Jeżeli po rozbrojeniu strefy nie ustaje szybkie miganie kontrolki, sygnalizuje to pamięć alarmów w strefie. Sygnalizację można skasować kolejnym naciśnięciem zielonego przycisku w segmencie z uprawnieniami do kasowania takiej sygnalizacji lub przy pomocy menu klawiatury, gdzie należy wybrać opcję „Anuluj ostrzeżenie".

9.2.2 Sterowanie systemem za pomocą klawiatur JA-110E i JA-150E

Najlepszy sposób sterowania systemem bezpieczeństwa i jego monitorowania polega na wykorzystaniu klawiatury systemu, gdzie dzięki kolorowej kontrolce stanu systemu na głównym przycisku sterowania zawsze można sprawdzić błędy i alarmy. Przy użyciu innych przycisków funkcji można sterować stanem 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.

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 uzbrajaniu może nastąpić uwierzytelnienie (w historii rejestrowane jest, kto uzbroił strefę) lub uwierzytelnienia może nie być (kod nie jest konieczny, w związku z czym w historii nie określa się, kto przeprowadził uzbrojenie strefy). Podczas rozbrajania systemu przyciskami funkcji uwierzytelnienie jest zawsze konieczne, by w pamięci centrali alarmowej zarejestrować, kto rozbrajał strefę.
2. Z menu klawiatury — nacisnąć „*" po uwierzytelnieniu i uzbroić częściowo, całkowicie lub rozbroić.
3. W drodze samego uwierzytelnienia — uwzględniając ustawienia, można uzbroić (jedynie) całkowicie lub rozbroić wyłącznie za pomocą uwierzytelnienia z kodem lub za pomocą 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):**

Całkowicie uzbrojony system sygnalizuje podświetlony na czerwono przycisk funkcji lub w pełni podświetlony numer strefy na wyświetlaczu LCD klawiatury podczas sterowania z 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:**

Częściowo uzbrojony system sygnalizuje podświetlony na żółto przycisk funkcji lub w pełni podświetlony numer strefy na wyświetlaczu LCD klawiatury podczas sterowania z menu.

Kiedy system jest uzbrojony częściowo, użytkownik pozostaje w chronionym obiekcie, a strzeżenie obejmuje wyłącznie ochronę terenu (zapewnia swobodny ruch wewnątrz obiektu). Istnieją dwa warianty sterowania:

1. Sterowanie za pomocą klawiatury umieszczonej wewnątrz chronionego obiektu z ochroną terenu (hol wejściowy itp.). Wszystkie czujki w holu wejściowym należy ustawić na reakcję Zdalną, aby zapewnić, że po uzbrojeniu systemu aktywują się one po upływie pewnego czasu od wejścia w celu rozbrojenia systemu.
2. 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 mają zadaną reakcję natychmiastową / opóźnioną A.

Sterowanie systemem z klawiatury — procedura:

System oferuje kilka profili systemu spełniających różne wymogi norm. Zmienia także zachowanie klawiatury oraz, rzecz jasna, sposób sterowania nią.

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 dokonaniu wyboru przycisk funkcji nie przestanie migać na czerwono lub żółto (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 systemu:

1. Uzbrojoną strefę sygnalizuje przycisk funkcji świecący na czerwono lub żółto. W przypadku wykrycia włamania do chronionego obiektu aktywuje opóźnienie na wejście sygnalizowane szybkim miganiem 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".

Podświetlony przycisk sygnalizacyjny na klawiaturze — przegląd stanów:

Przycisk podświetlony na zielono	Zwykła praca. Strefy sterowane za pomocą klawiatury są OK, bez błędów.
Przycisk podświetlony na żółto	Zwykła praca, w niektórych sterowanych strefach wykryto błąd. Po uwierzytelnieniu użytkownika na podstawie praw dostępu za pomocą menu klawiatury LCD można uzyskać bardziej szczegółowe informacje. Jeżeli po błędzie na klawiaturze LCD pojawi się obracające się logo JABLOTRON, oznacza to błąd komunikacji radiowej między centralą alarmową a klawiaturą.
Przycisk podświetlony na czerwono	Klawiatura w trybie ROZRUCHU podczas aktualizacji oprogramowania.
Przycisk miga na zielono (2 Hz)	Dokonano uwierzytelnienia, użytkownik może zmienić stan systemu z segmentów lub przeszukując menu klawiatury LCD. Czas na uwierzytelnienie wynosi 8 sekund od ostatniego naciśnięcia przycisku. Można go anulować klawiszem ESC.
Przycisk miga na żółto (8 Hz)	Ostrzeżenie o nieudanym uzbrajaniu.
Przycisk miga na czerwono (8 Hz)	Sygnalizacja aktualnie uruchomionego alarmu w konkretnej strefie na klawiaturze. Rodzaj alarmu, nazwa strefy, w której doszło do uruchomienia alarmu oraz źródło uruchomionego alarmu są widoczne na klawiaturze LCD.
Miga naprzemiennie na czerwono/żółto	Uruchomiony alarm z aktywnym błędem.
Miga naprzemiennie na zielono/czerwono	Uwierzytelnienie z aktualnie aktywnym alarmem lub pamięcią alarmów.
Miga naprzemiennie na zielono/żółto	Uwierzytelnienie z aktywnym błędem.
Przycisk miga na żółto (2x co 2 sekundy)	Programowanie / Tryb serwisowy. Cała sygnalizacja segmentu kontrolnego jest wyłączona dla użytkowników, podobnie jak menu klawiatury Administratora. Menu klawiatury jest dostępne wyłącznie dla serwisanta pod warunkiem podłączenia komputera do centrali alarmowej.
Przycisk miga na czerwono (2 x co 2 sekundy)	Sygnalizacja pamięci alarmów.
Przycisk miga na zielono (2x co 2 sekundy)	Tryb konserwacji. Sygnalizacja segmentu kontrolnego jest nieaktywna dla stref przełączonych w tryb konserwacji.
Przycisk miga na żółto (1x co 2 sekundy)	Sygnalizacja błędu na klawiaturze w trybie uśpienia (dotyczy jedynie profilu EN50131-1).
Przycisk miga na czerwono (1x co 2 sekundy)	Sygnalizacja pamięci alarmów na klawiaturze w trybie uśpienia (dotyczy jedynie profilu EN50131-1).
Brak sygnalizacji	Klawiatura w trybie uśpienia.

Przegląd sygnalizacji optycznej segmentu kontrolnego klawiatury:

Segment świeci na zielono	Stan strefy to Rozbrojona lub Wyjście PG WYŁ.
Segment miga na zielono (4 Hz)	Trwa opóźnienie na wejście i system oczekuje na uwierzytelnienie, aby móc dokonać rozbrojenia.
Segment świeci na żółto	Stan strefy to Częściowo uzbrojona.
Segment świeci na czerwono	Stan strefy to Uzbrojona lub Wyjście PG WŁ.
Segment miga na żółto (4 Hz)	System oczekuje na uwierzytelnienie w przypadku częściowego uzbrojenia lub zgłasza błąd podczas częściowego uzbrojenia.
Segment miga na żółto (8 Hz)	Ostrzeżenie o nieudanym uzbrajaniu.
Segment miga na czerwono (4 Hz)	System oczekuje na uwierzytelnienie podczas uzbrajania lub zgłasza problem podczas uzbrajania.
Segment miga na czerwono (8 Hz)	Sygnalizacja pamięci alarmów trwa do chwili anulowania.
Segment nie świeci	Wyłączony, Tryb serwisowy lub konserwacji 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. Wymaga przypisania modułu radiowego JA-11xR do systemu w celu komunikacji z urządzeniami bezprzewodowymi. Należy go umieścić w odpowiednim miejscu, by zapewnić niezawodną komunikację z manipulatorem zdalnym przy uwzględnieniu wymaganej odległości roboczej.

W przypadku korzystania z manipulatorów zdalnych (JA-15xJ, JA-16xJ) ich przyciski zachowują się tak samo jak segmenty kontrolne klawiatury. Każdy przycisk może sterować wybraną strefą (przycisk z prawej strony zawsze uzbraja, natomiast przycisk z lewej strony zawsze rozbraja). Manipulatory zdalne przestrzegają zasad uzbrojenia systemu, w związku z tym w przypadku jakichkolwiek przeszkód uniemożliwiających uzbrojenie nie można uzbroić systemu.

Segmenty kontrolne klawiatury i dwukierunkowe manipulatory zdalne mają ten sam sposób sygnalizacji za pomocą trzech kolorów kontrolek. Opisy poszczególnych stanów podano w poniższej tabeli:

Sygnalizacja stanu dwukierunkowych manipulatorów zdalnych (JA-15xJ) — wyświetlona po naciśnięciu:

Kontrolka świeci na zielono	Stan strefy to Rozbrojona lub Wyjście PG WYŁ.
Kontrolka świeci na żółto	Stan strefy to Częściowo uzbrojona
Kontrolka świeci na czerwono	Stan strefy to Uzbrojona lub Wyjście PG WŁ.
Kontrolka miga na czerwono	W strefie występuje przeszkoda uniemożliwiająca uzbrojenie
Kontrolka miga na żółto	Nieznany stan polecenia (błąd komunikacji, poza zasięgiem komunikacji itp.)

Przy pomocy jednokierunkowego manipulatora zdalnego (JA-16xJ, JA-18xJ) można sterować systemem w ten sam sposób. System za pomocą kontrolki sygnalizuje naciśnięcie przycisku i wysłanie polecenia. Nie ma odpowiedzi z centrali alarmowej, a użytkownik powinien wykorzystać inny rodzaj sygnalizacji stanu do potwierdzenia zmiany stanu 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 można ustawić na najwyżej 64 czynności kalendarza — sterowanie strefami i wyjściami PG. Za pomocą kalendarza można wybrać dokładną datę rocznego przeglądu serwisowego, niezależną od opcji „Wymóg serwisu” w zakładce Parametry.

Dla każdego działania można ustawić dzień tygodnia i miesiąca, a także miesiąc roku, gdy nastąpi realizacja. Tym samym działanie można ustawić od jednego, konkretnego dnia w roku do regularnych powtórzeń w określone dni (np. co tydzień lub co miesiąc). W wybrane dni można ustawić najwyżej 4 przypadki realizacji czynności kalendarzowej lub można wybrać jej powtarzanie w regularnych odstępach czasu. Częstotliwość powtarzania można dodatkowo określić jako „od–do”. Do typowych zastosowań należy automatyczne uzbrajanie strefy w sklepach, częściowe uzbrajanie budynku w nocy lub sterowanie oświetleniem w godzinach nocnych. Każde automatyczne zdarzenie rejestruje się w dzienniku historii z nazwą źródła wskazaną jako „Kalendarz”.

Opcje sterowania kalendarzem związane ze strzeżeniem:

Rozbrój	Rozbrajanie zadanej strefy z dowolnego poziomu strzeżenia (uzbrojenie całkowite lub częściowe).
Częściowo uzbrojona	Częściowo uzbraja zadane strefy i zaczyna od czasu opóźnienia na wyjście z brzęczykiem trwającym 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej). 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 opisano w Zakładka Parametry). Centrala alarmowa w pełni przestrzega zasad uzbrajania i sprawdzania gotowości systemów do uzbrojenia.

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 automatycznym zegarem. 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. 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	Częściowo uzbraja zadane strefy i zaczyna od czasu opóźnienia na wyjście z brzęczykiem trwającym 180 sekund (niezależnie od długości czasu na wyjście ustawionego w centrali alarmowej). W tym czasie wszystkie strefy alarmowe zachowują się jak strefa 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. System zostaje uzbrojony natychmiast, w związku z czym nie jest możliwy ruch w chronionym obiekcie. 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.
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 czynnością z kalendarza „Odblokuj PG”. Wejście do trybu serwisowego lub jego opuszczenie nie odblokowuje go.
Odblokuj PG	Odblokowuje blokadę zadanych wyjść PG.
Nie	Nie zadano funkcji blokowania.
Wymóg serwisu	W zadanym czasie w systemie uruchamia się zdarzenie „System wymaga przeglądu serwisowego”, co wyświetla się wraz z ikoną Informacja na klawiaturach z ekranem LCD.

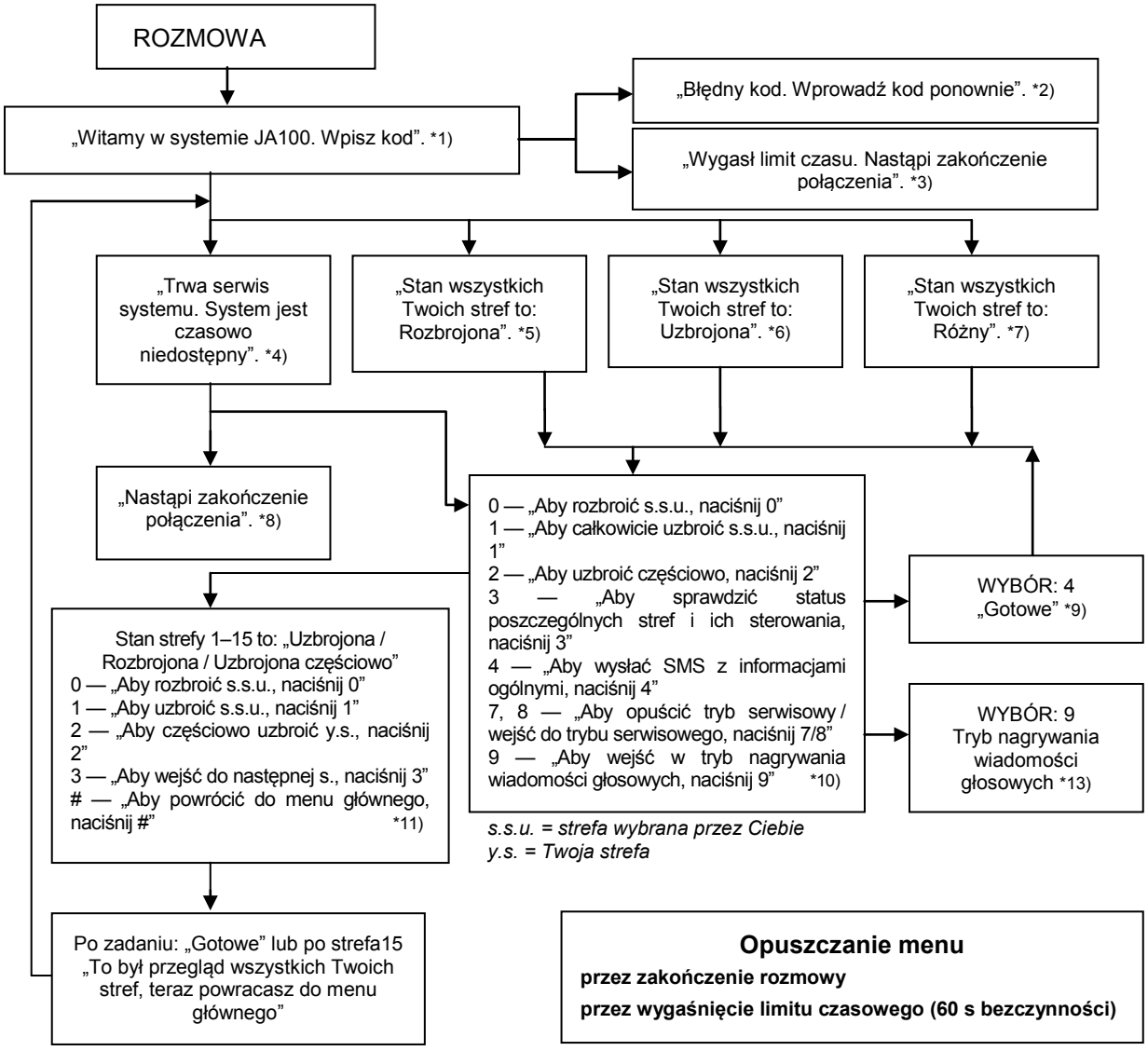
Zadanie blokowania funkcji przy użyciu kalendarza: Każdą czynność z kalendarza można zablokować za pomocą wybranych wyjść PG. Blokowanie oznacza: kiedy wyjście PG jest aktywne, nie dojdzie do realizacji konkretnej czynności w zadanym czasie.

9.5 Sterowanie systemem za pośrednictwem menu głosowego komunikatora (GSM)

Jeżeli w centrali alarmowej zainstalowano komunikator GSM JA-19xY, systemem bezpieczeństwa można sterować zdalnie dzięki wdrożonemu menu głosowemu i tonom DTMF na telefonie komórkowym dzwoniącego. W przypadku nawiązania połączenia z używanym numerem telefonu z kartą SIM system odbiera 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 stan całego systemu i zależnie od uprawnień dzwoniącego oferuje inne opcje sterowania. Parametr „Brak kodu do menu głosowego i SMS" w zakładce Komunikacja umożliwia użytkownikowi uwierzytelnienie zgodnie z zadanym numerem telefonu zapisanym na wykazie Użytkowników. W takim przypadku kod nie jest konieczny. 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.

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

Przegląd menu głosowego:



*1) Odpowiada po 3 sygnałach. Liczbę sygnałów do chwili odebrania (1.10) można ustawić w zakładce Komunikacja oraz zakładce odpowiedniego komunikatora, gdzie może być możliwe wejście do menu głosowego 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 stanu 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 (*)".
2 (3, 4, 5) — „Aby zarejestrować komunikaty raportu A (B, C, D), naciśnij 2 (3, 4, 5)", a potem „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 do sprawdzania stanu.
- 2 — „Wymagane zgłoszenie ważnej wiadomości, połączenie zostanie zakończone w ciągu 30 sekund" — raporty / ważne wiadomości do SMA mają priorytet względem aktualnego menu głosowego.
- Wejście w tryb rejestrowania jest sygnalizowane piknięciem. Zarejestrowany komunikat zostanie odtworzony tuż po jego nagraniu.
- Jeżeli nie są Państwo zadowoleni z nagrania, można natychmiast wybrać ponowne nagrywanie.
- Zaleca się rozpoczęcie nagrywania bezpośrednio po sygnale dźwiękowym, a tuż 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

Jeżeli w centrali alarmowej zainstalowany jest komunikator GSM JA-19xY, systemem można sterować za pomocą poleceń SMS. Polecenia SMS można wykorzystać do sterowania stanami uzbrojenia poszczególnych stref lub całego systemu (uzbrajanie, rozbrajanie) lub zadawania pytań o ich stan. Za pomocą poleceń SMS można sterować także wyjściami PG. Nie ma poleceń fabrycznych do sterowania wyjściami PG, należy je najpierw skonfigurować. Treści poleceń nie można zmieniać, z wyjątkiem poleceń do sterowania wyjściami PG.

Struktura polecenia:

ppp*cccc_polecenie

gdzie: **ppp** to numer pozycji kodu użytkownika (wyłącznie w przypadku kodu z prefiksem),

***** to separator (* jest niezbędna wyłącznie w przypadku kodu z prefiksem),

cccc to kod użytkownika,

_ to odstęp rozdzielający (pusty znak),

polecenie oznacza polecenie wykonawcze (patrz wykaz poleceń poniżej).

Polecenia zapytania:

Informacje o stanie systemu można uzyskać także przy użyciu następujących poleceń:

DINFO, STATUS, COM i GSM

Polecenie sterowania:

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

UZBRÓJ, ROZBRÓJ, lub UZBRÓJ x x x, ROZBRÓJ x x x, gdzie x to numery stref oddzielone spacją.

Polecenie do sterowania **wyjściami PG** są zadane fabrycznie jako **Wł. wyjście PG x** (x = 1 – 128).

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

Przegląd poleceń:

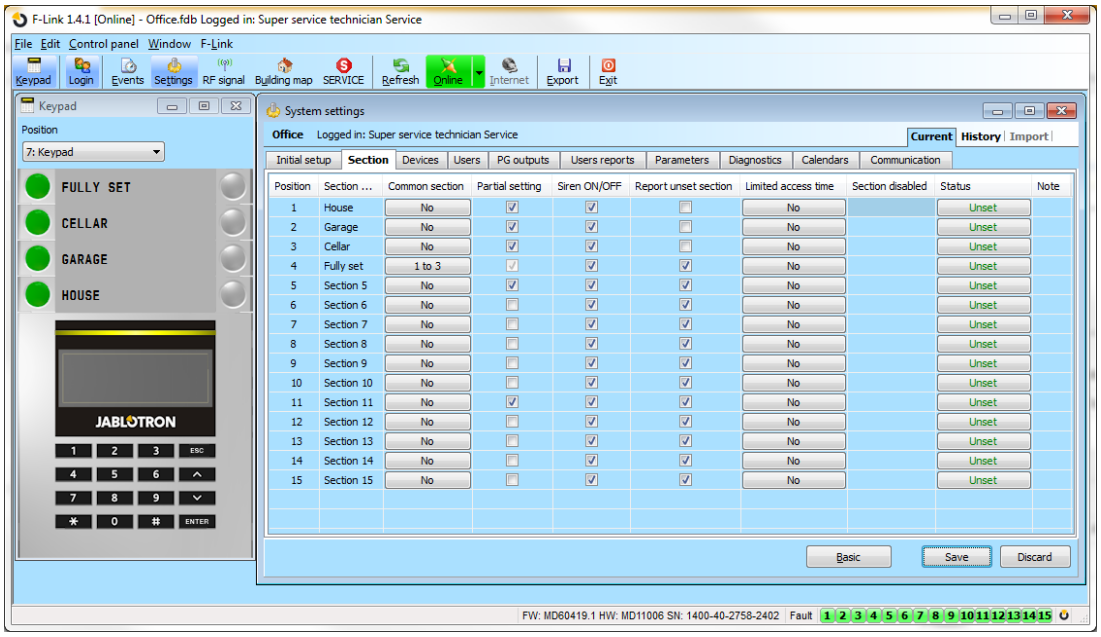
Polecenie sterowania	Uwierzytelnianie	Odpowiedź (próbka)	Uwaga
DINFO (podstawowe informacje o instalacji)	Serwis, Administrator	JABLOTRON 100+: TYP: JA-103K, Numer seryjny: 14004026532523, Oprogramowanie: LJ60418, Sprzęt: LJ16117, RC: C5U6G-215CP-D2A6, GSM: 90%, GPRS: Ok, LAN: wył. Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Typ centrali alarmowej Numer seryjny Wersja firmware Wersja sprzętu Kod rejestracji komunikatora GSM Sygnał GSM, dostępność danych GPRS Stan połączenia LAN (OK lub WYŁ) Data i godzina przekazania SMS do sieci GSM
STATUS (stan stref)	Serwis, Administrator, Użytkownik (Jeżeli użytkownik posiada dostęp jedynie do niektórych stref, zostanie zwrócony stan stref, do których ma dostęp).	JABLOTRON 100+: Stan: Strefa 1: Rozbrojona; Strefa 2: Uzbrojona; Strefa 3: Rozbrojona; Strefa 4: Uzbrojona, Błąd; Strefa 5: Uzbrojona; Strefa 6: Uzbrojona; Strefa 7: Rozbrojona; Strefa 8: Rozbrojona; GSM: 90%; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Stan: Nazwa i stan Strefy 1 Nazwa i stan Strefy 2 Nazwa i stan Strefy 3 Nazwa i stan Strefy 4 Nazwa i stan Strefy 5 Nazwa i stan Strefy 6 Nazwa i stan Strefy 7 Nazwa i stan Strefy 8 Jakość sygnału GSM Data i godzina przekazania SMS do sieci GSM
COM (informacje dot. komunikacji)	Serwis	JABLOTRON 100+: GSM: 90%, DANE: ok, CELLID: 44905, OPID: 23003, LAN: ok, MAC: hh:hh:hh:hh:hh:hh, PSTN: wył., SMA: 1:ok, 2:ok, 3:wył., 4:ok, 5:wył., Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Jakość sygnału GSM, dostępność danych GPRS Numer telefonu komórkowego i operator zapewniający połączenie GSM Stan połączenia LAN i adres MAC Stan połączenia linii telefonicznej (możliwy w przypadku JA-190X) Stan aktywacji transmisji do poszczególnych, możliwych SMA Data i godzina przekazania SMS do sieci GSM
GSM (ponowne uruchomienie GSM)	Serwis, Administrator, Użytkownik	JABLOTRON 100+: SMS przetworzony OK: GSM; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Potwierdzenie dostarczenia SMS (przed ponownym uruchomieniem) Data i godzina przekazania SMS do sieci GSM

UZBROJONY (sterowanie całym systemem)	(Zgodnie z używanym kodem)	JABLOTRON 100+: Stan: Strefa 1: Uzbrojona; Strefa 2: Uzbrojona; Strefa 3: Uzbrojona; Strefa 4: Uzbrojona, Błąd; Strefa 5: Uzbrojona; Strefa 6: Uzbrojona; Strefa 7: Uzbrojona ze strefą aktywną; Strefa 8: Uzbrojona ze strefą aktywną; GSM: 90%; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Stan: Nazwa i stan Strefy 1 Nazwa i stan Strefy 2 Nazwa i stan Strefy 3 Nazwa i stan Strefy 4 Nazwa i stan Strefy 5 Nazwa i stan Strefy 6 Nazwa i stan Strefy 7 Nazwa i stan Strefy 8 Jakość sygnału GSM Data i godzina przekazania SMS do sieci GSM
ROZBROJONY (sterowanie całym systemem)	(Zgodnie z używanym kodem)	JABLOTRON 100+: Stan: Strefa 1: Rozbrojona; Strefa 2: Rozbrojona; Strefa 3: Rozbrojona; Strefa 4: Rozbrojona, Błąd; Strefa 5: Rozbrojona; Strefa 6: Rozbrojona; Strefa 7: Rozbrojona; Strefa 8: Rozbrojona; GSM: 90%; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Stan: Nazwa i stan Strefy 1 Nazwa i stan Strefy 2 Nazwa i stan Strefy 3 Nazwa i stan Strefy 4 Nazwa i stan Strefy 5 Nazwa i stan Strefy 6 Nazwa i stan Strefy 7 Nazwa i stan Strefy 8 Jakość sygnału GSM Data i godzina przekazania SMS do sieci GSM
UZBRÓJ 1 3 5 7 (sterowanie wybranymi strefami w systemie)	(Zgodnie z używanym kodem)	JABLOTRON 100+: Stan: Strefa 1: Uzbrojona; Strefa 3: Uzbrojona; Strefa 5: Uzbrojona; Strefa 7: Uzbrojona ze strefą aktywną; GSM: 90%; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Stan: Nazwa i stan Strefy 1 Nazwa i stan Strefy 3 Nazwa i stan Strefy 5 Nazwa i stan Strefy 7 Jakość sygnału GSM Data i godzina przekazania SMS do GSM
ROZBRÓJ 2 4 6 8 (sterowanie wybranymi strefami w systemie)	(Zgodnie z używanym kodem)	JABLOTRON 100+: Stan: Strefa 2: Rozbrojona; Strefa 4: Rozbrojona; GSM: 90%; Godzina 17:01 22.7.	Nazwa instalacji jako zakładka Konfiguracja początkowa Stan: Nazwa i stan Strefy 2 Nazwa i stan Strefy 4 Jakość sygnału GSM Data i godzina przekazania SMS do GSM

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

9.7 Sterowanie systemem za pośrednictwem programu F-Link lub J-Link

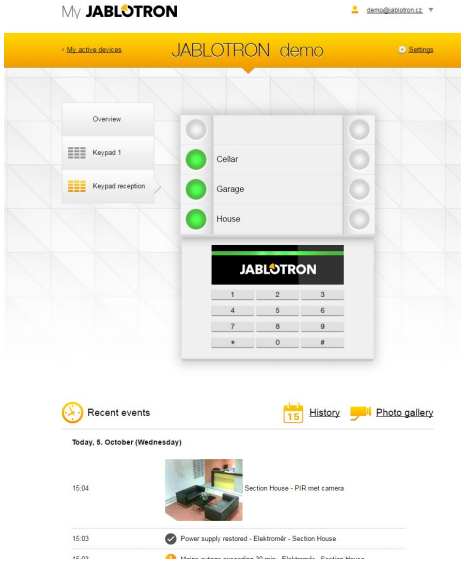
Program F-Link i J-Link służy do lokalnego i zdalnego programowania całego systemu lub edycji przez użytkownika. Zapewnia przegląd stanów stref i sterowanie strefami. Strefami i wyjściami PG można sterować przy użyciu segmentów wirtualnej klawiatury zgodnie z konfiguracją klawiatur obecnych fizycznie w systemie. Sterowanie jest możliwe także z zakładki „Strefa" w kolumnie „stan" lub z dolnego paska stanu. System rejestruje sterowanie systemem zgodnie z uprawnieniami po uwierzytelnieniu użytkownika w programie.



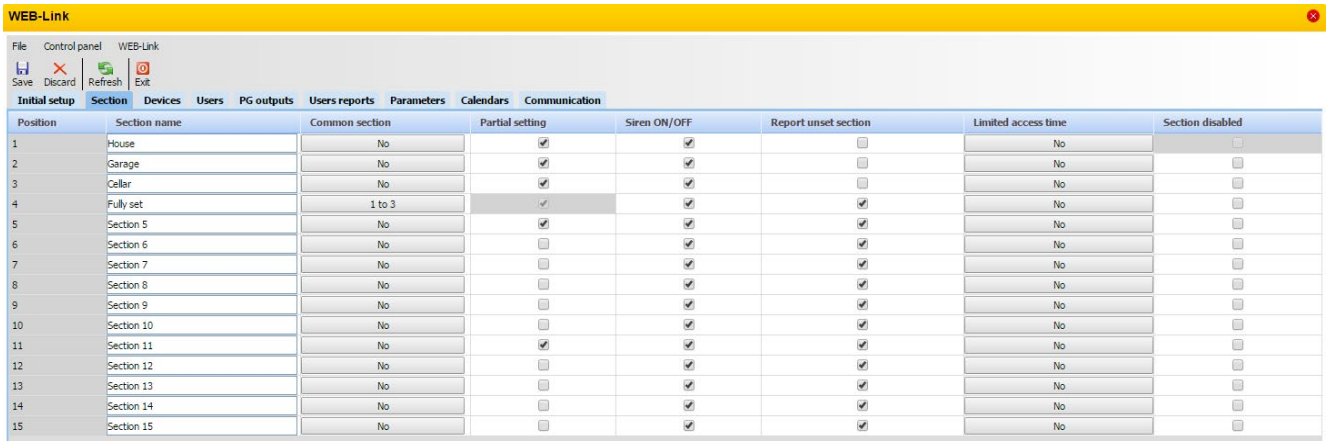
9.8 Sterowanie systemem za pomocą aplikacji sieciowej MyJABLOTRON

Zdalne sterowanie przy pomocy aplikacji sieciowej MyJABLOTRON jest najbardziej przyjaznym dla użytkownika sposobem sterowania systemem bezpieczeństwa 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 konfigurować wiadomości informujące o zdarzeniach w systemie lub przekroczeniu wartości zadanych przez użytkownika.

Przy każdym logowaniu w celu sterowania systemem należy dokonać uwierzytelnienia przy pomocy kodu użytkownika. Uzbrajanie stref przy pomocy segmentów przebiega identycznie jak ich faktyczna konfiguracja. Jeżeli segmenty umożliwiają uzbrojenie częściowe, można zdalnie uzbroić system częściowo. We wszystkich innych przypadkach sterowanie przy użyciu listy zawsze uzbraja całe strefy. Bardziej szczegółowe informacje znajdują się w rozdziale 14 MyJABLOTRON web application.

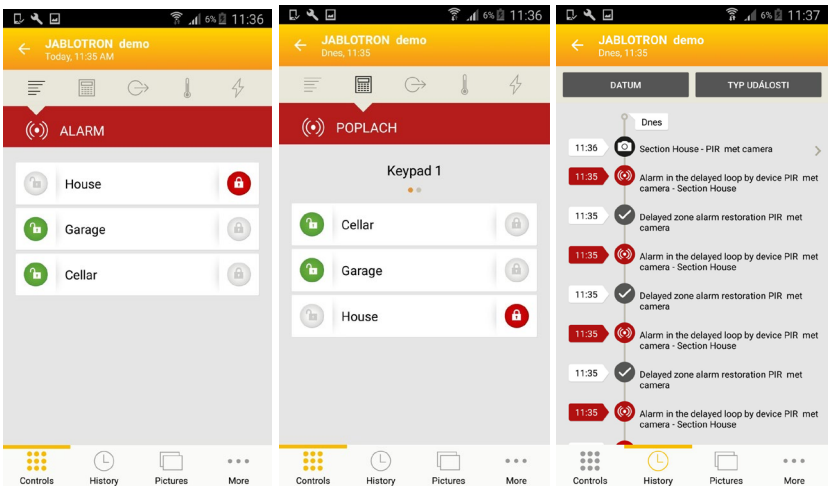


Część zdalnego programowania ze strony internetowej (niezależnie od platformy komputera zdalnego) nazywa się także WEB-Link. Jest dostępna w aplikacji MyCOMPANY → Zarządzanie instalacją → Przycisk Konfiguracja. WEB-Link jest dostępne wyłącznie dla firm instalujących, które mogą wykorzystać to narzędzie do uzyskiwania pośredniego, zdalnego dostępu w drodze zmiany parametrów w pliku konfiguracji znajdującym się na serwerze i ich natychmiastowego zapisania w danym czasie lub po rozbrojeniu systemu. Instalator może otrzymać powiadomienie o udanej zmianie konfiguracji za pomocą wiadomości SMS lub e-mail.



9.9 Sterowanie systemem za pomocą aplikacji mobilnej MyJABLOTRON

Użytkownicy MyJABLOTRON mogą pobrać aplikację na smartfony. Jest dostępna na platformę iOS i Android. Aplikacja mobilna jest najbardziej przyjaznym dla użytkownika sposobem sterowania systemem zabezpieczeń. Użytkownik może ją 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. Oznacza to, że niemal ten sam zakres funkcji jest dostępny w aplikacji sieciowej MyJABLOTRON. W przypadku niektórych platform oferuje dodatkowe elementy, na przykład TouchID lub FaceID zamiast kodu.



9.10 Sterowanie systemem za pomocą Antynapadowej kontroli dostępu

Ta opcja pozwala użytkownikom sterować (uzbrajać lub rozbrajać) systemem przy pomocy innego kodu w przypadku zagrożenia ze strony innej osoby. Taki kod dyskretnie zwróci uwagę na taką sytuację, aktywując **cichy alarm panika** bez jakiejkolwiek sygnalizacji dźwiękowej lub świetlnej. Cichy alarm panika uruchomi się po dodaniu 1 do istniejącego kodu użytkownika. Tę funkcję obsługują oba kody, z prefiksem i bez niego.

Przykład:

Kod użytkownika z prefiksem = 4*4444. Kod antynapadowej kontroli dostępu = 4*444**5**

Kod użytkownika bez prefiksu = 4444. Kod antynapadowej kontroli dostępu = 444**5**

Ostrzeżenie**: Jeżeli kod użytkownika kończy się na cyfrę 9 w przypadku antynapadowej kontroli dostępu, wówczas ostatnią cyfrą kodu będzie **0.

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

9.11 Przeszkody uniemożliwiające uzbrojenie systemu

Zgodnie ze **Sposobami uzbrajania** (patrz zakładka Parametry) centrala alarmowa może podczas uzbrajania poszczególnych stref systemu sprawdzać obecność stanu 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 stany, a także może nawet uniemożliwić uzbrajanie systemu w razie ich wystąpienia (**przeszkody niemożliwe do obejścia**).

Jedną z najpowszechniejszych przeszkód jest błąd systemu (sygnalizowany podświetlonym na żółto przyciskiem sygnalizacji na klawiaturze), utrata połączenia z czujką bezprzewodową lub aktywną czujką (zwykle czujką magnetyczną) ustawioną na reakcję alarmu opóźnionego (czujki drzwi frontowych i bramy garażowej), wyczerpana bateria systemu lub długotrwała awaria zasilania.

Przeszkodą niemożliwą do obejścia, uniemożliwiającą uzbrojenie systemu, jest na przykład **aktywna czujka** (zwykle magnetyczna czujka otwarcia drzwi) ustawiona na **reakcję natychmiastową**. Urządzenia należące do tej grupy to czujki 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 opcją „Uzbrój zawsze”. Kalendarz zawsze uzbroi każdą strefę pod warunkiem, że została ona skonfigurowana do realizacji takiej czynności (wyłącznie w przypadku używania „Domyślnego” profilu systemu).

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

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

Sposoby uzbrajania — zestawienie w tabeli

Sposoby uzbrajania	Klawiatura systemu	Za pośrednictwem menu głosowego / SMS / kalendarza	Aplikacja MyJABLOTRON	F-Link J-Link
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 naciśnięcie przycisku segmentu lub klawisza Enter.	Uzbroi zawsze pomimo błędów lub stanu aktywnych urządzeń.	Uzbroi zgodnie ze „Sposobami uzbrajania” (Uzbrój z kontrolą / Uzbrój bez kontroli) w zakładce Konfiguracji serwisowej.	Uzbroi zawsze pomimo błędów lub stanu aktywnych urządzeń.
Uzbrój po potwierdzeniu	Podczas próby uzbrojenia w obecności błędu lub aktywnego urządzenia klawiatura miga przez 8 sekund. System można uzbroić JEDYNIE ponownym naciśnięciem przycisku segmentu lub naciśnięciem przycisku Enter.	Uzbroi zawsze pomimo błędów lub stanu aktywnych urządzeń.	Uzbroi zgodnie ze „Sposobami uzbrajania” (Uzbrój z kontrolą / Uzbrój bez kontroli) w zakładce Konfiguracji serwisowej.	Uzbroi zawsze pomimo błędów lub stanu aktywnych urządzeń.

Nie uzbroi z aktywnym elementem	Podczas próby uzbrojenia w obecności błędu lub aktywnego urządzenia klawiatura miga przez 8 sekund. System można uzbroić ponownym naciśnięciem przycisku segmentu lub naciśnięciem przycisku Enter JEDYNIE, gdy czujka ustawiona na reakcję alarm NATYCHMIASTOWY NIE jest aktywna.	Nie uzbroi, kiedy aktywną czujkę ustawiono na reakcję NATYCHMIASTOWĄ Po wyborze „Uzbrój zawsze" Kalendarz uzbroi pomimo błędów lub aktywnego stanu urządzeń.	Nie uzbroi, kiedy aktywną czujkę ustawiono na reakcję NATYCHMIASTOWĄ.	Uzbroi zawsze pomimo błędów lub aktywnego stanu urządzeń.

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.).

W przypadku gdy uzbrojenie systemu nie jest możliwe, aktywuje się zdarzenie „Niepowodzenie konfiguracji" sygnalizowane szybkim miganiem przycisku sygnalizacyjnego podświetlonego na żółto na klawiaturach, a także brzęczykiem oraz dźwiękiem syreny zewnętrznej. Jednocześnie zostanie zgłoszone użytkownikowi, który usiłował uzbroić system lub administratorowi systemu, pod warunkiem że raport „SMS o niepowodzeniu konfiguracji" jest aktywny, patrz oprogramowanie F-Link, zakładka Komunikacja.

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

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

9.13 Zdarzenia zgłaszane użytkownikom

Wszystkie zdarzenia wysyłane do użytkowników przypisano do 5 podstawowych grup. Każdą grupę można dowolnie przypisywać użytkownikom. Użytkownicy, którym przypisano grupę, otrzymają raporty z tej grupy. Jeżeli podstawowe ustawienia grup nie wystarczą, można wykorzystać dwie specjalne grupy (określana przez użytkowników grupa 1 i 2). Do tych grup można dodawać zdarzenia przekazywane wyłącznie konkretnym użytkownikom.

Zestawienie tabelaryczne Grup zdarzeń zgłaszanych użytkownikom:

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 sieciowego 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	Wyciek gazu	Alerty SMS (1) / Połączenie alarmowe (2)
15	Alarm panika	Alerty SMS (1) / Połączenie alarmowe (2)
16	Anulowano alarm panika	Alerty SMS (1) / Połączenie alarmowe (2)
17	Problemy zdrowotne	Alerty SMS (1) / Połączenie alarmowe (2)
18	Zalanie	Alerty SMS (1) / Połączenie alarmowe (2)
19	Próba złamania kodu	Alerty SMS (1) / Połączenie alarmowe (2)
20	Uzbrojono ze strefą aktywną (przy aktywnym potwierdzeniu)	Alerty SMS (1) / Połączenie alarmowe (2)
21	Strefa bez ruchu	Alerty SMS (1) / Połączenie alarmowe (2)
22	Aktywacja przegrzania	Alerty SMS (1) / Połączenie alarmowe (2)
23	Dezaktywacja przegrzania	Alerty SMS (1) / Połączenie alarmowe (2)
24	Aktywacja zamarzania	Alerty SMS (1) / Połączenie alarmowe (2)
25	Dezaktywacja zamarzania	Alerty SMS (1) / Połączenie alarmowe (2)
26	Uruchomienie systemu (poza trybem serwisowym)	SMS o błędzie i serwisie (5)
27	Niski poziom baterii w urządzeniu	SMS o błędzie i serwisie (5)
28	Poziom baterii w urządzeniu OK	SMS o błędzie i serwisie (5)
29	Błąd (urządzenie, komunikator)	SMS o błędzie i serwisie (5)
30	Koniec błędu	SMS o błędzie i serwisie (5)
31	Wejście w tryb serwisowy	SMS o błędzie i serwisie (5)
32	Wyjście z trybu serwisowego	SMS o błędzie i serwisie (5)
33	Wejście w tryb konserwacji	SMS o błędzie i serwisie (5)
34	Opuszczenie trybu konserwacji	SMS o błędzie i serwisie (5)
35	Niski poziom BATERII	SMS o błędzie i serwisie (5)
36	BATERIA OK	SMS o błędzie i serwisie (5)
37	Błąd komunikacji z SMA	SMS o błędzie i serwisie (5)
38	Przywrócenie komunikacji ze SMA	SMS o błędzie i serwisie (5)
39	Tłumienie RF	SMS o błędzie i serwisie (5)
40	Koniec tłumienia RF	SMS o błędzie i serwisie (5)
41	Niskie saldo kredytu	SMS o błędzie i serwisie (5)

Przypisywanie zdarzeń rozpoznawanych przez system do grup podano w tabeli. W chwili wystąpienia zdarzenia system generuje wiadomość SMS w następującym formacie: Nazwa instalacji, Godzina, Zdarzenie, Źródło zdarzenia, Strefa, Godzina.

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 stan alarmu, ale także informować o innych stanach 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 segmentu uzbrajanie strefy lub włączanie PG
Dwa długie dźwięki	Dezaktywacja segmentu, 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
Ciągłe piszczenie	Opóźnienie na wejście
	Sygnalizacja stanu PG — ciągłe piszczenie
Brzęczyk	Alarm w strefie
Melodia (1–4) *	Sygnalizacja stanu PG

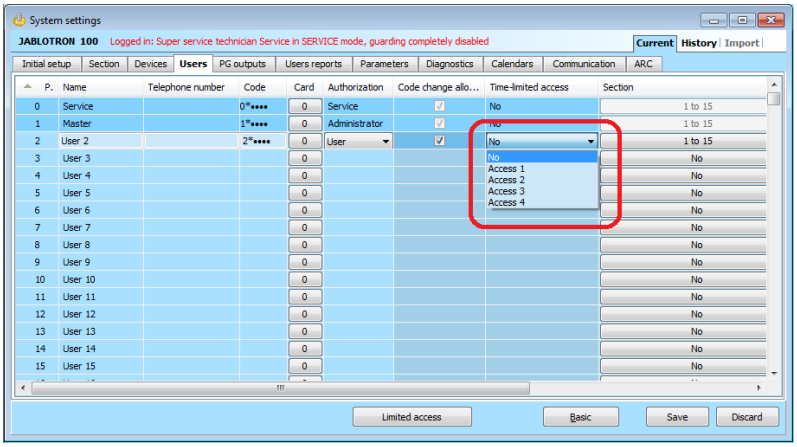
* Dotyczy jedynie syren obsługujących funkcję Melodii

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

Dźwięk	Opis działania
Ciągłe, szybkie pikanie	Alarm pożarowy
Ciągłe trąbienie	

9.15 Dostęp dla użytkowników w ograniczonym czasie

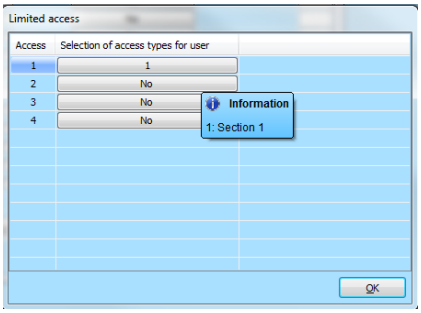
Funkcja dostępu dla użytkowników w ograniczonym czasie przeznaczona jest dla wybranych użytkowników podzielonych na 4 grupy. Do tych grup mogą dodawać różne „upoważnienia czasowe" na dostęp do przypisanych obszarów (stref) zgodnie z tygodniowym kalendarzem. To pozwala każdej grupie użytkowników blokować lub rozbrajać wybraną strefę w dwóch ramach czasowych (odstęp 1 i odstęp 2) dla każdego dnia w tygodniu. Ta funkcja przeznaczona jest głównie dla większych spółek, gdzie mogą być pracownicy, szefowie i kierownicy, lub przedszkoli ze sprzątaczkami, kucharkami, nauczycielami oraz rodzicami z dziećmi.

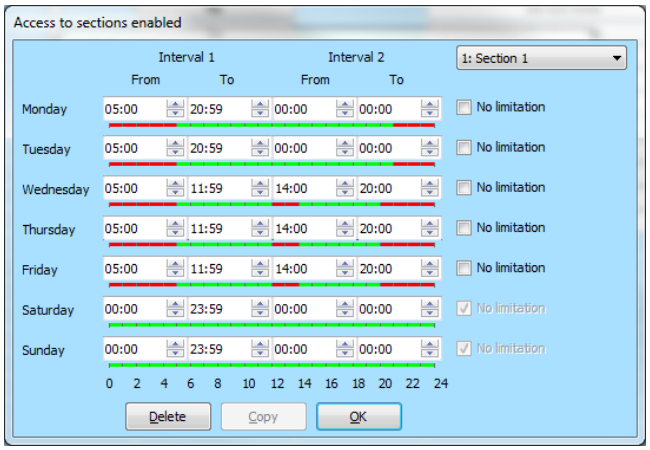


Każdy użytkownik systemu, który powinien mieć ograniczony dostęp zgodnie z zadanym kalendarzem, posiada aktywną opcję tj. „dostęp w ograniczonym czasie" za pomocą opcji z „Grupa 1" do „Grupa 4" i reprezentuje każdą grupę użytkowników.

Ograniczenie obowiązuje jedynie dla „Uwierzytelnienia użytkownika". Jeżeli użytkownik z aktywnym ograniczeniem czasu spróbuje rozbroić strefę w okresie blokowania, system odmówi. Natomiast jeśli użytkownik będzie znajdował się w chronionym obiekcie po upływie czasu opóźnienia na wejście, aktywuje się alarm włamania. Użytkownik posiada uprawnienie do anulowania alarmu, ale w ciągu czasu blokowania nie nastąpi rozbrojenie systemu.

W poniższym przykładzie istnieje wariant ustawień dostępu dopuszczonych dla wybranej grupy użytkowników, tj. „Grupy 1", gdzie dostęp jest ograniczony do „Strefy 1". W poniedziałek i wtorek dostęp jest dozwolony od godz. 5:00 rano do 20:59 wieczorem. Od środy do piątku dostęp jest dozwolony od 5:00 do 11:59, a następnie od 14:00 do 20:00. W weekend (sobota i niedziela) dostęp jest całkowicie zablokowany.





Aby zaprogramować dostęp w ograniczonym czasie przy pomocy oprogramowania F-Link w zakładce Użytkownicy, używa się przycisku o takiej samej nazwie, jak przycisk służący do ustawiania grupy użytkowników dla poszczególnych stref.

9.16 Dezaktywacja i blokowanie opcji

9.16.1 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 w menu klawiatury LCD lub za pośrednictwem programu J-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 J-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 J-Link sygnalizuje je czerwona kropka. Do dezaktywacji uprawniony jest jedynie Serwisant.

Dezaktywować można nie tylko urządzenie, ale także użytkownika, z wyjątkiem użytkowników w pozycji 0 (serwisant) i 1 (Administrator), wyjść PG lub czynności z kalendarza. Dezaktywacja ma charakter trwały do chwili jej anulowania przy pomocy procedury stosowanej do jej włączenia.

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

9.16.2 Blokowanie

Podczas uzbrajania strefy może się zdarzyć, że niektóre urządzenia pozostaną aktywne (na przykład otwarte okno lub drzwi balkonowe, czujka zalania w piwnicy itp.). System szybko zareaguje na tę sytuację podczas uzbrajania strefy i poinformuje o tym, ale po potwierdzeniu system zachowa się zgodnie z parametrem **Blokowanie podczas uzbrajania**, tj. w jeden z poniższych sposobów:

1. **Blokowanie aktywne** — aktywacja tej opcji zablokuje wszystkie aktywne czujki podczas uzbrajania, co oznacza, że w danym okresie uzbrojenia nie będą mogły uruchomić alarmu.
2. **Blokowanie nieaktywne** — dezaktywacja tej opcji spowoduje czasowe obejście wszystkich aktywnych czujek wyłącznie podczas uzbrajania, co oznacza, że jeżeli przejdą w tryb czuwania, będą mogły aktywować alarm (występuje ryzyko powstania fałszywego alarmu na przykład z powodu otwarcia okna przez przeciąg).

9.17 Funkcje niealarmowe — Funkcje wyjść PG

System bezpieczeństwa pozwala uprawnionym użytkownikom (zgodnie z ustawieniami) sterować funkcjami systemu, nie tylko funkcjami związanymi ze strzeżeniem stref, ale także programowalnymi wyjściami PG (włączanie/wyłączanie). Przy pomocy modułów przekaźnika lub modułu ze specjalnymi wyjściami półprzewodnikowymi mogą włączać urządzenia (jak kontrolki, sygnalizację świetlną, sygnalizatory dźwiękowe) lub inne elementy powiązane z systemem bezpieczeństwa (jak światła ruchu, AC po wejściu do pomieszczenia, blokowanie ogrzewania po otwarciu okna lub uzbrojeniu strefy), lub całkowicie odrębne elementy, tj. automatyka budynkowa (np. otwieranie elektrycznej bramy lub bramy garażowej, ogrzewanie, podlewanie ogrodu).

Funkcja wyjścia PG	Opis	Przykład
WŁ./WYŁ.	Stan wyjścia bistabilnego można zmienić dowolnym poleceniem lub urządzeniem.	Ręczne WŁĄCZANIE urządzeń segmentem kontrolnym, wiadomością SMS lub dowolnym urządzeniem z opcją ręcznego wyłączania bez ograniczeń. Zwykle sterowanie ogrzewaniem, klimatyzacją, oświetleniem.
Impuls	Stan wyjścia monostabilnego z zadanym czasem.	Impulsowe przełączanie innych dodatkowych obwodów sterowania, jak sterowanie bramą, roletami, żaluzjami, podlewaniem ogrodu, zamkami w drzwiach itp.
Kopiuj	Stan 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 stanów indywidualnych lub grupowych (zwykle otwartych okien, bramy garażu itp.) segmentem kontrolnym na klawiaturze. W podobny sposób można sygnalizować także stany wszystkich stref, alarmów, pamięci alarmów, błędów i wielu innych zdarzeń, gdzie podano początek i koniec.
Kopia opóźniona	Stan wyjścia monostabilnego z zadanym czasem włączenia/wyłączenia, z możliwością wielokrotnego przedłużania.	Zwykłe ustawienie wyjścia do sterowania oświetleniem w przypadku wykrycia ruchu przez czujkę ruchu. Każdy wykryty ruch przedłuża impuls.
Kopia poszerzona	Stan wyjścia opóźnionego z zadanym czasem takiego opóźnienia.	Używane zwykle do sygnalizacji drzwi otwartych przez czas dłuższy od zadanego ze względu na możliwość, że ktoś zapomniał je zamknąć (zasilanie sieciowe, drzwi lub brama garażu). Sygnalizacja może mieć postać świetlną na segmencie kontrolnym klawiatury lub dźwiękową z klawiatury lub syreny wewnętrznej/zewnętrznej.
Zmień	Stan wyjścia bistabilnego.	Wyjście przeznaczone do cyklicznego sterowania (WŁ., WYŁ.) na przykład za pomocą urządzenia impulsowego, w drodze uwierzytelnienia lub ustanowienia połączenia z uprawnionego numeru telefonu.

System oferuje także funkcje użytkownika, jak pomiar temperatury przy pomocy czujek temperatury lub termostatów, co może wyświetlać się na klawiaturze LCD i w aplikacji MyJABLOTRON, pomiar i monitorowanie zużycia energii elektrycznej, ilości wody i innych mediów. Do tego służy licznik impulsów JA-150EM-DIN w połączeniu z jakimś urządzeniem pomiarowym (licznik energii, gazu, wodomierz itp.). Nasze badania zastosowań i zalecenia znajdują się w MyCOMPANY, punkt MySTORAGE.

10 Konfiguracja systemu za pomocą oprogramowania F-Link

System JABLOTRON 100+ programuje się wyłącznie przy użyciu komputera, a dokładniej programu F-Link. F-Link sprawdza aktualną wersję oprogramowania od wersji 1.4.0 przez aktualizacje z serwera JABLOTRON, automatycznie oferując najnowszą wersję do pobrania. Po zalogowaniu można ją pobrać także z interfejsu sieciowego MyCOMPANY pod adresem www.myjablotron.com.

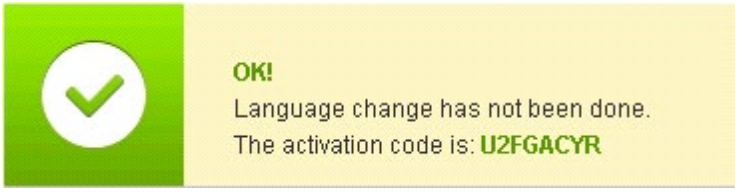
Tuż po otwarciu okna powitalnego w celu wyboru połączenia można przełączyć program F-Link na środowisko żądanego języka. W tym celu należy kliknąć ikonkę zmiany języka (flagi). Język można zmienić w dowolnym późniejszym czasie. Okno powitalne oferuje następujące opcje:

1. **Połącz lokalnie** — do łączenia komputera z centralą alarmową. Konieczny jest kabel USB (ze złączami A-B).
2. **Połącz zdalnie** — oferuje wybór z bazy danych w pliku, pozwalając ustanowić zdalne połączenie. Aby ustanowić zdalne połączenie z centralą alarmową, komputer musi mieć dostęp do internetu, używana karta SIM w centrali alarmowej musi mieć aktywną transmisję GPRS. W celu zapewnienia bezproblemowego połączenia należy spełnić inne wymagania, np. aktywna konfiguracja zdalna w centrali alarmowej, prawidłowy kod rejestracji, kod serwisowy, zaś przy braku używania komunikatora LAN również wystarczający sygnał GSM w lokalizacji centrali alarmowej.
3. **Ustawienia offline** — zapewnia dostęp do danych konfiguracji centrali alarmowej. Tu można uzyskać np. dostęp do wykazu urządzeń i rejestrów ostatniej wymiany baterii itp.

Oprogramowanie F-Link można wykorzystać do zmiany języka centrali alarmowej do komunikacji z użytkownikami. Język odnosi się nie tylko do tekstów wyświetlanych na ekranie LCD lub w wiadomościach SMS wysyłanych na telefony komórkowe użytkowników, ale także do menu głosowego komunikatorów używanych do komunikacji z użytkownikiem. Zmiana języka centrali alarmowej powoduje usunięcie wszystkich tekstów w systemie, a tym samym ten wybór powinien być pierwszym etapem przed instalacją i przypisywaniem nazw urządzeniom, strefom lub użytkownikom.

System JABLOTRON dostarczamy z fabrycznie ustawioną opcją języka komunikacji „Angielski", z możliwością wyboru „Czeski". Inne opcje języków centrali alarmowej ograniczają się do węższego wyboru języków dla kraju, do którego przeznaczona jest centrala alarmowa. Firma instalująca zarejestrowana w serwisie sieciowym MyCOMPANY www.myjablotron.com może zażądać „Klucza aktywacji", powiązanego z unikalnym kodem rejestracji sprzętu. „Klucz aktywacji" poszerzy dostępny wybór języków przeznaczonych przez producenta na dany rynek. Klucz aktywacji można uzyskać na trzy sposoby:

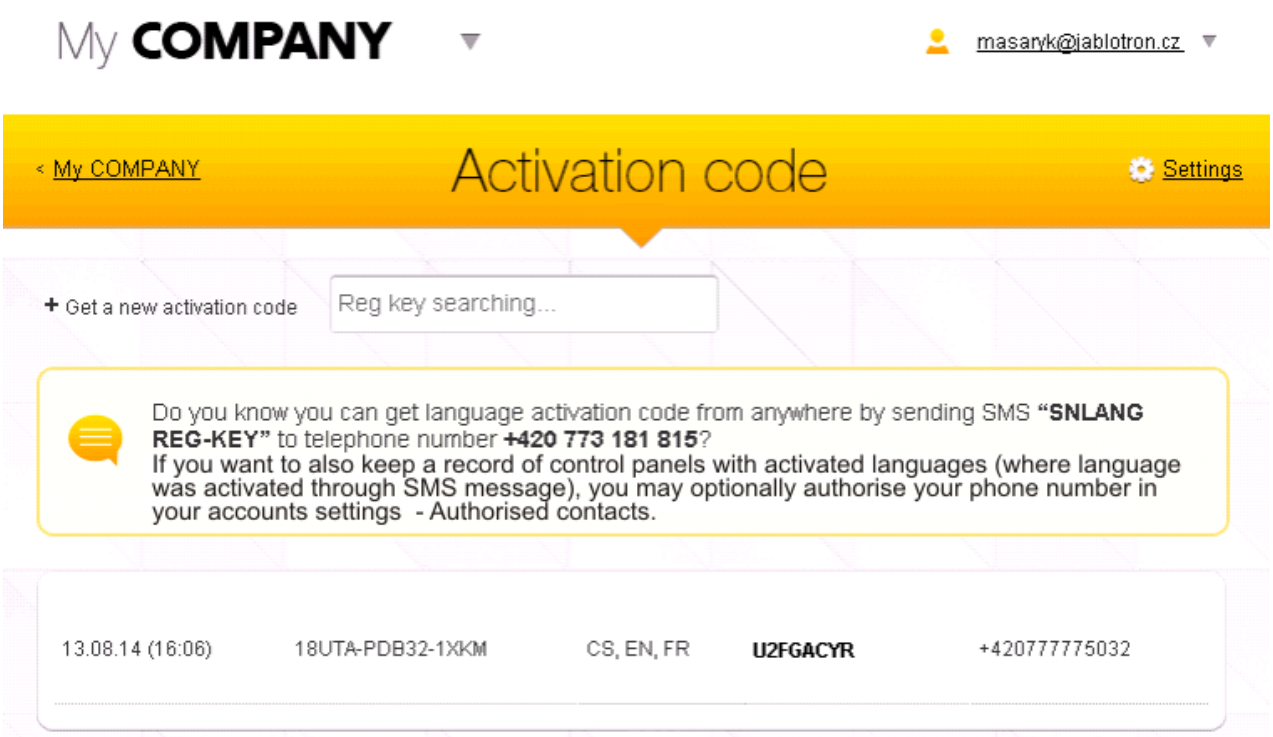
1. Z interfejsu sieciowego, dostępnego wyłącznie dla przeszkolonych instalatorów:
   a. Należy się zalogować do usługi sieciowej MyJABLOTRON www.myjablotron.com
   b. Otworzyć część MyCOMPANY.
   c. Wybrać usługę Kody aktywacyjne.
   d. Kliknąć pozycję + Pozyskać nowy kod aktywacyjny.
   e. Wprowadzić do centrali alarmowej Klucz rejestracji i zaznaczyć „Wyślij".
   f. Jeśli wyświetli się większa liczba języków, zaznaczyć żądane języki i zakończyć proces wyboru za pomocą „Wyślij".



   g. Zanotować Kod aktywacyjny wyświetlony na zielono i wpisać go do F-Link.

Lista wygenerowanych Kodów aktywacyjnych pozostanie zapisana na stronie do ewentualnego użytku w przyszłości.

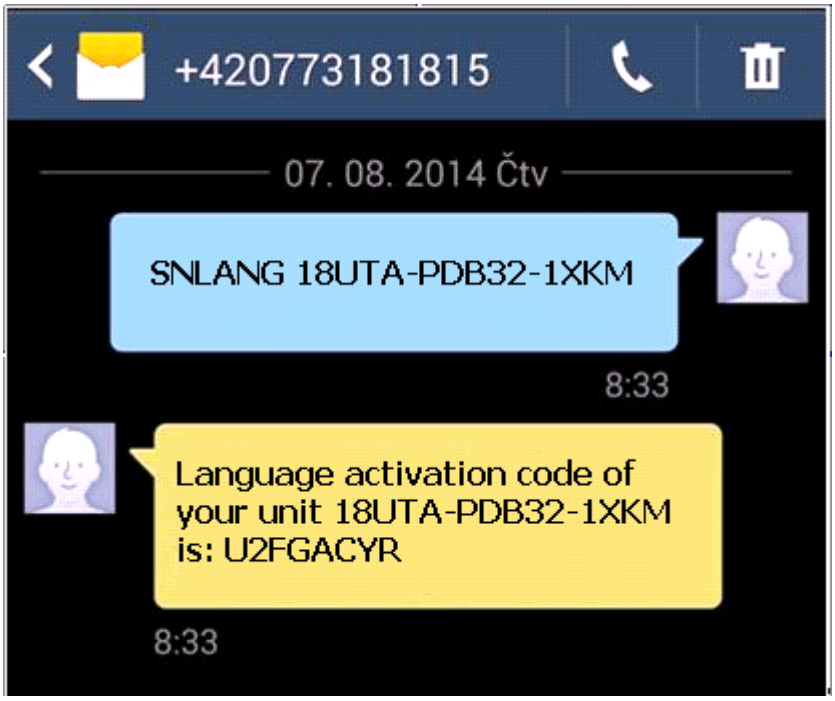
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com



2. Jeżeli instalator nie ma w danej chwili dostępu do internetu (usługi sieciowej MyJABLOTRON), Kod aktywacyjny można uzyskać w wiadomości SMS.

Komunikat SMS w formacie: „**SNLANG_kod rejestracji”** można wysłać na numer telefonu **+420 773 181 815**. Po chwili zostanie wysłana odpowiedź z kodem aktywacyjnym. Kod aktywacyjny może zawierać od 8 do 14 cyfr oraz wielkie i małe litery.

Otrzymany kod aktywacyjny należy wprowadzić do F-Link w zakładce Konfiguracja początkowa za pomocą przycisku Aktywuj.

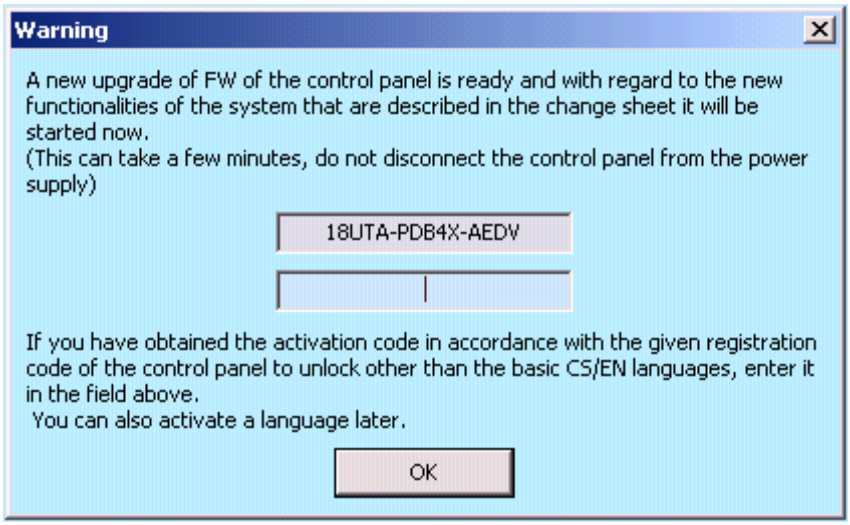


Przykład wysłania żądania przy pomocy SMS

3. Pozyskiwanie Kodu aktywacyjnego od dystrybutora. Przesyłając prośbę o Kod aktywacyjny, należy podać Kod rejestracji centrali alarmowej. Zależnie od kraju, kod aktywacyjny może znajdować się także na opakowaniu centrali alarmowej.

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 and FLEXI_LOG. Po wyświetleniu można zamknąć okno.
3. Uruchomić program F-Link. Jeżeli centrala alarmowa ma ustawienia domyślne, otworzy się zakładka **Konfiguracja początkowa**, a system automatycznie przejdzie w tryb serwisowy. Jeżeli centralę alarmową skonfigurowano wcześniej (zmieniono jej kod serwisowy), oprogramowanie zażąda wprowadzenia kodu. Należy go wprowadzić w formacie **cccc** (domyślne ustawienie kodu serwisowego to 1010). Przy aktywnym prefiksie (w zakładce Konfiguracja początkowa w F-Link) ma postać 0*cccc (0*1010). Aby program zapisał kod do chwili zamknięcia bazy danych, można użyć opcji **Zapamiętaj**. Do sprawdzenia wprowadzonego kodu, na przykład podczas używania klawiatury alfanumerycznej, gdzie można popełnić błąd, można użyć opcji **Wyświetl kod**. Uwaga: Po ustanowieniu połączenia przy pomocy przewodu USB zostanie wyłączona możliwość programowania zmian ustawień z klawiatury LCD (pozycja menu Ustawienia będzie nieaktywna). W ciągu kilku sekund po odłączeniu przewodu ta pozycja pojawi się ponownie w menu.
4. Po prawidłowym uwierzytelnianiu pojawi się poniższe okno:



W takim przypadku zalecamy przeprowadzenie aktualizacji. Po potwierdzeniu klucza zostanie pobrany nowy pakiet oprogramowania, co może potrwać kilka minut. Po zakończeniu aktualizacji wyświetli się pierwsza strona Kreatora (zakładka Konfiguracja początkowa).

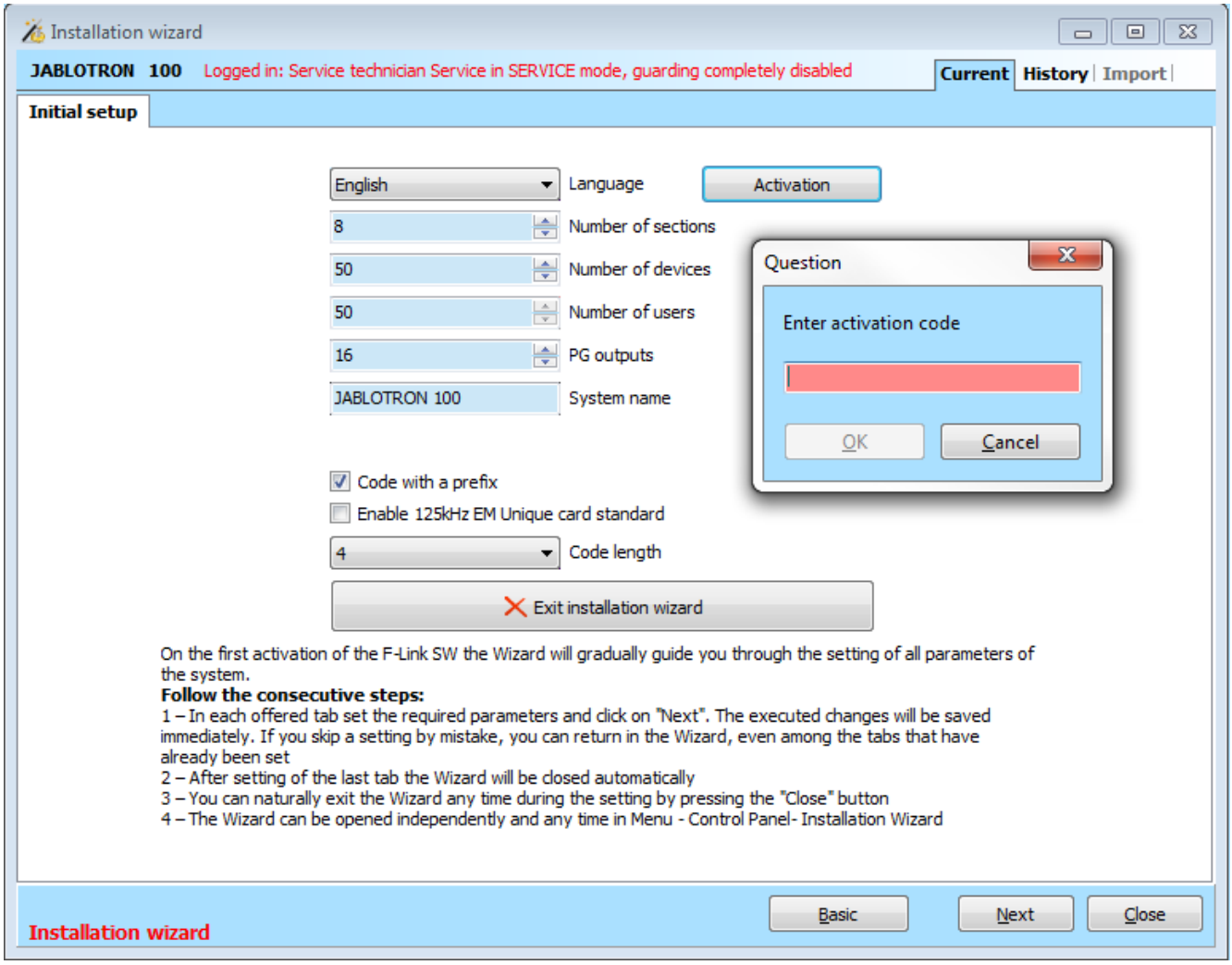
10.2 Uruchomienie Kreatora

1. W każdej oferowanej zakładce ustawić żądany parametr i kliknąć przycisk „Dalej”. W sytuacji przypadkowego pominięcia ustawienia można powrócić do zakładki ustawianej wcześniej w Kreatorze.
2. Po ustawieniu ostatniej zakładki nacisnąć „Zapisz” i zamknąć Kreatora przyciskiem „Wyjdź”.
3. Po opuszczeniu go użytkownik otrzyma pytanie, czy chce uruchamiać Kreatora instalacji podczas kolejnego uruchomienia oprogramowania F-Link.
4. Kreatora można opuścić w dowolnej chwili podczas procesu konfiguracji. W tym celu należy nacisnąć przycisk „Wyjdź”.
5. Kreatora można uruchomić niezależnie i w dowolnej chwili w menu Centrala alarmowa / Kreator instalacji.

10.3 Zakładka Konfiguracja początkowa

Ta zakładka służy do ustawiania podstawowego rozmiaru systemu. Zadane wartości można zmienić w dowolnej chwili. Wartości zasięgu wpływają na wielkość bazy danych, a tym samym czas potrzebny do ładowania i zapisywania danych (zwykle za pomocą dostępu zdalnego). Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym. Podczas pierwszego uruchomienia programu F-Link Kreator będzie prowadził użytkownika przez konfigurację kolejnych parametrów systemu.

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



Aktywacja: wprowadzając specjalny kod aktywacyjny, można dodać język (języki) do oferty języków wydanych dla kraju, dla którego przeznaczona jest centrala alarmowa.

Uwagi:

- Jeżeli konieczny jest jeden z języków domyślnych (EN/CZ), nie trzeba używać funkcji Aktywuj.
- Jeżeli użytkownik żąda innego języka, po wprowadzeniu kodu aktywacyjnego można wybrać jeden z dostępnych języków z menu Język.
- Trzeba także aktualizować oprogramowanie elementów bezprzewodowych (szczególnie modułów dostępowych z wyświetlaczem, aby wybrany język pozyskać również dla nich).

Opis zakładki Konfiguracji początkowej:

Kody z prefiksem — ta funkcja określa sposób wprowadzania wszystkich kodów dostępu do uwierzytelniania użytkownika. Jeżeli funkcja jest aktywna, system przed wprowadzeniem kodu dostępu wymaga prefiksu złożonego z 1 do 3 cyfr (pozycja kodu), po którym następuje symbol * (np. 12*3456). Pozwala on użytkownikom zmienić własne kody za pomocą wyświetlacza LCD. Jednakże aby móc sterować systemem, należy użyć kodu z kolejnym numerem kodu (prefiks). Jeżeli ten parametr jest nieaktywny, należy wprowadzić jedynie 4-cyfrowy kod dostępu, a kody może zmieniać Administrator systemu, który przypisze kody i będzie jedyną osobą upoważnioną do zmiany uprawnień użytkowników (tym samym będzie je znać). Administrator odpowiada także za unikanie powielania kodu.

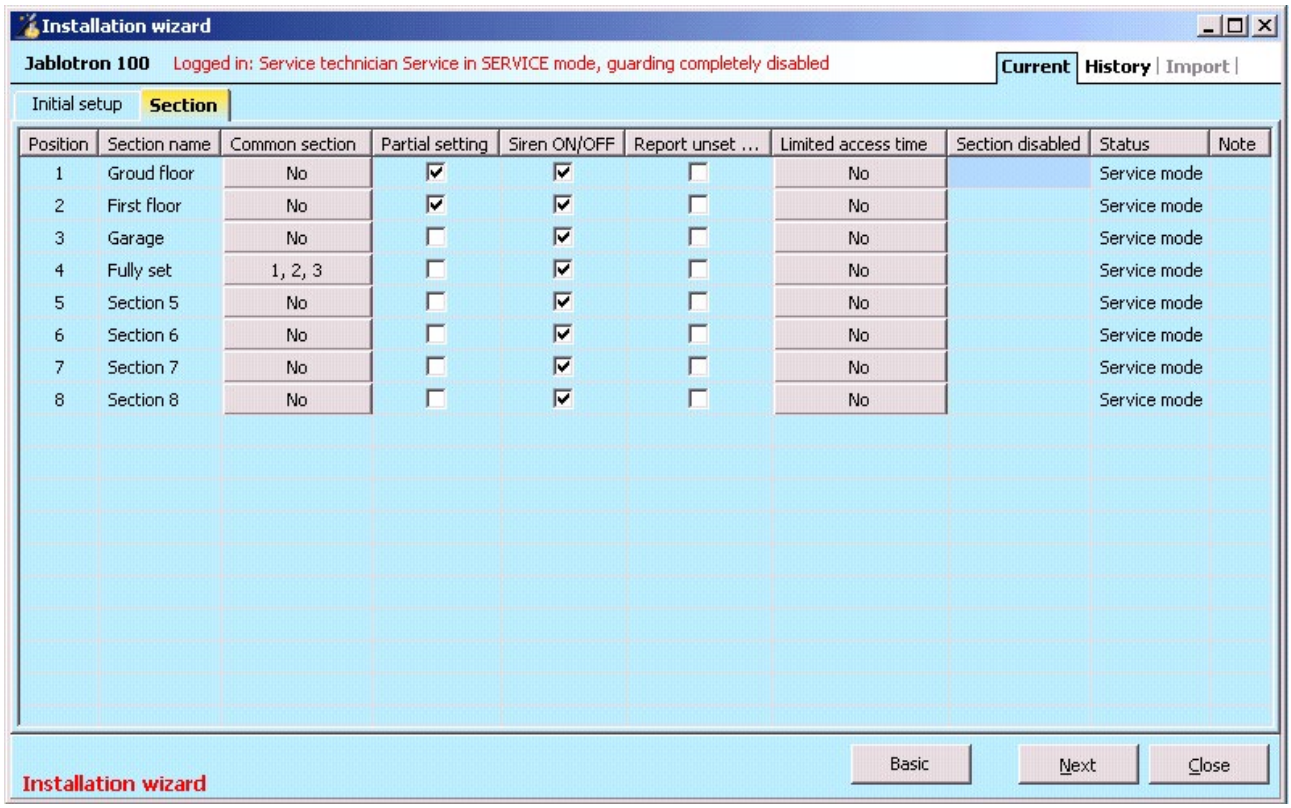
Ostrzeżenie: *Każda dezaktywacja tego parametru nieodwracalnie usunie wszystkie kody użytkownika oraz ustawienia Kodu serwisowego i Kodu administratora i przywróci wartości domyślne. Nie ulegają zmianie uprawnienia Użytkowników i karta/breloki RFID już istniejących użytkowników.*

Aktywować standard karty 125 kHz EM UNIQUE — jeżeli nieaktywny, można używać wyłącznie kart/breloków RFID służących do identyfikacji (JA-190J, JA-191J, JA-192J, JA-194J), zalecanych przez producenta. Jeżeli aktywny, dopuszczone są także karty innych producentów, działające z powyższą częstotliwością.

Długość kodu — aby zwiększyć poziom bezpieczeństwa systemu alarmowego podczas uwierzytelniania, można ustawić długość kodu użytkownika niezależnie od funkcji prefiksu. Kody mogą mieć długość 4, 6 lub 8 cyfr. Po zmianie długości kodu Kody serwisowe i Administratora ustawiają się na wartości domyślne, a wcześniej wprowadzone kody zostają wykasowane.

10.4 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.



* Opisane poniżej pozycje, oznaczone *, wyświetlają się wyłącznie przy aktywnym **widoku Ustawienia zaawansowane**.

Nazwa strefy — nazw stref używa się do przekazywania raportów tekstowych o zdarzeniu (SMS), wyświetlania na klawiaturze LCD i odczytu pamięci, aby ułatwić rozpoznawanie podczas raportowania (np. Parter, Skład itp.).

Strefa wspólna — pozwala wybrać automatyczne uzbrajanie strefy w przypadku uzbrojenia wszystkich stref, dla których jest wspólna (odpowiednie dla korytarzy, klatek schodowych i innych powierzchni wspólnych). Ostrzeżenie o ograniczeniu ewentualnego wykorzystania segmentu klawiatury dla strefy wspólnej: jeżeli którekolwiek ze stref rozbrojono oddzielnie, segmentu strefy wspólnej **nie można** użyć do rozbrojenia pozostałych stref. Te strefy należy rozbrajać oddzielnie.

Uzbrojenie częściowe* — pozwala uzbroić strefę częściowo, jeżeli ktoś pozostaje w środku (czujki z wybraną reakcją typu Wewnętrzny nie będą aktywne, patrz rozdział 8 System configuration). Bez aktywacji tego parametru w strefie nie można użyć uzbrojenia częściowego.

Zgłoś rozbrojoną strefę* — jeżeli strefa jest rozbrojona i nie nastąpi w niej aktywacja czujki w zadanym okresie, używa się raportu „Rozbrojona strefa”. Okres czasu ustawia się w zakładce Parametry / Zgłoś rozbrojoną strefę po upływie (1–48 h).

Automatyczne uzbrajanie — służy do automatycznego uzbrajania strefy w przypadku, gdy zgłoszono „Rozbrojoną strefę”. W zakładce Parametry można ustawić odstęp czasu w minutach, po którego upływie nastąpi automatyczne uzbrojenie strefy. Odstęp czasu zaczyna się z chwilą zgłoszenia „Rozbrojonej strefy”. Ta funkcja stanowi uzupełnienie funkcji „Zgłoś rozbrojoną strefę” i można jej używać wyłącznie przy aktywnej funkcji „Zgłoś rozbrojoną strefę”.

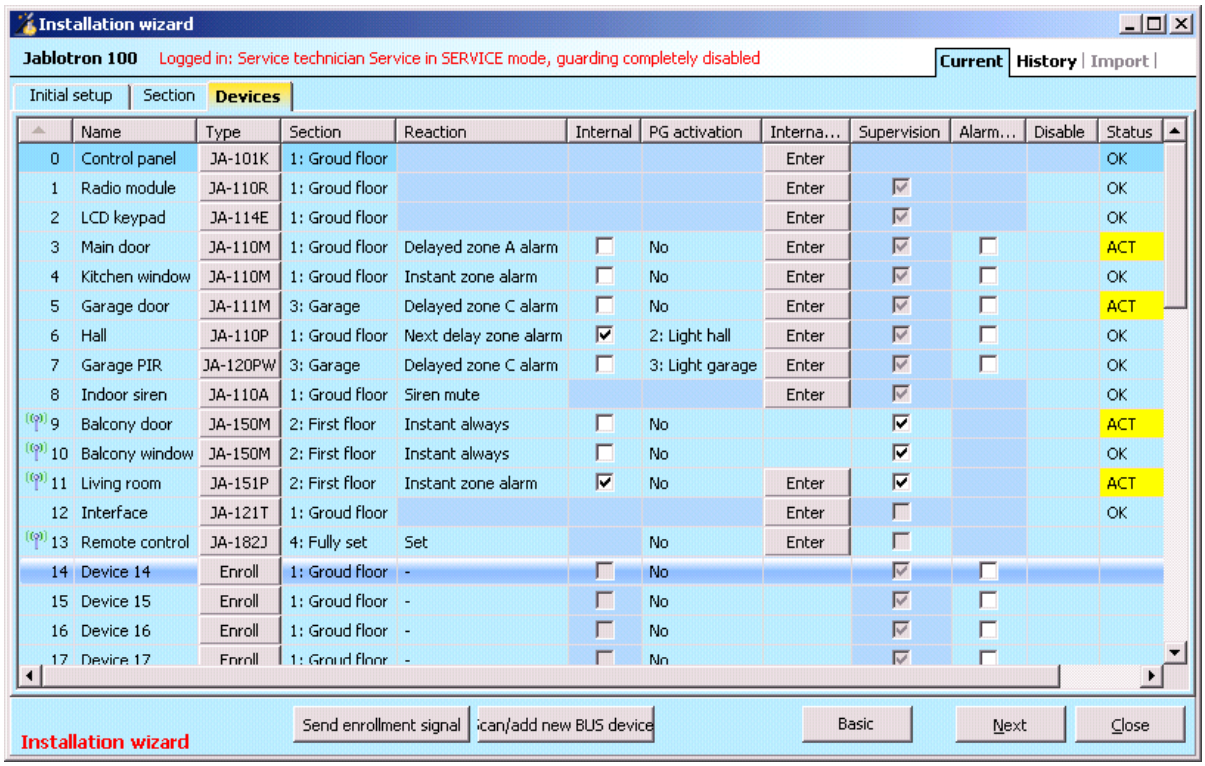
Ograniczony czas dostępu* — pozwala ustawić tygodniowy harmonogram, dopuszczający rozbrojenie strefy dla wybranych użytkowników. Bardziej szczegółowe informacje podano w rozdziale Dostęp dla użytkowników w ograniczonym czasie.

Stan — wskazuje aktualny stan strefy (Rozbrojony, Uzbrojony, Opóźnienie na wyjście, Opóźnienie na wejście, Częściowo uzbrojony, Alarm, Pamięć alarmu, Dezaktywacja, Tryb serwisowy). Naciśnięcie przycisku umożliwia sterowanie systemem zależnie od uwierzytelnienia nadanego loginem (zmienia stan strefy — uzbrojenie/rozbrojenie).

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

10.5 Zakładka Urządzenia

Służy do przypisywania zainstalowanego urządzenia w systemie i ustawiania jego parametrów. Zakładka wyświetli tyle pozycji, ile wybrano w zakładce Konfiguracja początkowa. 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.



* Opisane poniżej pozycje, oznaczone *, wyświetlają się wyłącznie przy aktywnym **widoku Ustawienia zaawansowane**.

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 10.4 Sections tab.*

Reakcja — określa, którą reakcję wywoła aktywacja danego urządzenia. Jeżeli urządzenie nie ma wejścia alarmowego (np. modułu dostępu MAGISTRALI), nie można mu przypisać reakcji. 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 10.4 Sections tab. Jeżeli dla strefy nie jest aktywne częściowe uzbrojenie, ustawienie tego parametru nie obowiązuje.

Aktywacja PG* — aktywacja urządzenia może aktywować programowalne wyjścia PG ze zdefiniowanymi reakcjami.
Ta opcja jest powiązana z pozycją Wyjścia PG / Aktywacja / przez urządzenie.

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 10.5.1 Keypad configuration. Ustawienia pozostałych urządzeń opisano w odpowiadających im instrukcjach.

Nadzór* — pozwala dezaktywować sprawdzanie regularnej komunikacji z urządzeniami bezprzewodowymi (nie można go wyłączyć dla elementów MAGISTRALI). Domyślnie ustawienie urządzeń bezprzewodowych (z wyjątkiem manipulatorów zdalnych i przycisków panika) jest zawsze aktywne.

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 alarmu, sabotażu, aktywacji PG, Awarii, raportów itp.).

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

Stan — wskazuje aktualny stan 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), INIT = odczyt konfiguracji urządzenia, Disabled = urządzenie jest nieaktywne. Przesunięcie kursora myszy na STATUS urządzenia wyświetli szczegółowe dane.

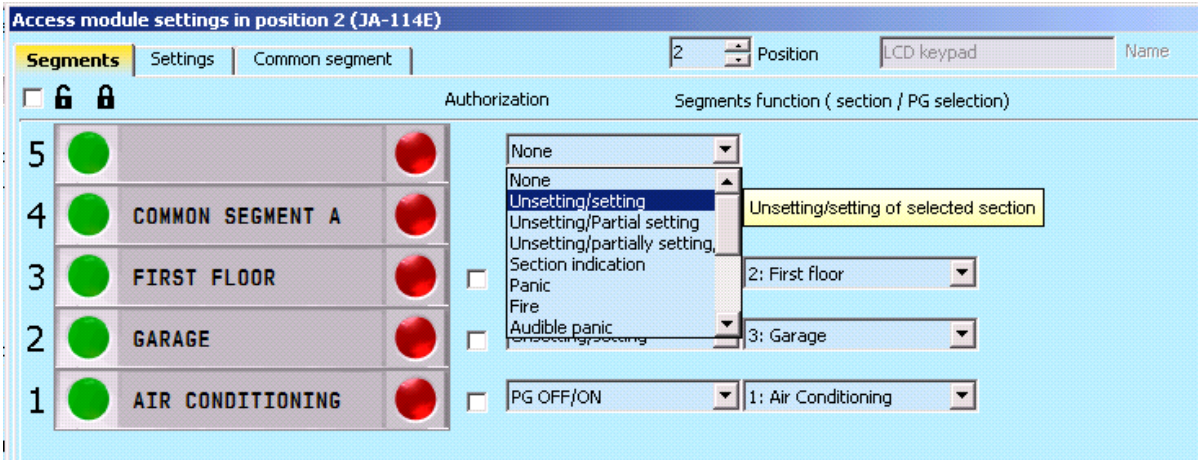
Notatka — pozwala opisać dane urządzenia, np. lokalizacja, data ostatniej wymiany baterii, średnia siła sygnału RF podczas ostatniego testu itp.

10.5.1 Konfiguracja klawiatury

- Najpierw należy mechanicznie zmontować klawiaturę sterującą. Do wybranego modułu dostępowego przymocować żądaną liczbę segmentów kontrolnych (maks. 20). Ich przewody wewnętrzne należy połączyć.
- Przypisać klawiaturę w wybranej pozycji w systemie (patrz rozdział 5 Installation of BUS devices).
- Przy wprowadzaniu ustawień wewnętrznych klawiatury (zakładka Urządzenia) otworzy się następujące okienko (przykład dotyczy klawiatury JA-114E). Dla innych klawiatur zakres ustawień może być mniejszy.

Przykład ustawień wewnętrznych klawiatury:

10.5.1.1 Zakładka Segmenty



Zamki zamknięte/otwarte — aktywuje wyświetlanie symboli blokowania dla przycisków sterowania segmentami do uzbrajania sekcji oraz symboli kropek (pusty/pełny) do sterowania wyjściami PG. Symbole uwzględnia się przy drukowaniu etykiet.

Teksty etykiet segmentów kontrolnych — Wyświetla się Nazwa strefy (z zakładki Strefy) lub Nazwa wyjścia PG (z zakładki Wyjścia PG). Tu można edytować także cały tekst do wydruku, klikając odpowiedni tekst. Takie zmiany nie zapisują się w systemie i służą jedynie do wydruku etykiet. Do drukowania etykiet segmentów służy przycisk **Drukuj etykiety** (na dolnym pasku karty).

Drukuj etykiety — umożliwia bezpośrednie drukowanie zadanych tekstów etykiet przy pomocy zainstalowanej drukarki. Teksty można edytować, klikając segment, co powoduje jedynie zmianę wydruku, a zmienione teksty nie zapisują się w bazie danych. Można wygodnie korzystać z drukarki etykiet PT-P700 firmy JABLOTRON, która umożliwia automatycznie docięcie do żądanego wymiaru etykiety.

Importuj — umożliwia kopiowanie aktualnych ustawień klawiatury do innych klawiatur, na przykład w sytuacji, gdy chroniony budynek ma kilka innych wejść, z których każde wymaga 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.

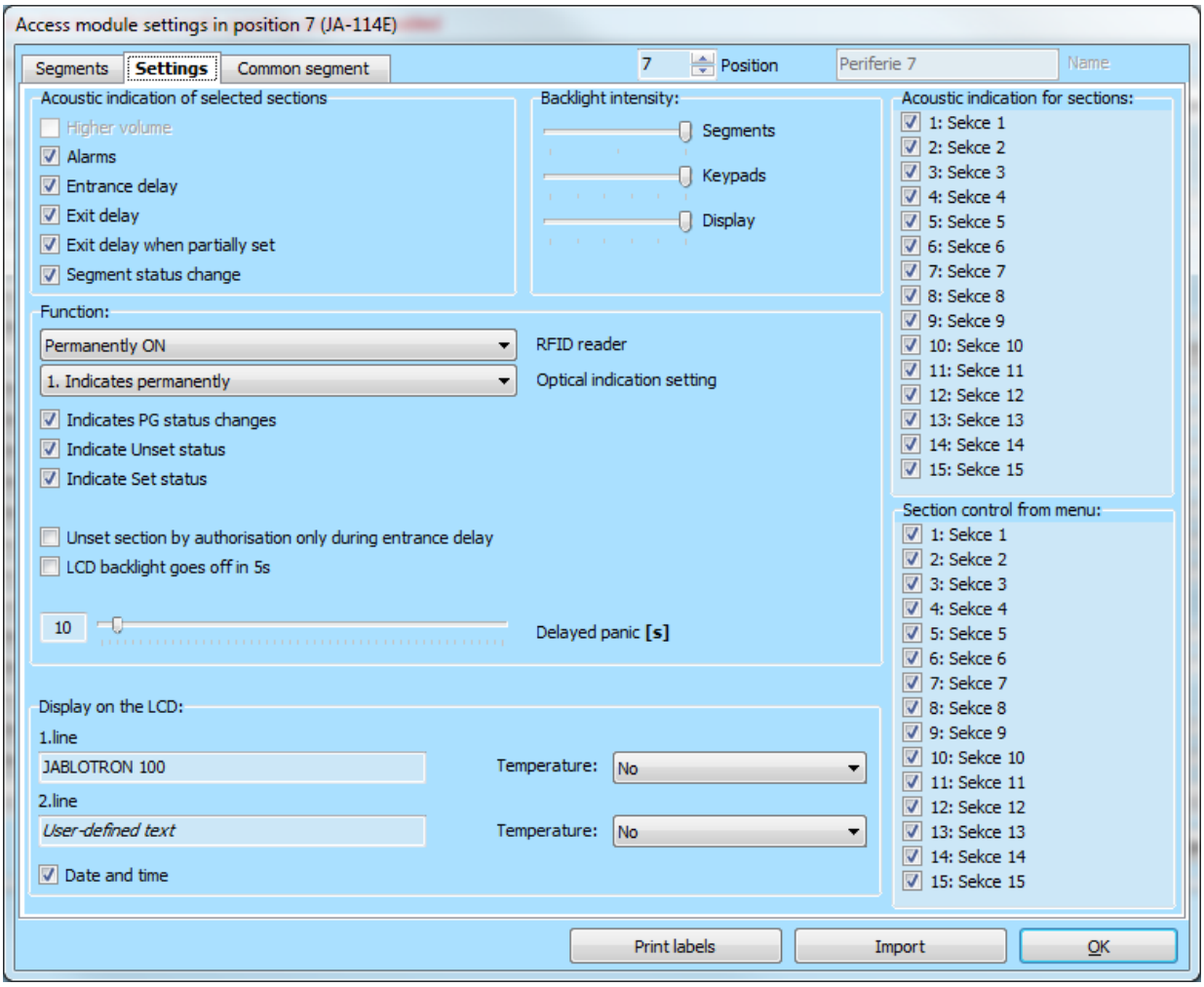
Uwierzytelnienie — do uzbrojenia i rozbrojenia konieczne jest uwierzytelnienie użytkownika. Jeżeli ten parametr jest nieaktywny, bez uwierzytelnienia można sterować wszystkimi segmentami z wyjątkiem funkcji Rozbrój strefę, który zawsze wymaga uwierzytelniania. W odniesieniu do aktywacji i dezaktywacji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

Funkcje Segmenty — z lewej strony wybiera się funkcję segmentu, z prawej strefę lub wyjście PG, do którego przypisano wybraną funkcję. Do segmentu można przypisać następujące funkcje:

Brak	Segment wył., używana do segmentów przygotowanych jako rezerwa do użytku w przyszłości.
Rozbrój/Uzbrój	Sterowanie strefą. Sygnalizacja segmentu: strefa rozbrojona = zielona, uzbrojona = czerwona.
Rozbrój / Uzbrój częściowo	Umożliwia aktywację trybu częściowego uzbrajania strefy (jeżeli aktywne w zakładce Strefy). Sygnalizacja segmentu: strefa rozbrojona = zielona, uzbrojona częściowo = żółta.
Rozbrój / Uzbrój częściowo / Uzbrój	Pozwala wybrać poziom uzbrajania. Po naciśnięciu prawego przycisku (Uzbrój) możliwe jest uzbrojenie częściowe, a po wielokrotnym naciśnięciu możliwe jest uzbrojenie pełne. Na potrzeby tego wyboru dla strefy w zakładce Strefy musi być aktywne uzbrojenie częściowe. Sygnalizacja segmentu: strefa rozbrojona = zielona, uzbrojona częściowo = żółta, uzbrojona całkowicie = czerwona.
Sygnalizuje strefę	Segment wskazuje jedynie stan strefy, ale nie umożliwia sterowania nią (odpowiednie np. do sygnalizacji stanu stref wspólnych, klatki schodowej itp.) W przypadku aktywacji alarmu pozwala na jego anulowanie przez naciśnięcie zielonego przycisku segmentu z późniejszym prawidłowym uwierzytelnieniem użytkownika.
Panika (cicha)	Segment umożliwia aktywację cichego alarmu panika. Po naciśnięciu prawego przycisku ze strefy, do której przypisana jest funkcja, zostanie wysłany raport Panika bez sygnalizacji dźwiękowej. Alarm panika może być także Opóźniony z możliwością dostosowania czasu i anulowania przed wygaśnięciem zadanego czasu (patrz Panika opóźniona). Jeżeli strefa jest uzbrojona, nie nastąpi jej rozbrojenie.
Pożar	Segment aktywuje alarm pożarowy. Po naciśnięciu prawy przycisk segmentu miga na zielono przez 3 sekundy (w tym czasie można anulować alarm pożarowy, naciskając lewy przycisk segmentu). Później nastąpi aktywacja alarmu pożarowego ze strefy, do której przypisano segment
Panika z sygnałem dźwiękowym	Segment umożliwia aktywację alarmu z sygnałem dźwiękowym. Po naciśnięciu następuje aktywacja alarmu panika ze strefy, do której przypisano segment. 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	Segment pozwala przesłać raport o zagrożeniach medycznych (bez aktywacji syreny). Po naciśnięciu prawy segment przycisku miga przez 3 sekundy (w tym czasie można anulować raport Zagrożenia medyczne, naciskając lewy przycisk segmentu). Później segment powraca w tryb czuwania, a system wysyła raport Zagrożenia medyczne ze strefy, do której przypisano segment.
Dezaktywuj PG / Aktywuj PG	Segment umożliwia sterowanie wyjściem PG. Wskazanie: PG nieaktywne = zielony, PG aktywne/aktywowane = czerwony.
Aktywuj PG	Ten segment można wykorzystać wyłącznie do aktywacji wyjścia PG (np. włączenia oświetlenia na zadany czas).
Dezaktywuj PG	Segment można wykorzystać jedynie do dezaktywacji wyjścia PG (np. funkcja przycisku STOP w nagłym wypadku).
Sygnalizuje PG	Segment sygnalizuje jedynie stan wyjścia PG bez możliwości sterowania nim (czerwony sygnalizuje stan aktywny).
Sygnalizacja odwrócona PG	Segment sygnalizuje wyłącznie stan wyjścia PG z odwróconą logiką (zielony sygnalizuje stan aktywny) bez możliwości sterowania nim.
Segment wspólny A/B	Umożliwia jednoczesne sterowanie większą liczbą stref, posiadających indywidualne segmenty na klawiaturze, za pomocą jednego segmentu. Po naciśnięciu przycisku w tym samym segmencie Polecenie Rozbrój/Uzbrój realizowane jest łącznie dla wybranych segmentów stref. Jeśli niektóre strefy sterowane za pomocą Wspólnego segmentu są uzbrojone, a inne rozbrojone, skorzystanie ze Wspólnego segmentu spowoduje rozbrojenie/uzbrojenie pozostałych segmentów. Jeżeli aktywne jest Uzbrojenie częściowe

	dla jednego z wybranych segmentów (szczegółowe informacje w rozdziale 9 System control options), Wspólny segment zachowa się następująco: 1. naciśnięcie Uzbrój = uzbrojenie częściowe, 2. naciśnięcie Uzbrój = uzbrojenie pełne. Nie należy łączyć funkcji Wspólnego segmentu z funkcjami Strefa / Wspólne dla stref. Sygnalizacja Wspólnego segmentu: wszystkie strefy rozbrojone = zielony, wszystkie strefy w pełni uzbrojone = czerwony, dowolna strefa uzbrojona (częściowo) = żółty. Na klawiaturze mogą być najwyżej 2 segmenty wspólne. Strefy do Wspólnego segmentu przypisuje się w górnej zakładce Wspólny segment. Uwaga: Pozycja „Wspólny segment x" pojawia się jedynie, gdy do modułu podłączono więcej niż dwa segmenty do sterowania strefą.
PG sygnalizuje/steruje	Segment może sterować innym wyjściem PG od tego, które sygnalizuje optycznie. W tym menu pierwszy parametr służy do wyboru wyjścia PG do sygnalizacji, a drugi (uzupełniający) wyjścia PG do sterowania. Ta funkcja służy np. do sterowania bramą garażu za pomocą impulsu wyjścia PG, przy czym segment kontrolny wyświetla aktualny stan bramy pozyskany z czujki bramy.

10.5.1.2 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, przerywane pikanie (1 raz na sekundę)
Opóźnienie na wyjście przy uzbrojeniu częściowym	Powolne, przerywane pikanie (domyślnie wyłączone)
Zmiana stanu segmentu	Sygnalizacja dźwiękowa z zastosowaniem jednego piknięcia podczas zmiany

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

Funkcje:

<table>
<tr><td rowspan="5">Czytnik RFID</td><td colspan="2">Aby zapewnić oszczędność energii, działanie czytnika można ograniczyć do 3 s od naciśnięcia jego pokrywy. Czytnik RFID można też całkowicie wyłączyć. To ustawienie odnosi się do klawiatur bezprzewodowych i modułów dostępowych, jeżeli otrzymują stałe zasilanie ze źródła zewnętrznego. W przeciwnym razie zawsze następuje automatyczne wyłączenie ich czytnika RFID.</td></tr>
<tr><td>Stale włączony</td><td>Czytnik RFID jest stale aktywny. W przypadku klawiatury MAGISTRALI nie przestrzega ustawienia wzbudzania.</td></tr>
<tr><td>Aktywacja przez naciśnięcie</td><td>Wzbudzanie czytnika RFID na 3 s po aktywacji na klawiaturze.</td></tr>
<tr><td>Wyłączony</td><td>Czytnik RFID jest trwale wyłączony.</td></tr>
<tr><td>Aktywacja po naciśnięciu lub żądaniu uwierzytelnienia</td><td>Czytnik RFID wzbudza się po aktywacji na klawiaturze lub za pomocą żądania uwierzytelnienia.</td></tr>
<tr><td rowspan="6">Ustawienia sygnalizacji świetlnej</td><td>1. Sygnalizacja stała</td><td>Klawiatura MAGISTRALI sygnalizuje nieprzerwanie. Klawiatura bezprzewodowa będzie sygnalizować nieprzerwanie jedynie przy zasilaniu zewnętrznym. Bez zasilania zewnętrznego zachowuje się jak opcja 2.</td></tr>
<tr><td>2. Po zmianie stanu strefy — klawiatura</td><td>Klawiatura sygnalizuje zmianę stanu strefy / PG. Zmiana stanu jest sygnalizowana jedynie na danym segmencie.
Opóźnienie na wejście i alarm sygnalizuje cała klawiatura.</td></tr>
<tr><td>3. Po zmianie stanu strefy — segment</td><td>Klawiatura sygnalizuje zmianę stanu strefy / PG. Zmiana stanu segmentu, opóźnienie na wejście i alarm sygnalizowane są jedynie na danym segmencie.</td></tr>
<tr><td>4. Po zmianie stanu segmentu</td><td>Opóźnienie na wejście i alarm jest sygnalizowany tylko dźwiękiem.
Zmiana stanu strefy / PG jest sygnalizowana jedynie na danym segmencie. Ta opcja jest ustawieniem domyślnym.</td></tr>
<tr><td>5. Po wejściu i alarmie</td><td>Klawiatura sygnalizuje opóźnienie na wejście i alarm na danym segmencie. Zmiana stanu strefy / PG nie posiada żadnej sygnalizacji.</td></tr>
<tr><td>6. Wzbudzanie przez naciśnięcie</td><td>Klawiatura zapewnia sygnalizację świetlną i dźwiękową wyłącznie po otwarciu pokrywy przedniej; naciśnięcie przycisku, segmentu lub pokrywy przedniej</td></tr>
<tr><td colspan="2">Sygnalizuje zmiany stanu PG</td><td>Sygnalizacja świetlna zmian stanu wyjścia PG na segmencie. Jest powiązana z ustawieniami sygnalizacji — opcje 2–4. Jeżeli nieaktywna, zmiany stanu wyjścia PG nie otrzymują sygnalizacji świetlnej.</td></tr>
<tr><td colspan="2">Sygnalizuje stan Rozbrojony</td><td>Segmenty klawiatury sygnalizują stan rozbrojony bez prawidłowego uwierzytelnienia.
Jeżeli nieaktywne, sygnalizują ten stan wyłącznie podczas prawidłowego uwierzytelnienia.</td></tr>
<tr><td colspan="2">Sygnalizuje stan Uzbrojony</td><td>Segmenty klawiatury sygnalizują stan uzbrojony bez prawidłowego uwierzytelnienia.
Jeżeli nieaktywne, sygnalizują ten stan wyłącznie podczas prawidłowego uwierzytelnienia.</td></tr>
<tr><td colspan="2">Rozbrój strefę przez uwierzytelnianie wyłącznie podczas opóźnienia na wejście</td><td>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 strefy wspólnej zwykle włącza się opóźnienie na wejście. W przeciwnym razie w wyniku danego uwierzytelnienia zostaną rozbrojone wszystkie strefy przypisane do strefy wspólnej.</td></tr>
<tr><td colspan="2">Podświetlenie LCD gaśnie w ciągu 5 s</td><td>Jeżeli aktywne, podświetlenie wyświetlacza LCD zgaśnie w ciągu 5 sekund od ostatniej obsługi przy użyciu modułu (naciśnięcie przycisku, segmentu lub pokrywy przedniej). Jeżeli nieaktywne, podświetlenie zgaśnie w chwili zgaśnięcia całej klawiatury. Aktywacja wydłuża żywotność baterii.</td></tr>
</table>

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 segmentu z ustawieniem na cichy alarm panika lub alarm panika z sygnałem dźwiękowym. Naciśnięcie prawego (czerwonego) przycisku powoduje włączenie zegara, natomiast naciśnięcie lewego (zielonego) powoduje jego anulowanie. Kiedy uwierzytelnienie jest aktywne, jest ono wymagane także do aktywacji i dezaktywacji. Opóźnienie można ustawiać w zakresie od 1 do 255 sekund.

Wyświetl na LCD:

1. wiersz	Pozwala wprowadzić tekst, który wyświetli się w 1. wierszu ekranu LCD klawiatury przy braku wyświetlania innych ważniejszych informacji, np. nazwy firmy, nazwy budynku, opisu wyświetlanej temperatury itp.
2. wiersz	Pozwala wprowadzić tekst, który wyświetli się w 2. wierszu ekranu LCD klawiatury przy braku wyświetlania innych ważniejszych informacji, np. nazwy firmy, nazwy budynku, opisu wyświetlanej temperatury itp.
Data i godzina	Możliwość wyświetlania daty i godziny centrali alarmowej na ekranie LCD klawiatury.
Temperatura	Możliwość wyświetlania temperatury 1. termometru lub termostatu na ekranie.
Temperatura	Możliwość wyświetlania temperatury 2. termometru lub termostatu na ekranie.

Intensywność podświetlenia:

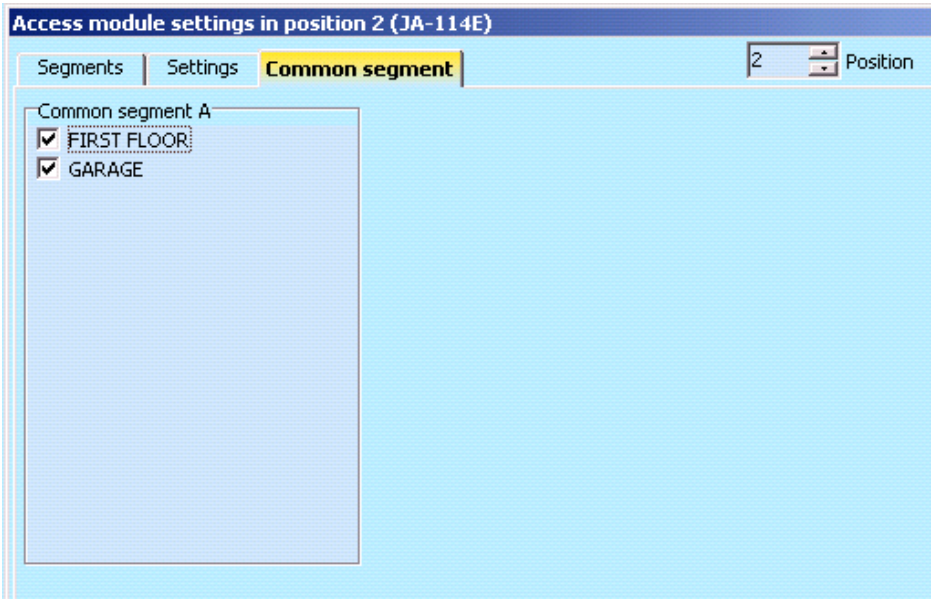
Segmenty	Dostosowanie podświetlenia LED na segmentach
Klawiatura	Regulacja podświetlenia klawiatury
Wyświetlacz	Konfiguracja podświetlenia wyświetlacza LCD

Uwaga: *Intensywność podświetlenia można ustawić odmiennie dla trybu dzień i noc, można wyciszyć także sygnalizację dźwiękową.*

Sygnalizacja dźwiękowa dla stref — pozwala zaznaczyć strefy, dla których aktywna będzie sygnalizacja dźwiękowa (alarmów, opóźnienia na wejście i wyjście, sterowanie wyjściem PG itp.).

Sterowanie strefami z menu — na klawiaturze mającej ekran LCD można określić, które strefy można aktywować lub dezaktywować z menu. W ten sposób można np. utworzyć klawiaturę, która zwykle steruje 2 strefami przy pomocy segmentów, ale w razie potrzeby może wykorzystać menu do sterowania innymi częściami domu, dla których zwykle nie ma zainstalowanych segmentów.

10.5.1.3 Zakładka Wspólny segment



Umożliwia jednoczesne sterowanie kilkoma strefami posiadającymi indywidualne segmenty na klawiaturze, połączone w jeden segment. Po naciśnięciu przycisku na tym samym segmencie polecenie Rozbrój/Uzbrój realizowane jest łącznie dla wybranych segmentów stref. Jeśli niektóre sekcje sterowane za pomocą wspólnego segmentu są uzbrojone, a inne rozbrojone, skorzystanie z Wspólnego segmentu spowoduje rozbrojenie / uzbrojenie pozostałych segmentów. Jeżeli dla jednego z wybranych segmentów aktywowano Uzbrojenie częściowe (szczegółowe informacje w rozdziale 9.2 Sterowanie systemem z klawiatury), Wspólny segment zachowa się następująco: 1. naciśnięcie Uzbrój = uzbrojenie częściowe, 2. naciśnięcie Uzbrój = uzbrojenie pełne. Wspólny segment umożliwia obejście aktywnej czujki w strefie, jeżeli jej tryb ustawienia to „Uzbraja z ostrzeżeniem" lub „Uzbraja po potwierdzeniu", bez wpływu na inne segmenty ustawione na „Uzbraja częściowo po pierwszym naciśnięciu i całkowicie po drugim" po drugim naciśnięciu.

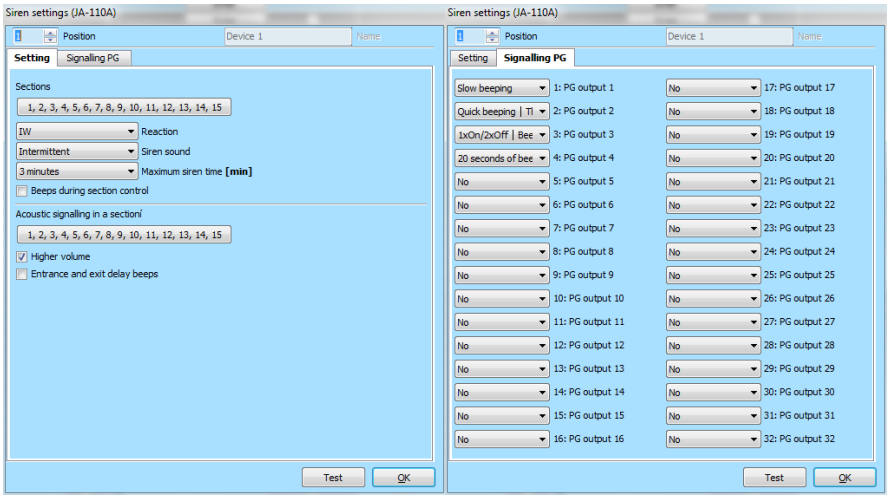
Sygnalizacja Wspólnego segmentu: Wszystkie strefy rozbrojone = zielony, wszystkie strefy w pełni uzbrojone = czerwony, dowolna strefa uzbrojona (częściowo) = żółty. Strefy do Wspólnego segmentu przypisuje się w górnej zakładce **Wspólny segment**.

Na klawiaturze mogą być najwyżej 2 segmenty wspólne. Wybrana strefa może być wspólna dla obu wspólnych segmentów.

Uwagi:

- „Wspólny segment" pojawia się jedynie, gdy do modułu podłączono więcej niż dwa segmenty do sterowania strefą.
- Nie należy łączyć funkcji Wspólnego segmentu z funkcją Strefa wspólna.

10.5.2 Przykładowe ustawienia syreny wewnętrznej



Sygnalizacja dźwiękowa alarmu włamania ze stref — służy do wyboru stref, dla których syreny będą sygnalizować alarm dźwiękiem.

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

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

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

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 sterowania strefą — dźwiękowe potwierdzenie zmian stanu strefy.

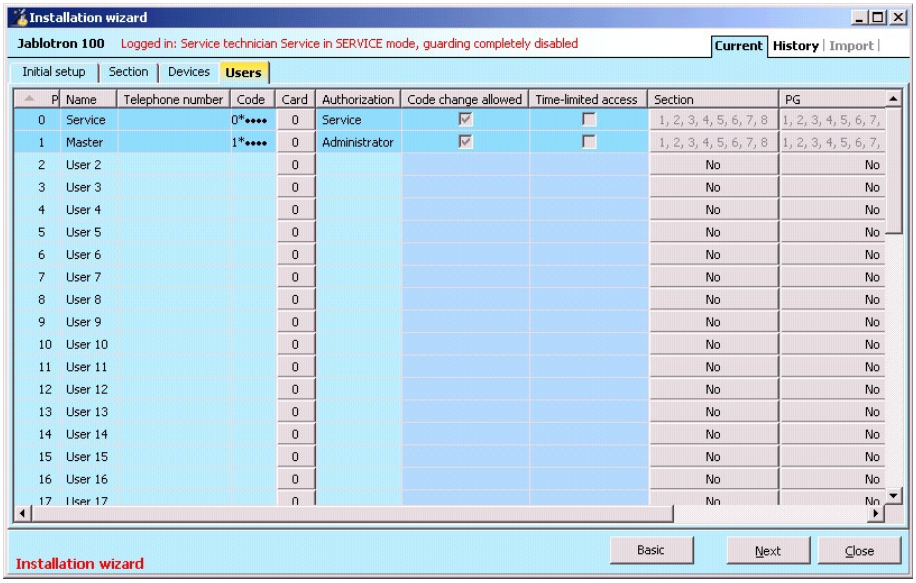
Pikanie sygnalizujące opóźnienie na wejście i wyjście — sygnalizacja dźwiękowa opóźnienia na wejście/wyjście.

Sygnalizacja PG — dźwiękowe potwierdzenie zmian wyjść PG wykorzystanych segmentów. Pozwala wybrać dźwięki przypisane do konkretnego wyjścia PG, aby rozróżnić je dźwiękowo, na przykład naciśnięcie przycisku dzwonka do drzwi ma dźwięk inny niż dźwięk wyjścia PG aktywowany po otwarciu drzwi.

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

10.6 Zakładka Użytkownicy

Służy do ustanawiania nowych użytkowników systemu i ustawiania ich praw. Zakładka wyświetli tyle pozycji, ile wybrano w zakładce **Konfiguracja początkowa**. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



* Pozycje oznaczone w ten sposób wyświetlają się przy włączonych **Ustawieniach zaawansowanych**.

Nazwa — nazwy użytkowników wykorzystuje się w tekstowych raportach zdarzeń w odczytach historii zdarzeń, w zakładkach raportów, ustawieniach uwierzytelniania lub do uwierzytelniania na klawiaturze lub do uwierzytelnienia na klawiaturze z ekranem LCD.

Numer telefonu — służy do raportowania zdarzeń oraz identyfikacji użytkowników podczas sterowania systemem z telefonu przy pomocy menu głosowego lub do aktywacji wyjść PG przez połączenie głosowe i SMS. Numer telefonu należy zawsze wprowadzać w formacie międzynarodowym (np. +420777123456).

Kod — kod dostępu użytkownika wprowadza się w formacie **p*cccc (p = prefiks (numer pozycji), * = separator, cccc = 4 cyfry kodu)**. Jeżeli prefiks jest nieaktywny (w zakładce Konfiguracja początkowa w F-Link), ma postać **cccc.** Kodu w pozycjach 0 i 1 nie można skasować (Serwis i Administrator główny). Kody mogą być 4-, 6- lub 8-cyfrowe.

Karta — służy do przypisywania kart dostępu RFID (breloków). Do każdego użytkownika można przypisać 2 karty. Karty można przypisać:

— przez wprowadzenie numeru seryjnego (można go odczytać za pomocą czytnika kodów paskowych z karty/breloka RFID).
— **za pomocą czytnika JA-190T** (podłączonego do portu USB komputera) przez przyłożenie 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.

Użytkownik modelowy — umożliwia kopiowanie wszystkich ustawień zależnie od użytkownika modelowego. Późniejsze zmiany ustawień użytkownika modelowego będą miały zastosowanie do wszystkich użytkowników ustawionych zgodnie z użytkownikiem modelowym.

Zmiana kodu dozwolona* — pozwala użytkownikowi zmienić własny kod (ale nie numer pozycji). Opcja jest dostępna wyłącznie po aktywacji parametru Kody z prefiksami (Administrator, Serwis i ARC mogą zmienić kod w dowolnej chwili).

Dostęp w ograniczonym czasie* — umożliwia ograniczenie dostępu użytkownika zgodnie z harmonogramem tygodniowym w zakładce **Strefy / Dostęp w ograniczonym czasie**, patrz rozdział 9.15 Dostęp w ograniczonym czasie dla użytkowników. Ograniczenie dostępu można zastosować jedynie dla użytkowników o poziomie uprawnień Użytkownik.

Strefa — określa, które strefy może definiować użytkownik (administrator). 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).

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

Raporty sterowania — pozwala użytkownikowi wysyłać raporty SMS na temat Uzbrajania/Rozbrajania przy sterowaniu dla klawiatury.

Wybór numeru aktywuje PG — okno informacji o przypisanym sterowaniu PG przez wybór numeru.

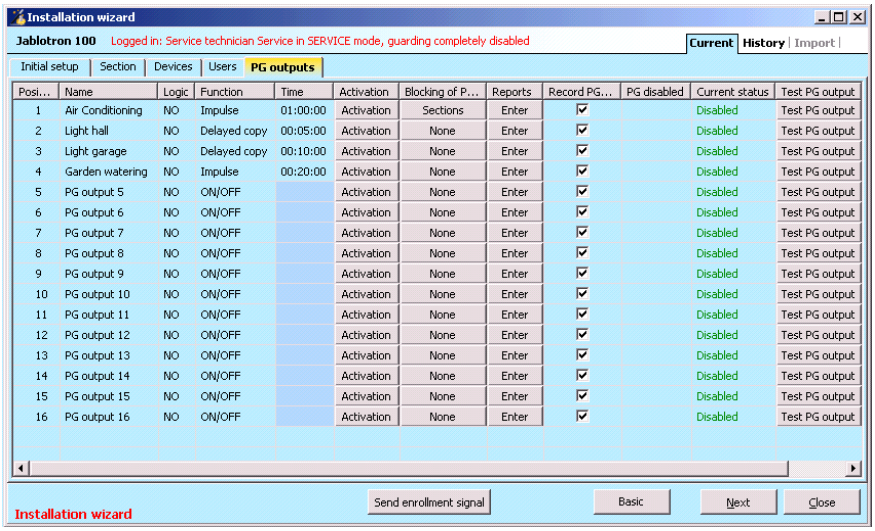
Dezaktywuj — możliwość zablokowania użytkownika. Nie można dezaktywować użytkownika w pozycji 0 (serwisant) i 1 (administrator główny). Dezaktywację użytkownika sygnalizuje czerwona kropka. Administrator (przy pomocy klawiatury LCD lub J-Link) oraz Serwisant (za pośrednictwem F-Link) mają prawo dezaktywować użytkowników.

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

Dostęp w ograniczonym czasie — przycisk służy do konfiguracji dostępu w ograniczonym czasie, patrz rozdział 9.15 Dostęp w ograniczonym czasie dla użytkowników.

10.7 Zakładka wyjścia PG

Służy do ustawiania funkcji wyjść programowalnych. Zakładka wyświetli tyle pozycji, ile wybrano w zakładce **Konfiguracja początkowa**. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



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

Logika — możliwość ustawiania odwróconej logiki wyjścia (NO = zwykle otwarte, NC = zwykle zamknięte).

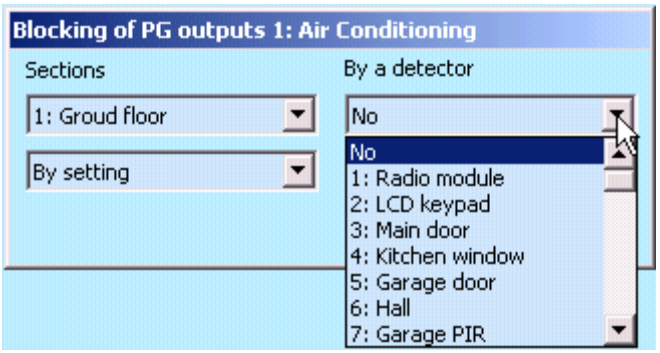
Funkcja — określa zachowanie wyjścia po aktywacji.

Impuls	Umożliwia aktywację z ograniczeniem czasowym (czas ustawia się w kolumnie Czas).
WŁ/WYŁ	Polecenie aktywacji spowoduje włączenie, polecenie dezaktywacji spowoduje wyłączenie przy braku sprawdzenia stanu źródła lub czasu trwania, ostatnie polecenie zawsze realizuje żądanie.
Kopiuj	Kopiuje aktywację czujki lub stan wewnętrzny. W przypadku żądania powyżej dwóch urządzeń stosuje się logikę OR.
Kopia opóźniona	Wysyła polecenie jedynie, gdy warunek aktywacji pozostaje w mocy dłużej niż ustawiono w kolumnie Czas (służy np. do sygnalizacji zapomnienia o zamknięciu bramy garażu).
Kopia poszerzona	Kopiuje aktywację urządzenia (lub stan wewnętrzny) i przedłuża ją o czas ustawiony w kolumnie Czas (służy np. do oświetlenia korytarza po otwarciu drzwi).
Zmień	Po aktywacji następuje odwrócenie bieżącego stanu PG na przeciwny (służy wyłącznie do sterowania impulsowego, np. za pomocą przycisku manipulatora zdalnego).

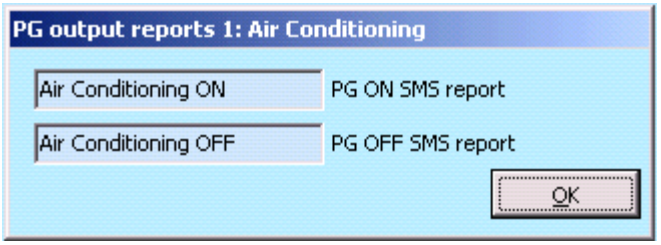
Czas — ustawienie czasu dla funkcji Impuls, Kopiuj po opóźnieniu i Kopiuj z nakładaniem. Czas ustawia się w formacie *gg:mm:ss* w zakresie od 00:00:01 do 23:59:59.

Aktywacja — Otwarcie Mapy aktywacji wyjścia PG — patrz rozdział 10.7.1 Activation Map of a PG outputs.

Blokowanie PG — umożliwia blokowanie wyjścia PG stanem strefy, czujką lub innym 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 stanu strefy można wybrać, czy blokowanie ma nastąpić w chwili, gdy strefa jest uzbrojona czy rozbrojona, a w przypadku blokowania za pomocą urządzenia lub innego wyjścia PG, czy ma nastąpić w wyniku jego aktywacji czy dezaktywacji. Wszystkie opcje blokowania można wykorzystać jednocześnie.



Raporty — ustawienie tekstów raportów SMS wysyłanych w chwili aktywacji lub dezaktywacji wyjścia PG. W zakładce Raporty użytkowników ustawia się użytkowników, do których wysyłany jest każdy z raportów. Zmienione teksty raportów rejestrowane są w dzienniku, w związku z czym nie można ich całkowicie usunąć.



Rejestracja PG w pamięci — umożliwia rejestrację aktywacji PG w historii zdarzeń, a tym samym także raportowanie SMS do użytkowników i komunikację ze SMA (np. do monitorowania wejścia użytkowników przez monitorowane drzwi, rejestracja w aplikacji MyJABLOTRON itp.)

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

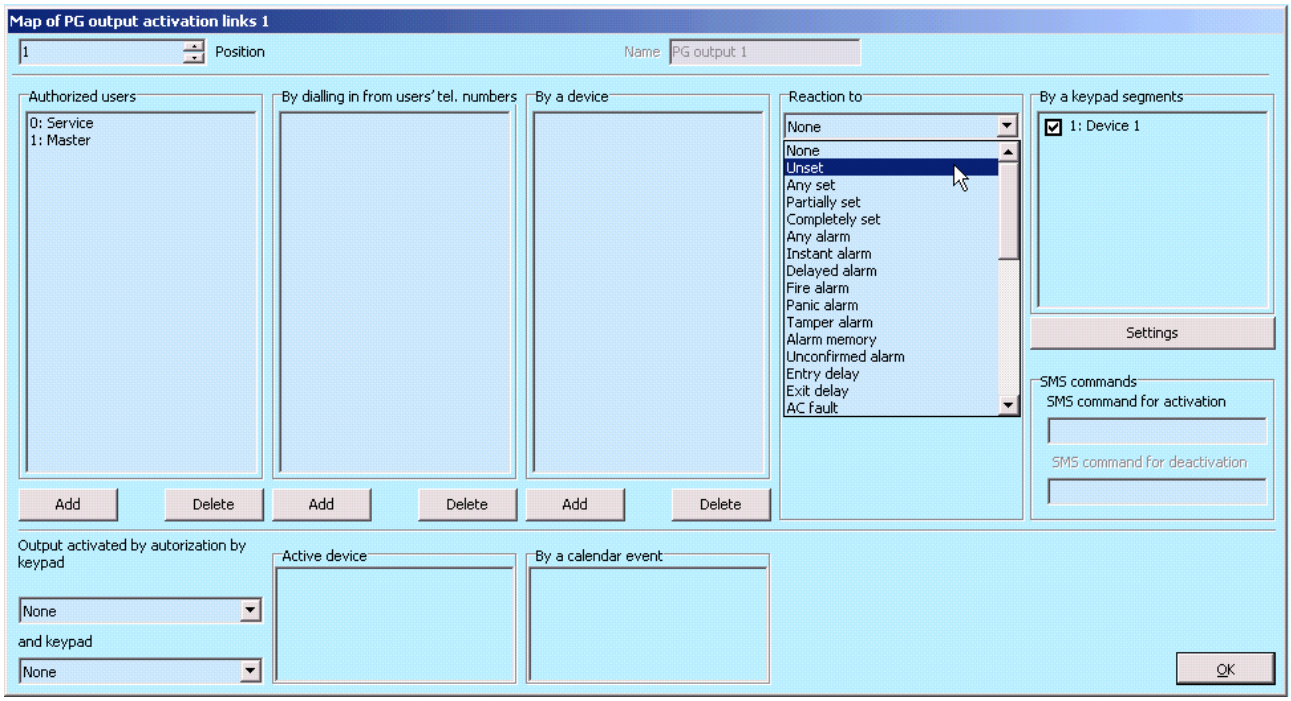
Aktualny stan — oznaczone kolorami informacje na temat aktualnego stanu wyjścia PG. Opis w kolorze zielonym odpowiada zielonej kontrolce segmentu, opis w kolorze czerwonym odpowiada czerwonej kontrolce segmentu.

Test — możliwość sterowania wyjściem ręcznie z komputera. 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.

10.7.1 Mapa aktywacji wyjść PG

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



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

Upoważnieni użytkownicy — określa użytkowników uprawnionych do sterowania wyjściem PG z wymaganiem uwierzytelnienia z klawiatury (za pomocą przycisków segmentów), z aplikacji MyJABLOTRON lub polecenia SMS. Ustawienia są powiązane z zakładką Użytkownicy.

W drodze uwierzytelnienia użytkownika z klawiatury — pozwala skonfigurować najwyżej 2 klawiatury aktywujące wyjście PG samym uwierzytelnieniem (zastosowanie karty/kodu lub wprowadzenie kodu). Ta funkcja jest przeznaczona do otwarcia zamka w drzwiach (tj. nie jest konieczna obsługa przycisków segmentu). Ta funkcja jest dostępna jedynie, gdy funkcję wyjścia ustawiono na Impuls.

Przez połączenie głosowe z numerów telefonu użytkownika — z określeniem użytkowników uprawnionych do aktywacji wyjścia PG przez połączenie z własnego telefonu (numery telefonu wpisano w zakładce Użytkownicy). Numery telefonu stosowane do aktywacji przez połączenie dźwiękowe nie mogą być ukryte (usługa CLIP nie może zostać wyłączona). Termin „połączenie dźwiękowe" oznacza, że po wybraniu numeru telefonu osoba dzwoniąca czeka przez co najmniej jeden sygnał dźwiękowy (jednakże zgodnie z ustawieniem odbierania, patrz liczba sygnałów dźwiękowych dla połączeń przychodzących w ustawieniach komunikatora) i kończy połączenie. 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.

Reakcja na — umożliwia aktywację wyjścia przez wybrane zdarzenie w systemie (np. uzbrojenie, alarm, awaria zasilania, błąd itp.). Dla stanu wewnętrznego (łącznie 39 stanów wewnętrznych, patrz poniższa tabela) można ustawić grupę stref, z których sygnał zostanie przyjęty (logika OR). Dane wyjście PG można ustawić ma kopiowanie stanu innego wyjścia PG lub kilku innych wyjść z możliwością wyboru wzajemnej logiki (OR lub AND). Ostatnia pozycja w menu „Zdarzenie w systemie" umożliwia ustawienie aktywacji wyjścia i jego dezaktywacji w odpowiedzi na całkowicie inne zdarzenie (np. aktywacja w przypadku alarmu, ale dezaktywacja samym rozbrojeniem).

Za pomocą segmentu klawiatury — pokazuje listę klawiatur i manipulatorów zdalnych w systemie. Za pomocą przycisku Ustawienia (pod listą klawiatur) można wejść do menu wewnętrznego wybranej klawiatury i dostosować jej ustawienia, patrz rozdział 10.5.1 Keypad configuration.

Za pomocą poleceń SMS — pozwala ustawić polecenia tekstowe do aktywacji i dezaktywacji wyjścia PG telefonicznie. Odbiór danej wiadomości SMS ma skutek podobny do naciśnięcia przycisku Uzbrój lub Rozbrój na segmencie kontrolnym klawiatury. Do sterowania wyjściami należy użyć SMS w formacie **kod_polecenie**, np. **2*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.

Aktywne urządzenie — wykaz urządzeń aktywowanych danym wyjściem PG, na przykład zdjęcie z PIR z kamerą (tylko okno informacyjne, funkcję należy ustawić w ustawieniach wewnętrznych urządzenia).

Przez czynność z kalendarza — wykaz planowanych czynności z kalendarza, które aktywują lub dezaktywują, lub blokują dane wyjście PG (okno informacji)

Ostrzeżenie 1: *Centrala alarmowa JA-107K zapewnia 128 wyjść PG. Bezprzewodowe czujki PG można przypisać jedynie w wyjściach od 1 do 32. Wszystkie 128 wyjść PG można wykorzystać do modułów MAGISTRALI.*

Ostrzeżenie 2: *Wyjścia PG nie działają, jeżeli system znajduje się w trybie serwisowym. Naciśnięcie przycisku Test pozwala sprawdzić wszystkie wyjścia PG. W chwili aktywacji trybu serwisowego następuje dezaktywacja wszystkich wyjść PG. Po opuszczeniu trybu serwisowego może nastąpić ich ponowna aktywacja, z wyjątkiem Ostrzeżenia 3.*

Ostrzeżenie 3: *Jeżeli wprowadzono ustawienie Parametry / Po uruchomieniu F-Link należy automatycznie aktywować tryb serwisowy i jeżeli w chwili połączeniu centrali alarmowej z F-Link w oknie Ostrzeżenia wybrano pozycję Rozbrój, po tym bezpośrednim wejściu w tryb serwisowy F-Link nie rejestruje jakichkolwiek możliwych wyjść PG z aktywacją impulsową (np. aktywowanych segmentem klawiatury i funkcją Aktywuj/Dezaktywuj lub ustawieniem w harmonogramie). Oznacza to, że po opuszczeniu trybu serwisowego nie pojawia się także pytanie, czy należy ponownie aktywować takie wyjścia PG.*

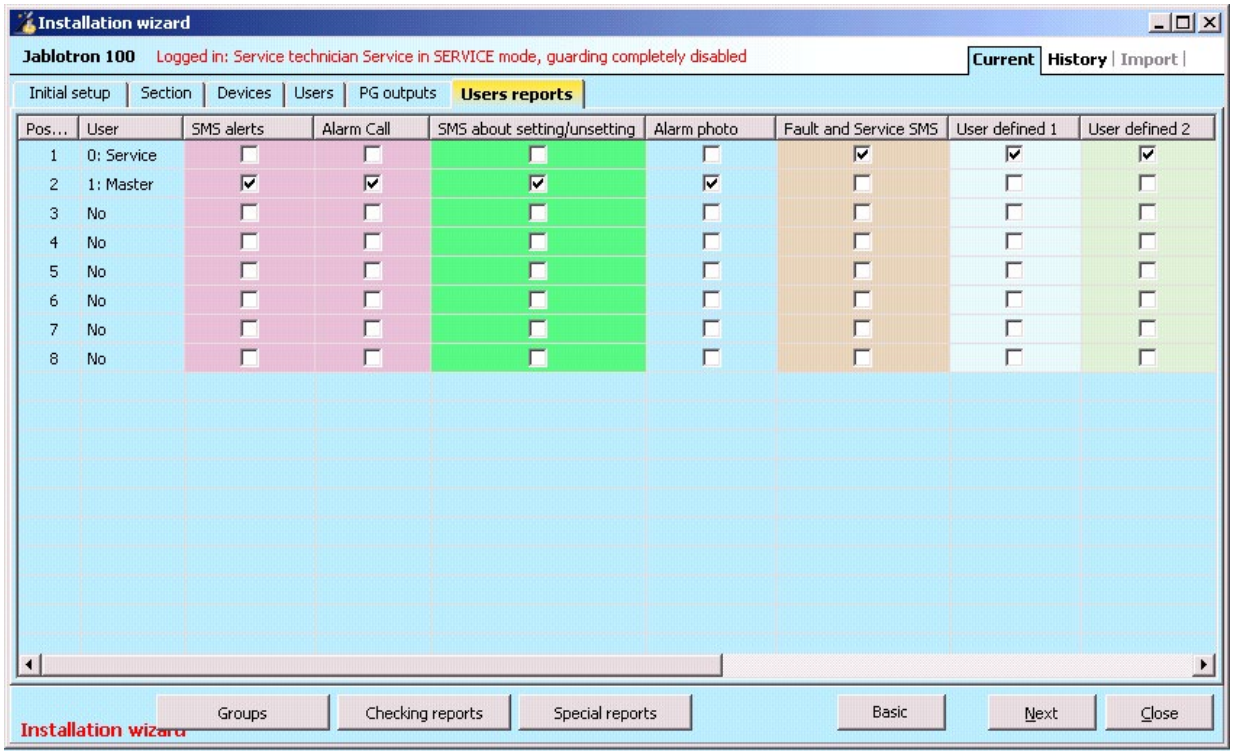
Stany wewnętrzne do sterowania wyjściami PG:

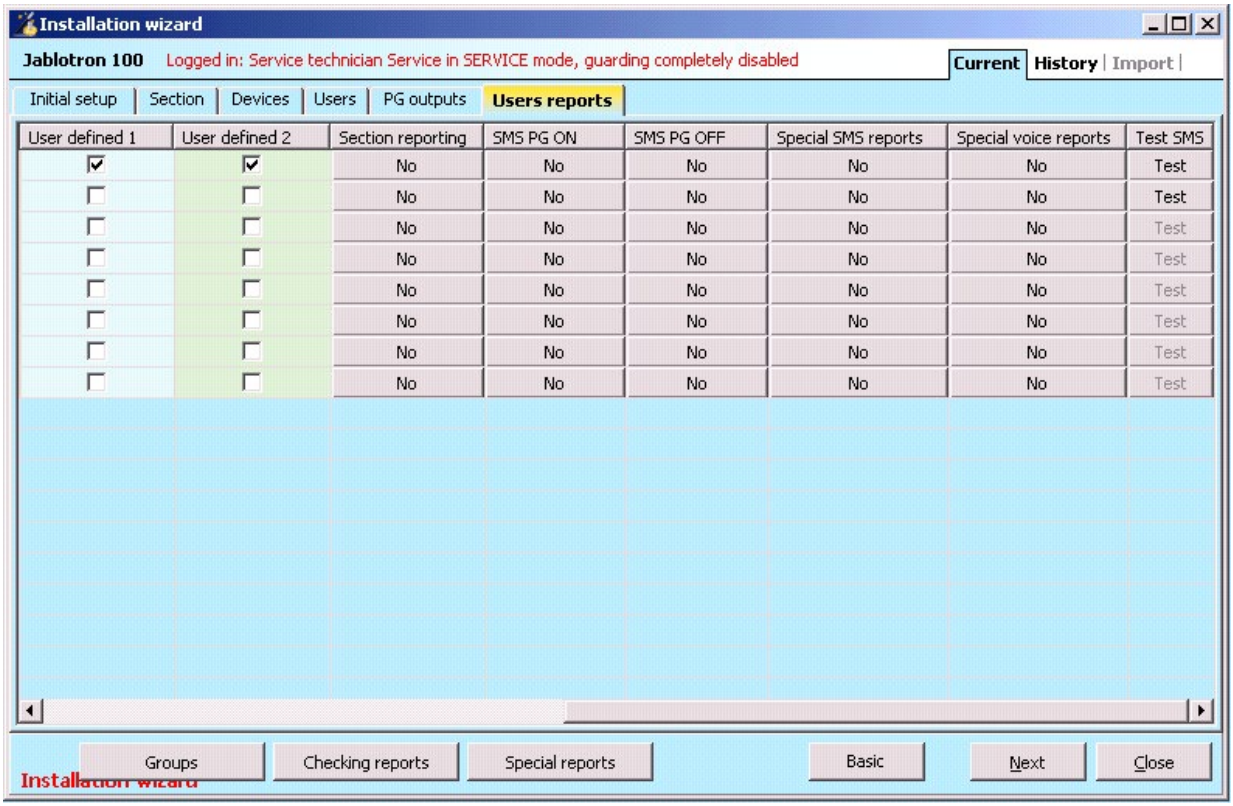
1. Rozbrój	14. Opóźnienie na wyjście	27. Urządzenie z aktywnym sabotażem
2. Dowolny uzbrojony	15. Awaria prądu stałego	28. Brak ruchu w strefie
3. Częściowo uzbrojona	16. Awaria prądu stałego przez 30 minut	29. Gotowe do uzbrojenia
4. Całkowicie uzbrojona	17. Awaria baterii awaryjnej	30. Gotowe do uzbrojenia częściowego
5. Dowolny alarm	18. Ostrzeżenie wewnętrzne (IW)	31. Niepowodzenie uzbrojenia
6. Alarm natychmiastowy	19. Ostrzeżenie zewnętrzne (EW)	32. Żądanie kontroli corocznej
7. Alarm opóźniony	20. Błąd	33. Błąd GSM
8. Alarm pożarowy	21. Aktywna czujka	34. Błąd LAN
9. Alarm panika	22. Uruchomiona dowolna czujka poza czujką z opóźnieniem	35. Błąd PSTN
10. Alarm sabotażowy	23. Aktywna czujka z opóźnieniem	36. Tryb nocny
11. Pamięć alarmu	24. Pominięcie w strefie	37. Tryb konserwacji
12. Alarm niepotwierdzony	25. Utrata urządzenia na 20 minut	38. Inne PG
13. Opóźnienie na wejście	26. Niski poziom baterii w urządzeniu	39. Zdarzenie w systemie

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

10.8 Zakładka Raporty użytkowników

Ta zakładka służy do określania użytkowników, którym system będzie zgłaszał wybrane grupy zdarzeń w formie SMS lub wiadomości głosowych na telefony. Grupy i format SMS opisano w tabeli 9.13 Zdarzenia zgłaszane użytkownikom. Podstawową strukturę menu głosowego opisano w załączonej tabeli w rozdziale 9.5 Sterowanie systemem za pośrednictwem menu głosowego komunikatora (GSM). 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 przypadku których wysyłany jest raport o zdarzeniu alarmowym w wybranej strefie, awarii lub przywróceniu zasilania po upływie 30 minut, uzbrojeniu z otwartą strefą lub ewentualnie raport o rozbrojonej strefie bez ruchu (patrz zakładka Strefy).

Połączenie alarmowe — grupa raportów, w których przypadku (po wysłaniu raportów SMS) system przekazuje użytkownikowi alarmowy komunikat głosowy. Połączenie dźwiękowe trwa około 30 sekund. Jeżeli nie zostanie odebrane, system wybierze numer kolejnego użytkownika. Odebranie połączenia powoduje wielokrotne przesyłanie komunikatu głosowego. Struktura komunikatu jest następująca: 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. Strukturę menu głosowego opisano w rozdziale 9.5 Sterowanie systemem za pośrednictwem menu głosowego komunikatora (GSM).

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 zostanie zgłoszone użytkownikowi, który go dokonał (jednakże można ustawić jego zgłaszanie w zakładce Użytkownicy). Wyjątek stanowi uzbrojenie strefy wspólnej (dokonane przez centralę alarmową, nie przez użytkownika).

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

SMS 1 definiowany przez użytkownika — specjalna pierwsza grupa, gdzie instalator może przesłać pewne zdarzenia przeznaczone do zgłoszenia (zwykle raporty o awariach i przywróceniu zasilania lub ewentualnie uzbrojeniu z aktywnym urządzeniem) wyłącznie wybranym użytkownikom.

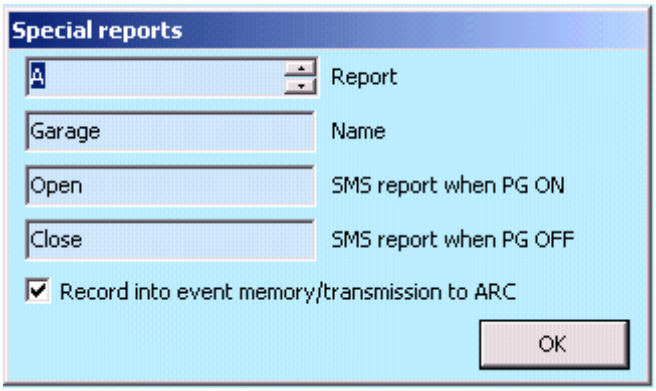
SMS 2 definiowany przez użytkownika — specjalna druga grupa, gdzie instalator może przesłać pewne zdarzenia do zgłoszenia (zwykle niski poziom baterii w urządzeniach lub niski poziom baterii awaryjnej) wyłącznie wybranym użytkownikom.

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

SMS PG WŁ* — możliwość raportowania aktywującego wyjścia PG do użytkownika. Komunikaty są wysyłane ze stałym opóźnieniem 60 sekund. Teksty komunikatów SMS ustawia się w zakładce Wyjścia PG, patrz rozdział 10.7 PG outputs tab.

SMS PG WYŁ* — możliwość raportowania dezaktywującego wyjścia PG do użytkownika. Komunikaty są wysyłane ze stałym opóźnieniem 60 s. Teksty komunikatów SMS ustawia się w zakładce Wyjścia PG, patrz rozdział 10.7 PG outputs tab.

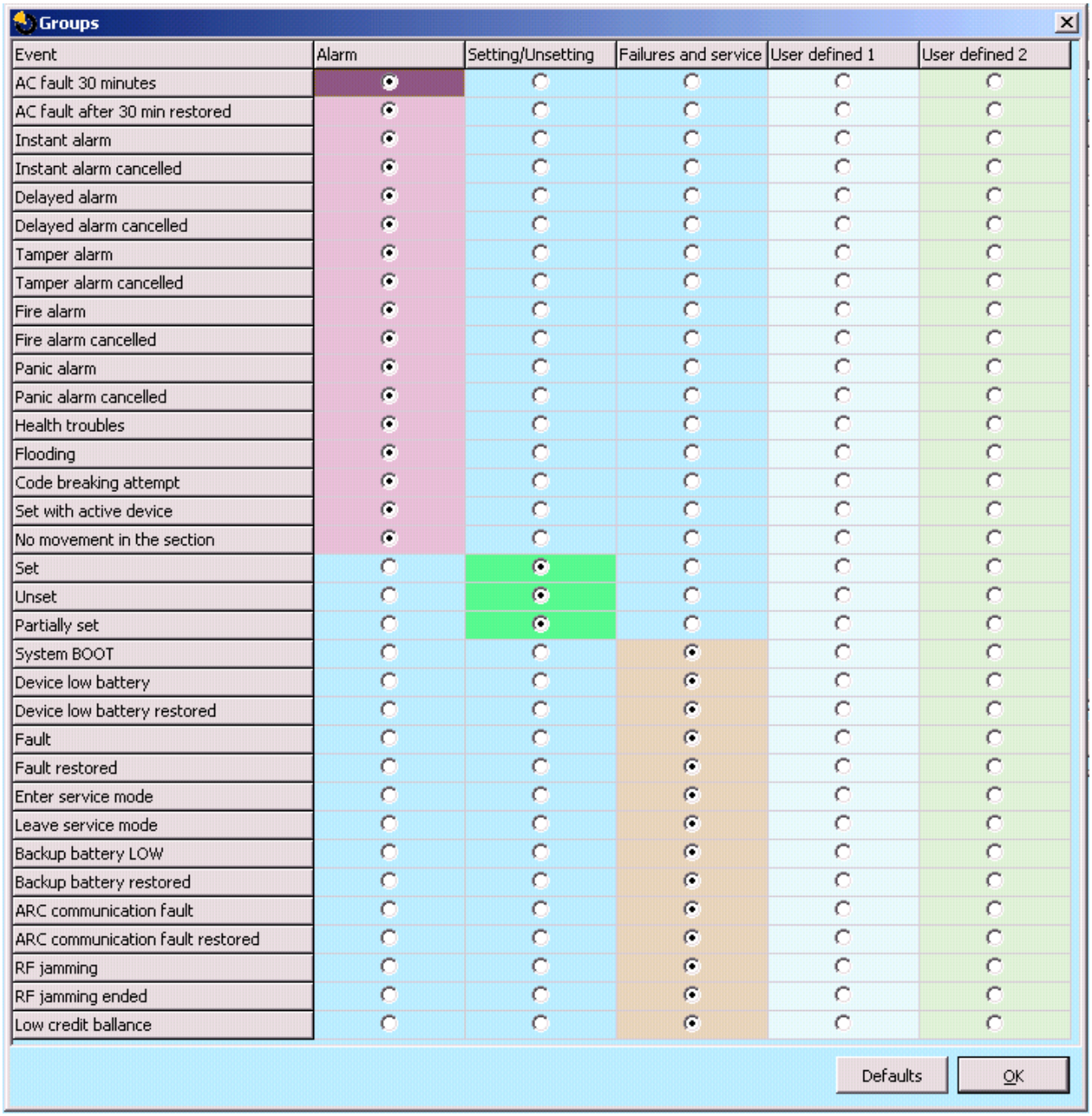
SMS Raporty specjalne* — możliwość raportowania aktywacji czujek, dla których ustawiono reakcję Raport specjalny (A, B, C lub D) do użytkownika za pomocą wiadomości SMS. Teksty raportów specjalnych ustawia się przy pomocy przycisku **Raporty specjalne** z prawej strony na dole zakładki Raporty do użytkowników.

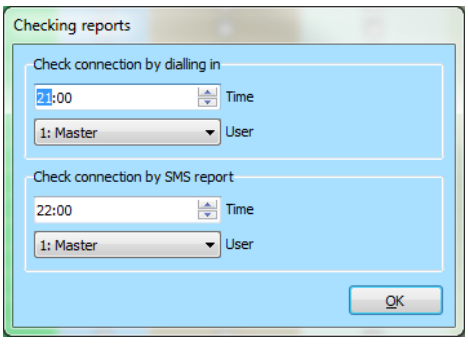


Raporty specjalne głosowe* — możliwość raportowania aktywacji czujek, dla których ustawiono reakcję Raport specjalny (A, B, C lub D) do użytkownika za pomocą komunikatu głosowego. Komunikaty głosowe można nagrać ponownie przez wykonanie połączenia z numerem telefonu centrali alarmowej, gdzie po odebraniu połączenia i uwierzytelnieniu za pomocą kodu administratora można użyć przycisku 9, aby wejść do nagrywania komunikatów głosowych, patrz rozdział 9.5 System control via communicator voice menu (GSM).

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

Tabela zdarzeń i zadanych grup:

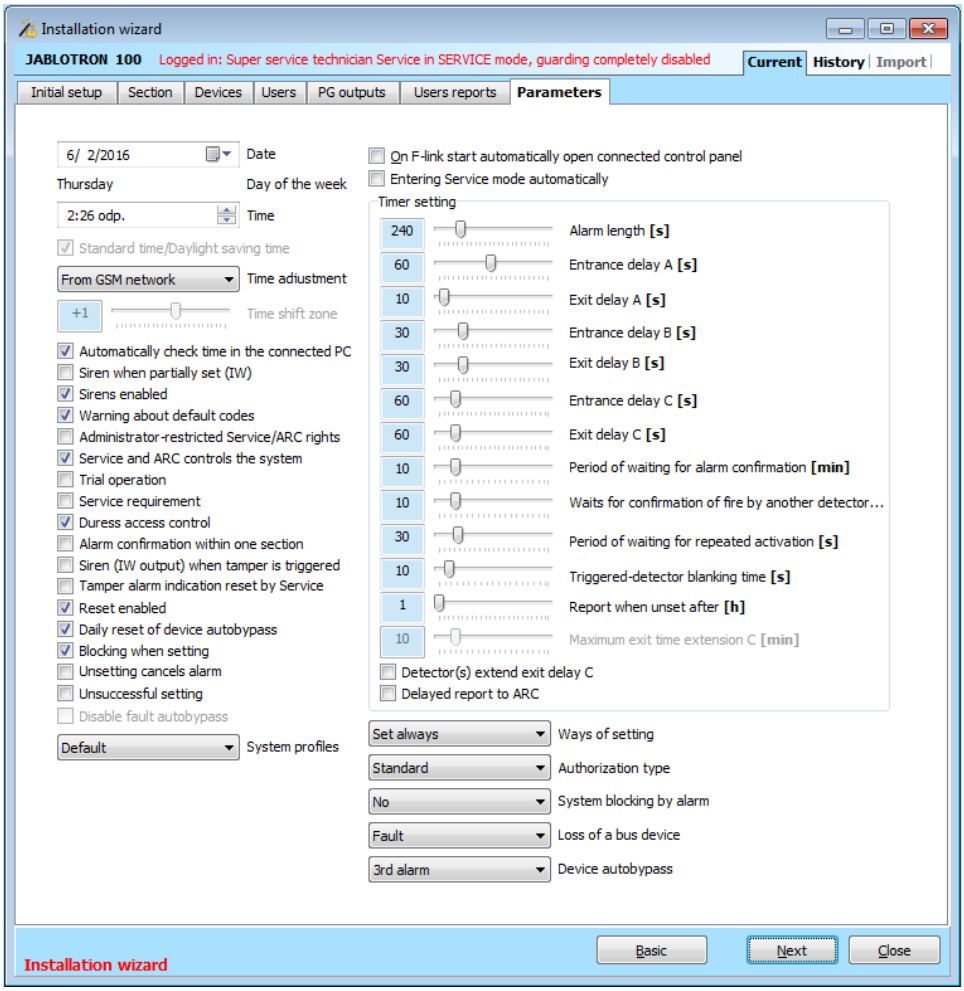




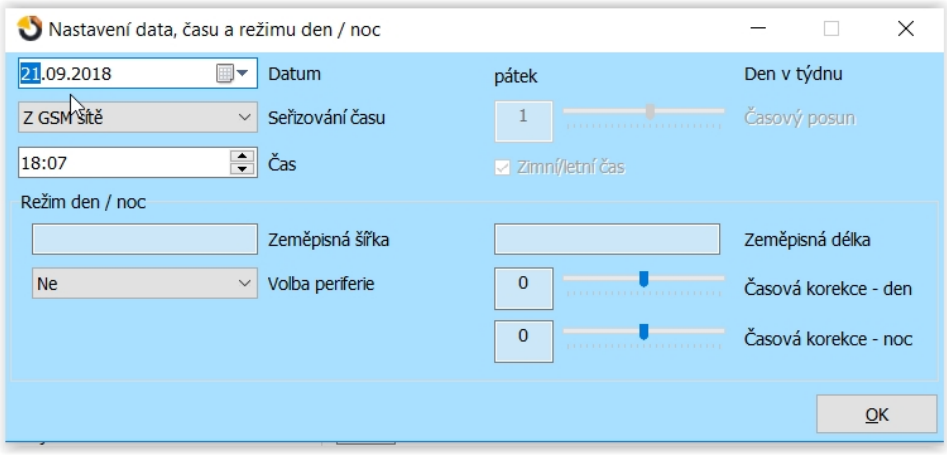
Raporty specjalne — Przycisk na dolnym pasku narzędzi do otwierania tabeli programowania, służący do konfiguracji nazwy, SMS-ów do aktywacji/dezaktywacji i opcji ponownego kodowania raportów od A do D w pamięci zdarzeń, będących reakcją strefy, patrz rozdział 8.4.2 List of applicable reactions.

10.9 Zakładka Parametry

Służy do ustawiania parametrów i wybieralnych funkcji centrali alarmowej. Zakładka jest identyczna z zakładką Urządzenia / Centrala alarmowa / Ustawienia wewnętrzne. Aby wprowadzić większość zmian w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



Po naciśnięciu przycisku **Data/Godzina**



* Pozycje oznaczone w ten sposób wyświetlają się przy włączonych **Ustawieniach zaawansowanych**.

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

Data		Wewnętrzne ustawienie kalendarza.	
Dzień tygodnia		Wyświetlanie dnia tygodnia.	
Regulacja czasu*		Sposób regulacji wewnętrznego czasu i daty:	
		Ręcznie	Ręczne ustawianie godziny i daty (przy użyciu programu F-Link lub J-Link).
		Z sieci GSM	Godzinę i datę pobiera się od dostawcy usług GSM przy każdym logowaniu do sieci GSM.
		Z serwera JABLOTRON	Godzinę i datę reguluje się automatycznie zgodnie z serwerem komunikacji (GMT 0). Opcja nic nie robi, gdy typ komunikacji ustawiono na „Bez programowania zdalnego” (ustawienie domyślne).
Zmiana czasu		Ustawianie zmiany czasu ze strefy czasowej GMT 0.	
Godzina		Wewnętrzne ustawienie zegara.	
Czas standardowy / Czas zimowy*		Do ręcznej regulacji czasu można wybrać jedynie automatyczne przełączanie 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).	
Tryb dzienny/nocny	**Szerokość geograficzna**	Format wprowadzania xx.xxxxxxN (np. 50.729058N)	
	Długość geograficzna	Format wprowadzania xx.xxxxxxE (np. 15.176636E)	
	Wybór urządzenia	Aktywacja wybranego urządzenia przełącza centralę alarmową w tryb nocny.	
	Korekta czasu Dzień	Opcja korekty czasu do przełączania w tryb dzienny.	
	Korekta czasu Noc	Opcja korekty czasu do przełączania w tryb nocny.	
Automatycznie sprawdzić czas w podłączonym komputerze*		Jeżeli zegar komputera i centrali alarmowej różni się o ponad 1 minutę, F-Link ostrzeże użytkownika o tym fakcie.	
IW syreny przy uzbrojeniu częściowym		Pozwala ustawić alarm dźwiękowy przy systemie IW, jeżeli strefa jest częściowo uzbrojona (nie dotyczy alarmów pożarowych i 24 godziny).	
Syreny aktywne*		Aktywuje wszystkie syreny MAGISTRALI i bezprzewodowe systemu (przeznaczone do dezaktywacji alarmu dźwiękowego podczas testów systemu).	
Ostrzeżenie o kodach domyślnych*		Po ukończeniu serwisu do serwisanta w pozycji 0 wysyłana jest wiadomość SMS informująca, że w systemie pozostawiono kody domyślne.	
Serwis ograniczony do Administratora i SMA		Blokuje niezależny dostęp serwisantów i SMA do systemu. 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 technika z centralą alarmową za pomocą przewodu USB administrator może dokonać zdalnego uwierzytelnienia przy pomocy 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 uprawnień do sterowania strefami i będzie w stanie wejść w tryb serwisowy jedynie po rozbrojeniu wszystkich stref przez Administratora lub użytkownika.	
Działanie próbne		Wszystkie alarmy są ograniczone do 60 sekund i raportowane za pomocą wiadomości SMS do zdefiniowanych użytkowników i serwisanta (pozycja 0), choć dla niego nie aktywowano raportów alarmów. Działanie próbne zostaje zakończone automatycznie po upływie 7 dni od opuszczenia trybu serwisowego.	
Wymagany serwis		Jeżeli ta funkcja jest włączona, 12 miesięcy od ostatniego zamknięcia trybu serwisowego uruchamia zdarzenie „System wymaga przeglądu serwisowego”, co wyświetla się na klawiaturach z ekranem LCD wraz z ikoną Informacja i jest rejestrowane w historii zdarzeń. Po naciśnięciu	

	przycisku „i” wyświetli się tekst „wezwij serwisanta” z jego numerem telefonu. Wiadomość na wyświetlaczu LCD znika automatycznie, gdy serwisant uzyska zdalny dostęp do systemu. Wówczas licznik sprawdzania rocznego wyzeruje się.
Tryb konserwacji	Pozwala Administratorom na przełączenie systemu w tryb konserwacji.
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 intruza. Alarm Panika aktywuje się podczas sterowania systemem przez wprowadzenie kodu, do którego ostatniej cyfry dodano 1. Ta funkcja jest dostępna w przypadku kodów z prefiksem i bez niego. **Przykład:** kod użytkownika z prefiksem = 4*4444, w przypadku antynapadowej kontroli dostępu wpisać 4*444**5**; kod użytkownika bez prefiksu = 4444, w przypadku antynapadowej kontroli dostępu wpisać 444**5**. **Przestroga:** Gdy ostatnią cyfrą kodu użytkownika jest 9, w kodzie antynapadowej kontroli dostępu należy ją zastąpić **0**.
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 uzbrojonej. W przypadku w pełni uzbrojonej syrena zawsze sygnalizuje alarm sabotażu.
Sygnalizacja alarmu sabotażu resetowana przez Serwis*	Sygnalizacje pamięci sabotażu może zresetować wyłącznie serwisant lub serwisant SMA. Jeżeli ta opcja nie jest zaznaczona, sygnalizację może zresetować także Administrator (ale nie Użytkownik).
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.
Dobowe resetowanie auto-pominięcia urządzenia*	Ta opcja odnosi się jedynie do wejść aktywacji (ale nie do wejść sabotażu i błędu). Jeżeli ta opcja jest aktywna, system automatycznie zresetuje urządzenia pominięte, codziennie o godzinie 12:00. Jeżeli ta opcja nie jest aktywna, auto-pominięcie urządzenia zostanie zresetowane wyłącznie przy zmianie stanu systemu. Ta opcja służy np. do używania czujek z reakcją 24 h lub czujek zalania znajdujących się w strefie, gdzie uzbrojenie/rozbrojenie nie jest konieczne.
Blokowanie podczas uzbrajania	Jeżeli jest aktywne, nastąpi blokowanie wszystkich aktywnych wejść podczas uzbrajania strefy, w okresie takiej ochrony nie mogą aktywować alarmu. Jeżeli nie jest aktywne, nastąpi czasowe pominięcie wszystkich aktywnych wejść do chwili, gdy przejdą one w tryb czuwania, a czujki ponownie rozpoczną strzeżenie (ryzyko aktywacji fałszywego alarmu, np. nieprawidłowo zamknięte okno).
Rozbrojenie anuluje alarm	Funkcja określająca, czy alarm zostanie anulowany przez uwierzytelnienie wyłącznie prawidłowym kodem, czy też przez rozbrojenie strefy, gdzie wystąpił alarm. Jeżeli jest aktywne, alarm można anulować przez rozbrojenie strefy, w której aktywowano alarm lub z menu klawiatury LCD przyciskiem „Anuluj ostrzeżenie”.
Niepowodzenie uzbrojenia	Przetwarzanie tej funkcji zachodzi podczas każdej procedury uzbrajania. W przypadku aktywacji natychmiastowej w czasie opóźnienia na wyjście lub otwarcia strefy z opóźnieniem po wygaśnięciu czasu na wyjście nie nastąpi uzbrojenie systemu i aktywuje się zdarzenie „Niepowodzenie uzbrajania”, które zostanie zarejestrowane w historii. To zdarzenie zostanie zgłoszone także za pomocą SMS na numer zadanego użytkownika pod warunkiem aktywacji wysyłania zdarzenia „SMS o niepowodzeniu uzbrojenia”. Wskazują je klawiatury oraz syrena zewnętrzna. Aby anulować sygnalizację niepowodzenia uzbrojenia, należy nacisnąć „Anuluj ostrzeżenie” w menu klawiatury LCD.

Auto-pominięcie usterki	Jest dostępne jedynie, gdy wybrano jeden z profili systemu „EN50131-1" lub „INCERT". Służy do dezaktywacji ograniczonej liczby aktywnych usterek od maks. 3 błędów do liczby nieograniczonej.	
Profile systemu	Wybór z zadanych profili systemu zgodnie z wymogami.	
	Domyślny	Parametry ustawione na domyślną wartość fabryczną, z opcją modyfikacji zależnie od potrzeb.
	EN50131-1, Klasa 2	Niektóre parametry zostają zadane automatycznie w celu zapewnienia zgodności z normą EN50131-1, klasa 2 (ryzyko niskie – średnie), bez możliwości modyfikacji.
	INCERT, klasa 2	Niektóre parametry zostają zadane automatycznie w celu zapewnienia zgodności 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, do najwyższego poziomu, kiedy systemu nie można uzbroić z aktywnymi urządzeniami (alarm natychmiastowy). Powiązane z opcją profilu systemu.	
	Uzbrój zawsze	Uzbraja zawsze niezależnie od stanu systemu (błędy, aktywne urządzenia itp.).
	Uzbrój z ostrzeżeniem	Sygnalizuje optycznie (na segmencie i wyświetlaczu) stan systemu (błędy, aktywne urządzenia itp.) przez 8 sekund, a po zakończeniu tego okresu uzbraja automatycznie. Uzbrojenie jest możliwe także przez wielokrotne naciśnięcie segmentu lub klawisza ENTER.
	Uzbrój po potwierdzeniu	Sygnalizuje optycznie (segment i wyświetlacz) stan systemu (błędy, aktywne urządzenia itp.) przez 8 sekund. Można uzbroić WYŁĄCZNIE wielokrotnym naciśnięciem segmentu lub naciśnięciem klawisza ENTER.
	Nie uzbrajać z aktywnym elementem	Sygnalizuje optycznie (segment i wyświetlacz) stan systemu (błędy, aktywne urządzenia itp.) przez 8 sekund. Można uzbroić, wielokrotnie naciskając segment 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 MyJABLOTRON, czynność z kalendarza z wyjątkiem „Uzbrój zawsze").
Typ uwierzytelniania	Wybór sposobu, w jaki system przetwarza uwierzytelnienie użytkownika. Powiązane ze sterowaniem wyjściem PG po uwierzytelnieniu.	
	Standardowy	Wprowadzenie kodu użytkownika lub korzystanie z karty/breloka RFID zapewni poprawne uwierzytelnienie. Do sterowania systemem konieczna jest tylko jedna z tych opcji.
	Potwierdzenie karty kodem	Użytkownicy posiadający przypisane karty i kody muszą dokonać uwierzytelnienia za pomocą obu tych metod (niezależnie od kolejności uwierzytelnienia). Jeżeli użytkownicy posiadają karty lub kody, przeprowadzą uwierzytelnienie zgodnie z opcją Standardową. Dostęp zdalny telefoniczny jest aktywny jedynie dla uprawnionych numerów.
	Uwierzytelnianie podwójne	Wprowadzenie kodu użytkownika i korzystanie z karty RFID zapewni poprawne uwierzytelnienie (niezależnie od kolejności uwierzytelniania).

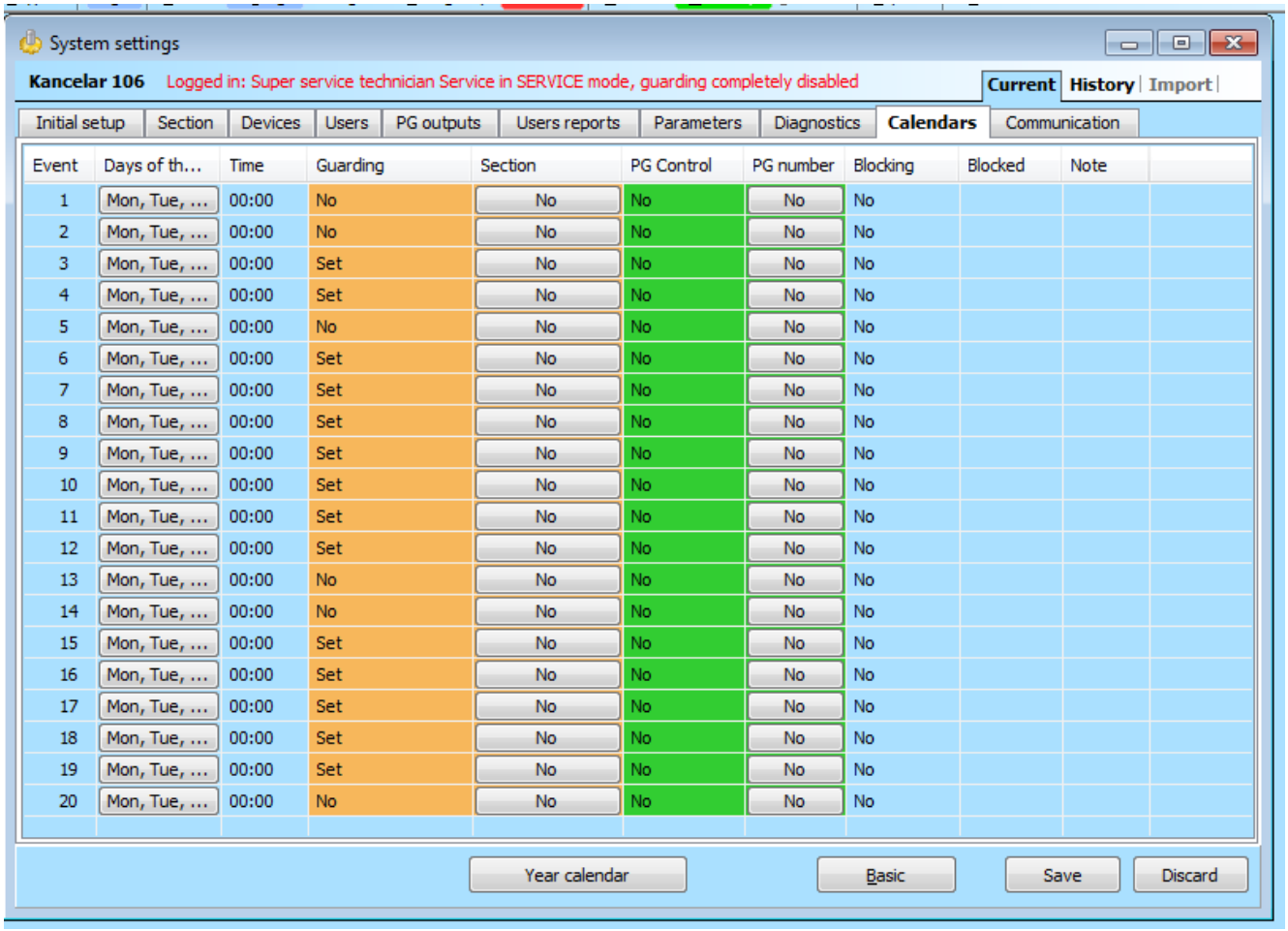
		Program F-Link monitoruje, czy kod i karta zostały przypisane do użytkownika w Zakładce Użytkownicy (w przeciwnym razie F-Link nie pozwoli na zapisanie konfiguracji). Dostęp zdalny telefoniczny jest aktywny jedynie dla uprawnionych numerów.
Blokowanie systemu przez alarm	Parametr umożliwia blokowanie systemu po pierwszej aktywacji alarmu (włamanie lub sabotaż), aby uniknąć aktywacji kolejnych alarmów. Odblokowanie można wykonać specjalnym kodem do Odblokowania lub przez uprawniony dostęp ze SMA (dla Wielkiej Brytanii). Odblokowanie po aktywacji alarmu sabotażu może przeprowadzić także użytkownik z uprawnieniami serwisowymi (dla obszaru krajów Beneluksu).	
	Nie	Brak blokowania
	Przez alarm sabotażu	System zostaje zablokowany w chwili aktywacji alarmu sabotażu (przez otwarcie urządzenia, tłumienie RF lub 10 nieprawidłowo wprowadzonych kodów itp.).
	Dowolny alarm	System zostaje zablokowany po aktywacji dowolnego alarmu (włamanie, alarm pożarowy, zalania, alarm 24 h lub alarm panika).
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 utratę urządzenia MAGISTRALI lub zwarcie w MAGISTRALI w postaci alarmu sabotażu. Jeżeli moduł radiowy ma aktywne wykrywanie tłumienia RF i je wykryje, również aktywuje alarm sabotażu. Po alarmie sabotażu występuje błąd, a kiedy ten błąd zniknie, anuluje 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.
Auto-pominięcie urządzenia	Opcja służy do wyboru metody auto-pominięcia.	
	3. aktywacja	Pominięcie urządzenia nastąpi po trzykrotnej aktywacji w jednym okresie uzbrojenia niezależnie od długości alarmu. Wszelkie inne próby aktywacji urządzenia będą ignorowane do chwili rozbrojenia strefy.
	3. alarm	Urządzenie umożliwia trzykrotną aktywację w 1 okresie alarmowym. Obejście danego urządzenia nastąpi po 3 okresach alarmowych, co oznacza po możliwości najwyżej 9 aktywacji tego urządzenia.
Po uruchomieniu F-Link automatycznie otworzyć podłączoną centralę alarmową.	Jeżeli centrala alarmowa jest podłączona do komputera przewodem USB, połączenie zostaje nawiązane automatycznie z chwilą uruchomienia oprogramowania F-Link.	
Automatyczne wejście w tryb serwisowy	Automatycznie wchodzi w tryb serwisowy, gdy centrala alarmowa jest podłączona do komputera przewodem USB. Jeżeli niektóre strefy są uzbrojone, otrzymają Państwo prośbę o rozbrojenie z uwierzytelnieniem. W przypadku korzystania z kodów domyślnych uwierzytelnienie nie jest konieczne.	

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

Ustawienia zegara	W każdej strefie osobno odmierza się opóźnienie na wejście i wyjście A, B i C. Jeżeli dla czujek w obrębie strefy określono różną długość opóźnienia na wyjście, system odmierzy najdłuższą z nich. W przypadku różnych długości czasu opóźnienia na wejście mierzy się czas dotyczący aktywnej czujki. W przypadku aktywności większej liczby czujek odmierza się czas najkrótszego zdefiniowanego opóźnienia na wejście. Czujki z opóźnieniem C mogą przedłużać czas trwania opóźnienia na wyjście (patrz opcja „Czujka z reakcją Opóźniona C przedłuża czas na wyjście" w zakładce Parametry).
Długość alarmu	Długość alarmu — dotyczy wszystkich stref. Zakres 5 sek.–20 min.
Opóźnienie na wejście A	Zegar A. Zakres 5 sek.–2 min.
Opóźnienie na wyjście A	Zegar A. Zakres 5 sek.–2 min.
Opóźnienie na wejście B	Zegar B. Zakres 5 sek.–2 min.
Opóźnienie na wyjście B	Zegar B. Zakres 5 sek.–2 min.
Opóźnienie na wejście C	Zegar C. Zakres 5 sek.–6 min.
Opóźnienie na wyjście C	Zegar C. 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 A (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.).
Oczekuje na wielokrotną aktywację czujki	Czas oczekiwania na wielokrotną aktywację tej samej czujki. Zadany czas musi być dłuższy niż minimalne przywrócenie czujki przed powtórzeniem. Dotyczy wszystkich czujek z reakcją Powtórzona natychmiastowa / Powtórzona opóźniona A (6–120 sek.).
Czas ignorowania aktywnej czujki	Minimalny czas, przez który czujka nie podlega ocenie, zanim może powtórzyć aktywację. Dotyczy wszystkich czujek z reakcją Powtórzona natychmiastowa / Powtórzona opóźniona A (5–60 sek.).
Raportuj przy rozbrojeniu po	Czas, po którego upływie strefa rozbrojona zgłasza rozbrojenie, jeżeli nie nastąpiła w niej aktywacja żadnej czujki (raportowanie jest aktywne w zakładce Strefa — Zgłoś nieuzbrojoną strefę (1–48 godz.).
Automatyczne uzbrajanie	Czas, po którego upływie następuje automatyczne uzbrojenie strefy, gdzie zgłoszono zdarzenie „Rozbrój strefę" (0–120 min.).
Maksymalne przedłużenie czasu na wyjście	Maksymalny czas, o jaki aktywna czujka z opóźnieniem przedłuża opóźnienie na wyjście w strefie. Działa jedynie łącznie z opcją „Czujka z reakcją Opóźniona C przedłuża opóźnienie na wyjście". W przypadku dłuższej aktywności czujki następuje uzbrojenie strefy i pominięcie czujki (1–60 min.).
Czujki przedłużają opóźnienie na wyjście C	„Funkcja bramy garażu" — aktywna czujka z reakcją Opóźniona C (otwarta brama) przedłuża opóźnienie na wyjście w danej strefie. Takie przedłużenie mogą spowodować jedynie czujki z reakcją stanu (zwykle czujki otwarcia). Maksymalny czas ewentualnego przedłużenia ustawia się za pomocą poprzedniej opcji.
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. Użytkownik ma 15 sekund więcej na rozbrojenie systemu bez aktywacji alarmu zgłaszanego do SMA.

10.10 Zakładka Kalendarze

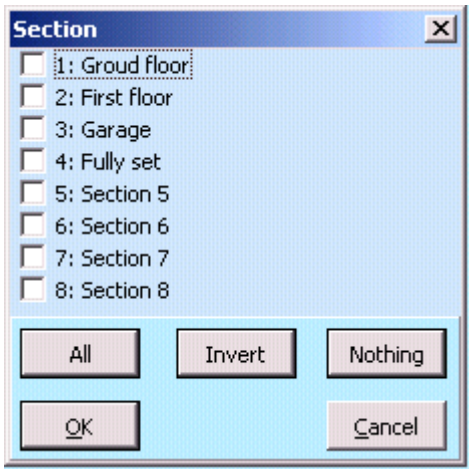
Tutaj można ustawić harmonogram czasowy czynności, które system będzie realizował automatycznie i regularnie. Aby wprowadzić zmiany w tej zakładce, nie trzeba znajdować się w trybie serwisowym.



Event	Days of th...	Time	Guarding	Section	PG Control	PG number	Blocking	Blocked	Note
1	Mon, Tue, ...	00:00	No	No	No	No	No		
2	Mon, Tue, ...	00:00	No	No	No	No	No		
3	Mon, Tue, ...	00:00	Set	No	No	No	No		
4	Mon, Tue, ...	00:00	Set	No	No	No	No		
5	Mon, Tue, ...	00:00	No	No	No	No	No		
6	Mon, Tue, ...	00:00	Set	No	No	No	No		
7	Mon, Tue, ...	00:00	Set	No	No	No	No		
8	Mon, Tue, ...	00:00	Set	No	No	No	No		
9	Mon, Tue, ...	00:00	Set	No	No	No	No		
10	Mon, Tue, ...	00:00	Set	No	No	No	No		
11	Mon, Tue, ...	00:00	Set	No	No	No	No		
12	Mon, Tue, ...	00:00	Set	No	No	No	No		
13	Mon, Tue, ...	00:00	No	No	No	No	No		
14	Mon, Tue, ...	00:00	No	No	No	No	No		
15	Mon, Tue, ...	00:00	Set	No	No	No	No		
16	Mon, Tue, ...	00:00	Set	No	No	No	No		
17	Mon, Tue, ...	00:00	Set	No	No	No	No		
18	Mon, Tue, ...	00:00	Set	No	No	No	No		
19	Mon, Tue, ...	00:00	Set	No	No	No	No		
20	Mon, Tue, ...	00:00	No	No	No	No	No		

Strzeżenie — pozwala ustawić, którą czynność należy realizować dla strefy lub wyjścia PG (Rozbrój, Uzbrój, Uzbrój częściowo, Sterowanie PG, wymóg Serwisu). Możliwe warianty obejmują „Natychmiast" (bez opóźnienia na wyjście) i „Zawsze" (nie przestrzega wybranego wcześniej sposobu uzbrajania). Czynność Wymóg serwisu aktywuje to samo zdarzenie w systemie, co opcja Wymóg serwisu w zakładce Parametry.

Strefa/PG — określa, w której strefie realizuje się czynność zadanego typu lub którymi wyjściami PG się steruje.



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

Dni miesiąca — określa, w które dni miesiąca należy wykonywać daną czynność.

Miesiące roku — określa, w które miesiące roku należy wykonywać daną czynność.

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

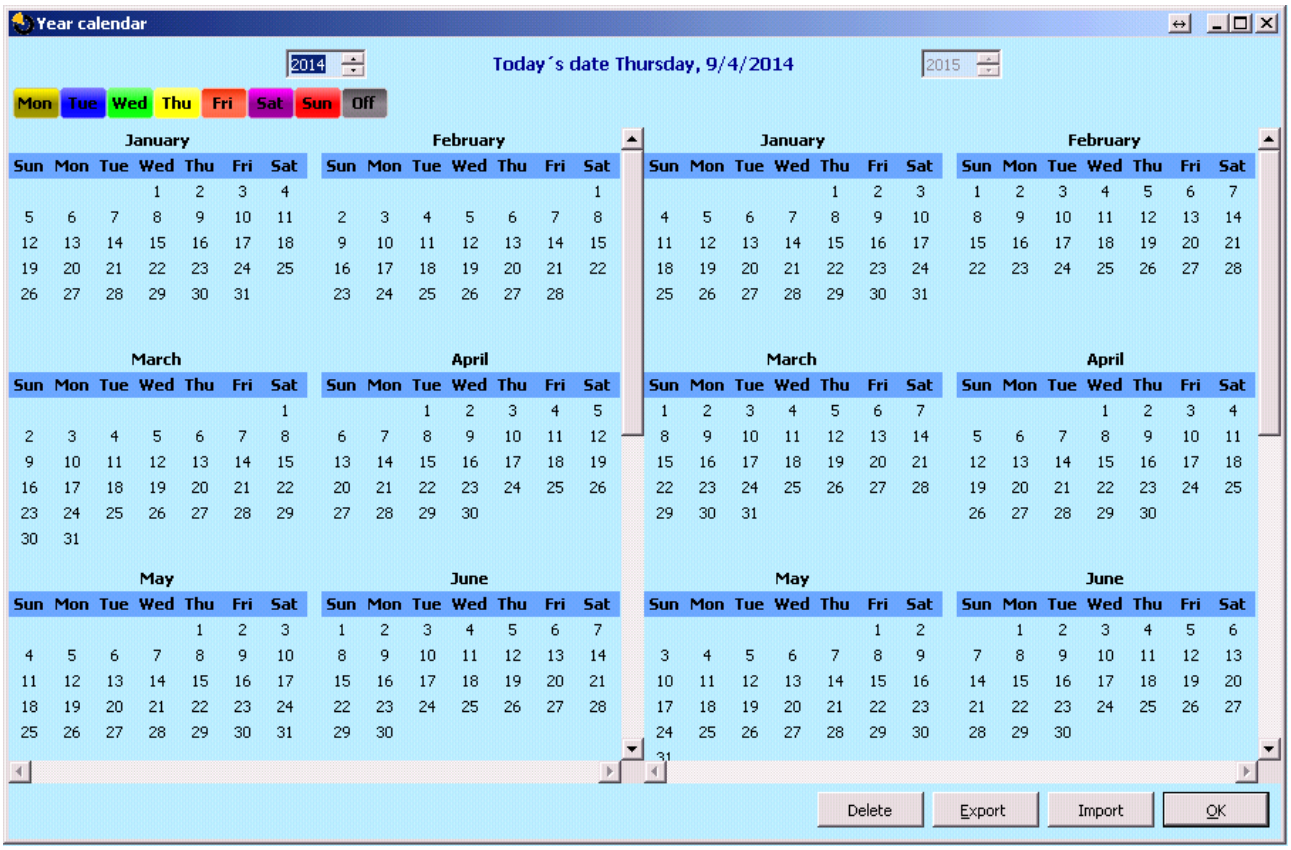
Czas — system pozwala skonfigurować najwyżej 4 razy na dobę lub odstęp czasowy regularnych powtórzeń żądanej czynności. Powtarzanie można zdefiniować jako czas OD–DO.

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

Dezaktywuj — możliwość zablokowania konkretnego działania. Dezaktywację sygnalizuje czerwona kropka. Administrator (przy użyciu J-Link) i Serwisant (przy użyciu F-Link) są uprawnieni do dezaktywacji zaplanowanej czynności.

Notatka — pozwala dodać indywidualny opis planowanych czynności.

Harmonogram roczny — pozwala zmienić atrybut dni (pon., wt.... niedz.) dla poszczególnych dni w obecnym i przyszłym roku. Ten atrybut można zmienić (wielokrotnym) kliknięciem myszą na wybranym dniu. Przykład zastosowania: Jeżeli święto państwowe (dzień wolny od pracy) przypada w środę, można zmienić atrybut dnia ze środy na niedzielę. W tym dniu nie będą realizowane czynności automatycznie planowane zgodnie z ustawieniami podstawowymi Harmonogramu i obowiązujące dla dni roboczych. Jednakże zostanie zachowany program dla niedziel. W ten sposób można dostosować sterowanie Strefami lub Sterowanie PG np. do świąt firmowych itp. Atrybut „Wył.” oznacza nieaktywne — w dni opisane w taki sposób nie realizuje się planowanej czynności.

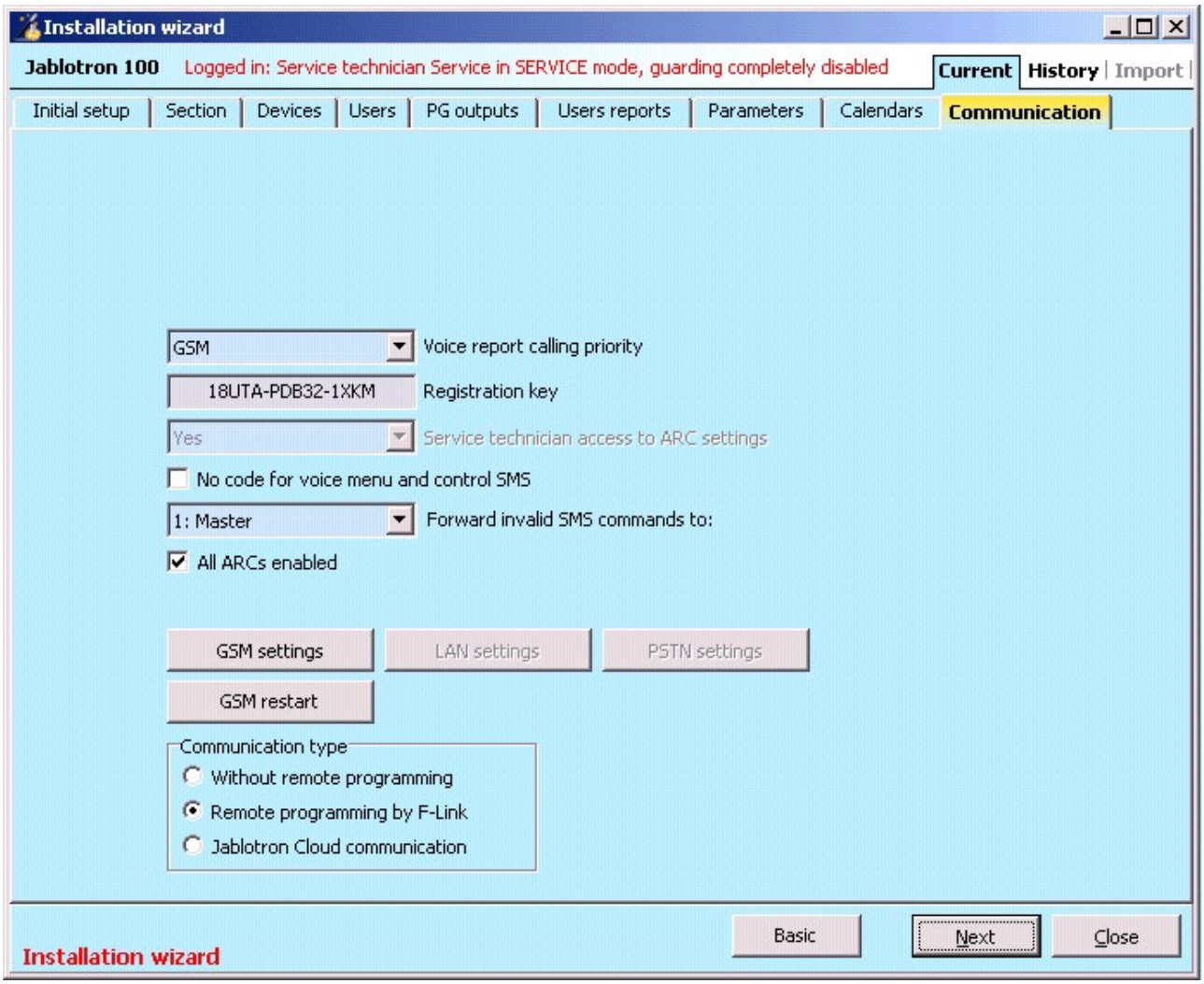


Uwagi:

- 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 wyboru Uzbrój natychmiast uzbrajanie realizuje się natychmiast bez opóźnienia na wyjście, a wszystkie pętle są bezzwłocznie aktywne (w tym czujki z opóźnieniem).

10.11 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.



Priorytet wybierania numeru do raportu głosowego — wybór kanału, który centrala alarmowa wykorzysta do głosowego zgłaszania zdarzeń (opcje GSM/PSTN).

Klucz rejestracji — unikalny numer rejestracji centrali alarmowej.

Dostęp serwisanta do ustawień SMA — pozwala technikowi SMA ograniczyć dostęp serwisanta do zakładki SMA.

Menu głosowe bez kodu — 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 — wybór użytkownika, któremu zostaną przekazane komunikaty SMS niezrozumiałe dla centrali alarmowej (informacje o fakturach od operatora itp.).

SMS o niepowodzeniu uzbrajania — centrala alarmowa wysyła SMS o niepowodzeniu uzbrajania. W przypadku niepowodzenia uzbrajania z uwierzytelnieniem (przez uprawnionego użytkownika) do tego użytkownika wysyłany jest komunikat SMS. W przypadku niepowodzenia uzbrajania bez uwierzytelnienia komunikat SMS wysyłany jest do Administratora w pozycji 1.

Wszystkie SMA aktywne — opcja dezaktywacji całej komunikacji ze SMA — niedostępna, jeżeli serwisant SMA ograniczył dostęp.

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

- **Brak** — zachowuje się jak autonomiczne urządzenie z własną kartą SIM. Urządzenie komunikuje się na zewnątrz (wysyła komunikaty SMS i głosowe) i odbiera wiadomości SMS z poleceniem. Ma także menu głosowe. Konfiguracja zdalna za pomocą oprogramowania F-Link nie jest możliwa.

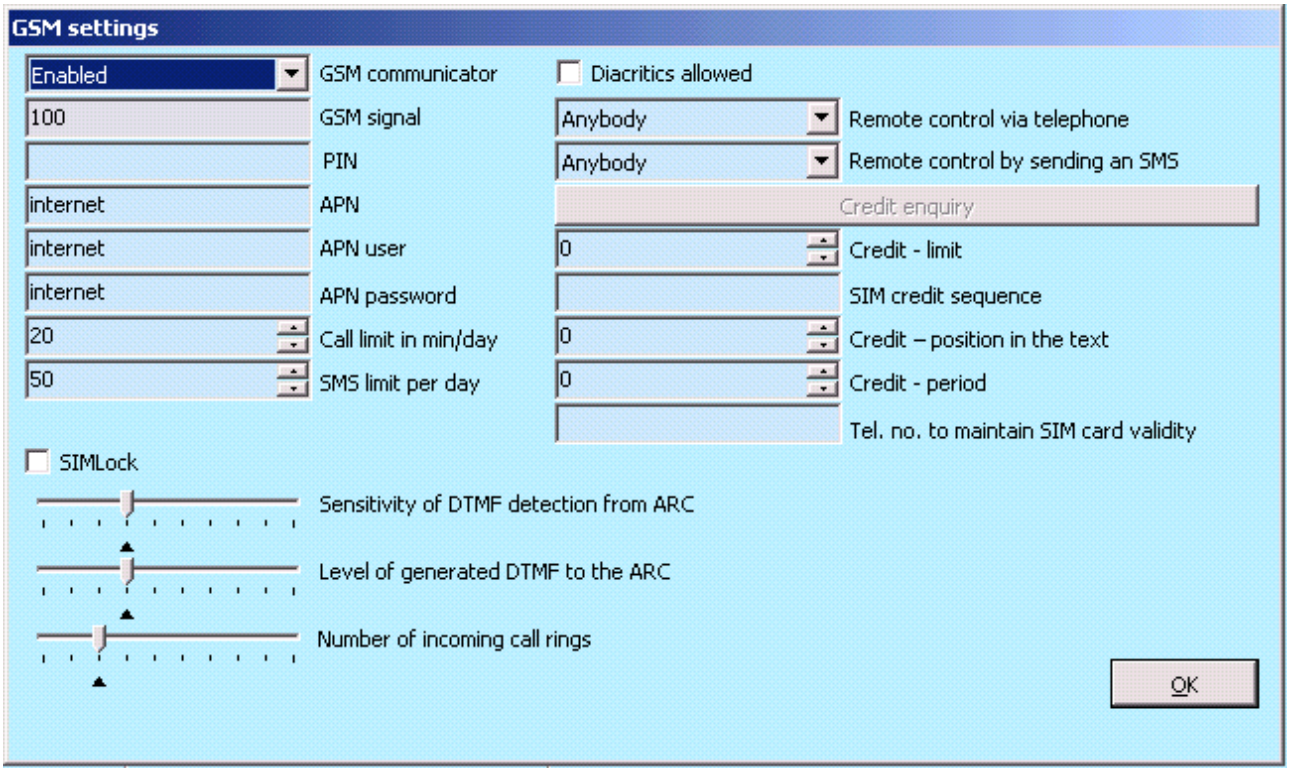
- **Ograniczone (GSM)** — komunikuje się jak poprzedni typ, a dodatkowo obsługuje zdalną konfigurację systemu. Konfiguracja zdalna jest możliwa z komputera z oprogramowaniem F-Link (J-Link) z dostępem do internetu. Aby ustanowić połączenie z centralą alarmową, F-Link łączy się z serwerem producenta, aby przekazać mu kod rejestracji i numer telefonu karty SIM umieszczonej w komunikatorze centrali alarmowej. W centrali alarmowej musi istnieć czynna komunikacja danych (LAN lub GSM/GPRS).
- **Stała (LAN)** — centrala alarmowa utrzymuje stałą komunikację danych z serwerem, umożliwia zdalne połączenie z oprogramowaniem F-Link.
- **Komunikacja JABLOTRON** — urządzenie komunikuje się z serwerem producenta (aplikacja MyJABLOTRON) i nieustannie wysyła do niego informacje o stanie urządzenia. Tym samym, jeżeli F-Link (J-Link) prześle żądanie połączenia zdalnego, serwer jest natychmiast gotowy do ustanowienia połączenia. Dodatkowo taka komunikacja pozwala użytkownikowi korzystać z usług serwera. Aplikacje pozwalające użytkownikowi obsługiwać system można instalować na urządzeniach mobilnych z systemem Android i iOS. W przypadku tej opcji należy używać karty SIM JABLOTRON Security.

Informacje na temat możliwości korzystania z poszczególnych rodzajów komunikacji we własnym kraju można pozyskać od dystrybutora.

Ustawienia — przycisk służy do rejestracji systemu do usługi JABLOTRON w CHMURZE. Po wypełnieniu formularza i przesłaniu danych do potwierdzenia utworzy żądanie rejestracji. Potwierdzenie wypełnionego formularza nastąpi w ciągu kilku chwil.

10.11.1 Ustawienia GSM

Przycisk służy do ustawiania parametrów i zachowania komunikatora GSM.



* Pozycja oznaczona w ten sposób zostaje uzbrojona automatycznie po aktywacji centrali alarmowej, jeżeli zainstalowano komunikator GSM i przed aktywacją włożono do niego sprawną kartę SIM (usługa serwera JABLOTRON).

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 dla komunikatora (ogranicza podłączenie modułu do 1 komórki sieci = niestabilna komunikacja). Informacje o jakości sygnału można uzyskać także przy pomocy polecenia SMS STATUS (patrz rozdział 9.6 SMS commands).

PIN karty SIM — zalecamy stosowanie karty SIM z wyłączonym kodem PIN.

APN sieci* — ustawienia komunikacji danych GPRS. Komunikacja danych zapewnia dostęp do usług serwera JABLOTRON, umożliwia dostęp zdalny serwisanta, komunikację ze SMA itp. Oprócz ustawień APN konieczna jest obsługa transmisji danych przez używaną kartę SIM.

Informacje na temat możliwości takiej komunikacji można uzyskać od dystrybutora JABLOTRON.

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

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

Limit połączeń min./doba — ogranicza zakres faktycznych połączeń do 5–250 minut na dobę.

Ogranicznik SMS — Ogranicznik ogranicza liczbę SMS-ów wysyłanych przez centralę alarmową w ciągu doby. Obejmuje on zdarzenia alarmowe i niealarmowe (zdarzenia alarmowe — alarm, sabotaż, awaria, raport itp.; niealarmowe – PG, serwis itp.). Zakres można ustawić na 5 do 250 SMS-ów. System wysyła najwyżej 250 SMS-ów na dobę. Tę maksymalną liczbę dzieli między *ogranicznik SMS-ów* i *ogranicznik SMS-ów alarmowych* (F-Link automatycznie sprawdza, czy ustawienie obu ograniczników nie przekracza 250).

Ogranicznik SMS-ów alarmowych — ogranicznik ogranicza liczbę SMS-ów o alarmie wysyłanych przez centralę alarmową w ciągu doby, jeżeli osiągnięto już limit wysłanych wiadomości SMS (*ogranicznik SMS*). Jest powiązany ze zdarzeniami alarmowymi (alarmy, sabotaże, błędy, raporty itp.). Zakres można ustawić na 0 do 245 SMS-ów. **Przykład:** *Ogranicznik wysłanych SMS-ów* ustawiono na 30, *Ogranicznik SMS-ów alarmowych* ustawiono na 20. System zachowa się następująco: Kiedy w danym dniu system wyśle 30 SMS-ów dowolnego typu (alarmowych i nie), w danym dniu nie wyśle żadnych więcej SMS-ów niealarmowych. Może jednak nadal wysyłać SMS-y o alarmie (do 20). Dzięki temu system ma rezerwę na wypadek alarmu, może więc powiadomić użytkownika za pomocą wiadomości SMS.

Dopuść znaki diakrytyczne — 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 wysłanie 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.

Zapytanie o kredyt — przez naciśnięcie tego przycisku można natychmiast pozyskać informację o saldzie kredytowym z odpowiedzi 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. **Przestroga: 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 cyfry i ignoruje inne znaki).

Okres sprawdzania kredytów — ustawienie częstotliwości sprawdzania salda kredytów przez system (można ustawić od 0 do 99 dni, gdzie 0 oznacza wyłączone).

Nr tel. do utrzymania ważności karty SIM — jeżeli karta SIM typu pre-paid wymaga utrzymywania rozmów, można ustawić numer telefonu, który system automatycznie wybierze (np. usługa dokładnego czasu) w przypadku, gdy przez okres ponad 90 dni nie było rozmowy wychodzącej z systemu (system zakończy połączenie 10 s po odebraniu go przez adresata).

SIMLock — funkcja łącząca numer telefonu karty SIM z ustawieniami SMA. Oznacza to, że w przypadku zastąpienia karty SIM inną, przy zalogowaniu karty SIM do sieci GMS wszystkie ustawienia **zakładki SMA zostaną usunięte.** Usunięcia nie można cofnąć, a serwisant SMA musi ponownie wprowadzić inne ustawienia (rejestracja do usługi sieciowej MyJABLOTRON).

Czułość wykrywania DTMF ze SMA — ustawienia czułości odbioru sygnałów generowanych przez SMA. Czułość ustawia się w 10 etapach; optymalną domyślną wartością jest 4.

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

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

Numer telefonu karty SIM — numer telefonu karty SIM używanej w komunikatorze.

Pozyskaj numer telefonu komunikatora — żądanie SMS zostaje wysłane po naciśnięciu przycisku. Po udanej odpowiedzi numer telefonu wyświetli się w polu „Numer telefonu karty SIM".

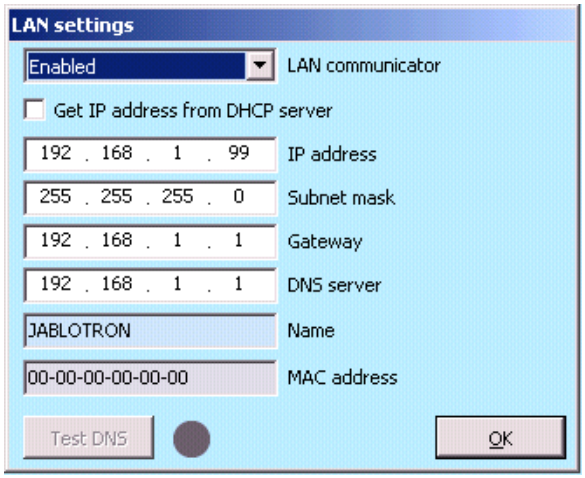
[1]**Security Data Connector™** — w centrali alarmowej używa się usługi Security Data Connector™. Wszystkie parametry GSM są zadane automatycznie i nie można ich zmodyfikować.

[1]**Zmiana dostawcy GSM** — ta opcja umożliwia automatyczne przełączanie między dostawcami GSM.

[1] — wszystkie pozycje oznaczone w ten sposób są dostępne w przypadku używania Security Data Connector™

10.11.2 Ustawienia LAN

Służy do ustawiania komunikatora LAN (jeśli centrala alarmowa go ma).



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 to 192.168.1.99.

Maska podsieci — ustawienie do ręcznego przypisywania maski podsieci IP, które jest dostępne jedynie, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne to 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 to 192.168.1.1.

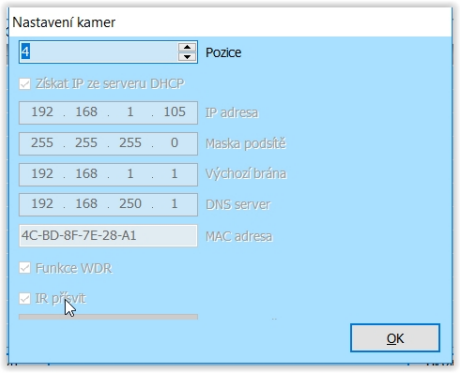
Serwer DNS — ustawienie do ręcznego przypisywania IP serwera, które jest dostępne jedynie w przypadku, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne to 192.168.1.1.

Nazwa — nazwa urządzenia, ułatwiająca identyfikację w sieci lokalnej.

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

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.

10.11.3 Kamery



Przycisk Kamery pozwala przeprowadzić test łączności (jeżeli żądane porty są dozwolone) oraz test prędkości połączenia. Po udanym ukończeniu testu wyświetla się wykres z propozycją liczby kamer, które mogą działać w poszczególnych rozdzielczościach w danej sieci. Jeżeli w sieci istnieje już działająca kamera, jej podstawowe parametry można ustawić w F-Link.

Pozycja — pozycja w systemie

Pozyskaj adres IP z serwera DHCP — automatyczne ustawienie parametrów sieci. Jeżeli sieć nie obsługuje tej funkcji, odpowiednie parametry należy wprowadzić ręcznie. Ręczne wprowadzanie jest możliwe wyłącznie 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 to 192.168.1.99.

Maska podsieci — ustawienie do ręcznego przypisywania maski podsieci IP, które jest dostępne jedynie, gdy automatyczne przypisywanie z serwera DHCP nie jest aktywne. Ustawienie domyślne to 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 to 192.168.1.1.

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

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

Funkcja WDR — dezaktywacja WDR (Wide Dynamic Range — kompensacja podświetlenia) np. dla obszarów o dużym kontraście miejsc jasnych i ciemnych.

Oświetlenie IR — dezaktywacja oświetlenia IR dla obszarów o stałym oświetleniu.

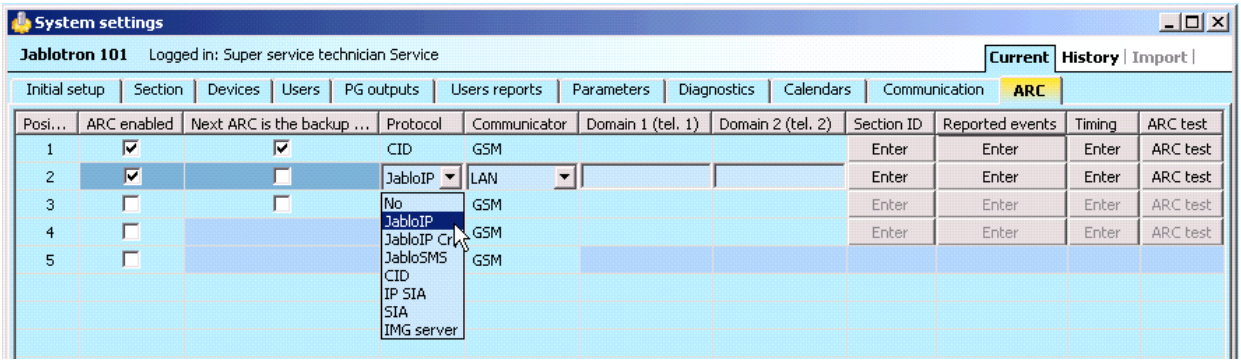
Tryb kamery — wybór trybu kamery, można wybrać tryb Dzień, Noc i Automatyczny.

10.11.4 Restart modułu GSM

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

10.12 Zakładka SMA

Ta zakładka służy do ustawiania komunikacji dla centrum odbioru alarmów (SMA). Jeżeli w zakładce Komunikacja zostanie ograniczony dostęp serwisanta, 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 aktualnej.

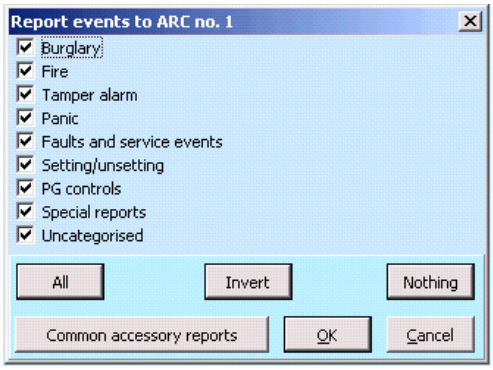
Protokół — ustawienie protokołu transmisji.

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

Komunikator — jeżeli wybrany protokół można transmitować do SMA na więcej sposobów, tutaj wybiera się rodzaj komunikatora. Opcje obejmują GSM, LAN, Linia telefoniczna i Automatycznie, ale widoczne są jedynie aktualnie dostępne opcje. Opcja Automatycznie wykorzystuje połączenie komunikatorów LAN/GSM, przede wszystkim LAN, a gdy ta możliwość jest niedostępna, przełącza się na awaryjny moduł GSM. W przypadku awarii transmisji z obu komunikatorów system zgłosi błąd — brak przesyłu danych do SMA.

Domena 1 (telefon 1) — ustawienia domeny głównej (przy pomocy adresu URL lub IP) lub głównego numeru telefonu zależnie od używanego protokołu. W przypadku używania komunikacji IP należy po adresie IP wpisać port komunikacji oddzielony średnikiem. Dane portu komunikacji i adres IP można pozyskać ze SMA, do której przekierowano komunikację. Bez wpisania portu komunikacji nie dojdzie do transmisji zdarzenia.

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



ID strefy — ustawienie identyfikacji budynku (wspólne dla całego budynku lub osobne dla stref). Ostrzeżenie: Domyślnym ustawieniem jest zero i wówczas komunikator nie wysyła żadnych raportów!

Zgłaszane zdarzenia — wybór typów zgłaszanych zdarzeń i możliwość ustawiania kodów raportów uzupełniających (wyjścia PG, raporty specjalne A do D).

Czas — ustawianie limitów czasu do transmisji i ustawianie 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.

10.12.1 JABLOTRON 100 + kody 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
1130	BA	Szafka na klucze	Raporty specjalne
1133	BA	Alarm 24 h	Włamanie
1134	BA	Alarm opóźniony	Włamanie
1138	BG	Alarm niepotwierdzony	Włamanie
1138	BG	Alarm niepotwierdzony	Włamanie
1144	TA	Sabotaż urządzenia peryferyjnego	Sabotaż
1151	FA	Wyciek gazu	Pożar
1154	WA	Alarm zalania	Włamanie
1158	KA	Przegrzanie (od FW20 w górę)	Nieskategoryzowany
1159	ZA	Zamarzanie (od FW20 w górę)	Nieskategoryzowany
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	Nieskategoryzowany
1300	ET	Błąd	Błędy i zdarzenia serwisowe
1300	ET	Błąd	Błędy i zdarzenia serwisowe
1301	AT	Utrata zasilania sieciowego	Błędy i zdarzenia serwisowe

1302	YT	Centrala alarmowa o niskim ACU	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	Zresetowano ustawienie SMA	Nieskategoryzowany
1344	XQ	Zakłócenia radiowe	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	Błędy i zdarzenia serwisowe
1389	TO	Test nieudany	Błędy i zdarzenia serwisowe
1401	OP	Rozbrojony	Uzbrajanie/Rozbrajanie
1402	OG	Częściowo rozbrojony	Uzbrajanie/Rozbrajanie
1406	BC	Alarm odwołany przez użytkownika	Włamanie
1406	BC	Alarm odwołany przez użytkownika	Włamanie
1406	BC	Alarm odwołany przez użytkownika	Włamanie
1406	BC	Alarm odwołany przez użytkownika	Włamanie
1406	BC	Alarm odwołany przez użytkownika	Włamanie
1407	OQ	Rozbrojony zdalnie	Uzbrajanie/Rozbrajanie
1412	LF	Dostęp zdalny	Nieskategoryzowany
1416	LS	Konfigurację zapisano	Nieskategoryzowany
1454	NA	Strefa bez ruchu	Błędy i zdarzenia serwisowe
1455	CI	Niepowodzenie uzbrajania	Nieskategoryzowany
1461	JA	Przekroczono liczbę prób złamania kodu	Sabotaż
1521	BL	Syrena wyciszona	Nieskategoryzowany
1570	EB	Pomiń urządzenie peryferyjne (wyłączone)	Nieskategoryzowany
1572	TB	Pominięcie sabotażu	Błędy i zdarzenia serwisowe
1573	BB	Pominięcie aktywacji	Błędy i zdarzenia serwisowe
1573	BB	Pominięcie aktywacji	Błędy i zdarzenia serwisowe
1574	UB	Pomiń strefę (wyłączone)	Nieskategoryzowany
1578	UO	Pominięcie błędu	Błędy i zdarzenia serwisowe
1601	RX	Test ręczny	Błędy i zdarzenia serwisowe
1601	RX	Test ręczny	Błędy i zdarzenia serwisowe
1601	RX	Test ręczny	Błędy i zdarzenia serwisowe
1601	RX	Test ręczny	Błędy i zdarzenia serwisowe
1602	RP	Test okresowy	Nieskategoryzowany
1602	RP	Test okresowy	Nieskategoryzowany
1602	RP	Test okresowy	Nieskategoryzowany
1602	RP	Test okresowy	Nieskategoryzowany
1602	RP	Test okresowy	Nieskategoryzowany
1602	RP	Test okresowy	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
1665	RC	PG5 WŁ.	Sterowniki PG
1666	RC	PG6 WŁ.	Sterowniki PG

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

1667	RC	PG7 Wł.	Sterowniki PG
1668	RC	PG8 Wł.	Sterowniki PG
1669	RC	PG9 Wł.	Sterowniki PG
1670	RC	PG10 Wł.	Sterowniki PG
1671	RC	PG11 Wł.	Sterowniki PG
1672	RC	PG12 Wł.	Sterowniki PG
1673	RC	PG13 Wł.	Sterowniki PG
1674	RC	PG14 Wł.	Sterowniki PG
1675	RC	PG15 Wł.	Sterowniki PG
1676	RC	PG16 Wł.	Sterowniki PG
1677	RC	PG17 Wł.	Sterowniki PG
1678	RC	PG18 Wł.	Sterowniki PG
1679	RC	PG19 Wł.	Sterowniki PG
1680	RC	PG20 Wł.	Sterowniki PG
1681	RC	PG21 Wł.	Sterowniki PG
1682	RC	PG22 Wł.	Sterowniki PG
1683	RC	PG23 Wł.	Sterowniki PG
1684	RC	PG24 Wł.	Sterowniki PG
1685	RC	PG25 Wł.	Sterowniki PG
1686	RC	PG26 Wł.	Sterowniki PG
1687	RC	PG27 Wł.	Sterowniki PG
1688	RC	PG28 Wł.	Sterowniki PG
1689	RC	PG29 Wł.	Sterowniki PG
1690	RC	PG30 Wł.	Sterowniki PG
1691	RC	PG31 Wł.	Sterowniki PG
1692	RC	PG32 Wł.	Sterowniki PG
3101	QR	Problem zdrowotny (dezaktywacja)	Włamanie
3110	FR	Alarm pożarowy (dezaktywacja)	Pożar
3118	FH	Niepotwierdzony alarm pożarowy (dezaktywacja)	Pożar
3120	PR	Panika (dezaktywacja)	Panika
3130	BR	Alarm natychmiastowy (dezaktywacja)	Włamanie
3130	BR	Szafka na klucze (dezaktywacja)	Raporty specjalne
3133	BR	Alarm 24 h (dezaktywacja)	Włamanie
3134	BR	Alarm opóźniony (dezaktywacja)	Włamanie
3138	BH	Alarm niepotwierdzony (dezaktywacja)	Włamanie
3138	BH	Alarm niepotwierdzony (dezaktywacja)	Włamanie
3144	TR	Sabotaż (dezaktywacja)	Sabotaż
3151	FR	Wyciek gazu (dezaktywacja)	Pożar
3154	WR	Alarm zalania (dezaktywacja)	Włamanie
3158	KH	Przegrzanie (dezaktywacja) (od FW20 w górę)	Nieskategoryzowany
3159	ZH	Zamarzanie (dezaktywacja) (od FW20 w górę)	Nieskategoryzowany
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	Nieskategoryzowany
3300	ER	Błąd (dezaktywacja)	Błędy i zdarzenia serwisowe
3301	AR	Przywrócenie zasilania sieciowego	Błędy i zdarzenia serwisowe

3301	AR	Przywrócenie zasilania sieciowego	Błędy i zdarzenia serwisowe
3302	YR	Bateria centrali alarmowej OK	Błędy i zdarzenia serwisowe
3306	LX	Opuszczenie trybu serwisowego	Błędy i zdarzenia serwisowe
3313	YZ	Odblokowane po alarmie	Błędy i zdarzenia serwisowe
3344	XH	Zakłócenia radiowe (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 peryferyjnego OK	Błędy i zdarzenia serwisowe
3389	TI	Test OK	Błędy i zdarzenia serwisowe
3401	CL	Uzbrojony	Uzbrajanie/Rozbrajanie
3402	CG	Częściowo uzbrojony	Uzbrajanie/Rozbrajanie
3407	CQ	Uzbrojony zdalnie	Uzbrajanie/Rozbrajanie
3412	LE	Dostęp zdalny zamknięty	Nieskategoryzowany
3570	EU	Zdalnie uzbrojony częściowo	Uzbrajanie/Rozbrajanie
3572	TU	Koniec pominięcia urządzenia peryferyjnego (dezaktywacja)	Nieskategoryzowany
3573	BU	Koniec pominięcia sabotażu	Błędy i zdarzenia serwisowe
3573	BU	Koniec pominięcia aktywacji	Błędy i zdarzenia serwisowe
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
3665	RO	PG5 WYŁ.	Sterowniki PG
3666	RO	PG6 WYŁ.	Sterowniki PG
3667	RO	PG7 WYŁ.	Sterowniki PG
3668	RO	PG8 WYŁ.	Sterowniki PG
3669	RO	PG9 WYŁ.	Sterowniki PG
3670	RO	PG10 WYŁ.	Sterowniki PG
3671	RO	PG11 WYŁ.	Sterowniki PG
3672	RO	PG12 WYŁ.	Sterowniki PG
3673	RO	PG13 WYŁ.	Sterowniki PG
3674	RO	PG14 WYŁ.	Sterowniki PG
3675	RO	PG15 WYŁ.	Sterowniki PG
3676	RO	PG16 WYŁ.	Sterowniki PG
3677	RO	PG17 WYŁ.	Sterowniki PG
3678	RO	PG18 WYŁ.	Sterowniki PG
3679	RO	PG19 WYŁ.	Sterowniki PG
3680	RO	PG20 WYŁ.	Sterowniki PG
3681	RO	PG21 WYŁ.	Sterowniki PG
3682	RO	PG22 WYŁ.	Sterowniki PG
3683	RO	PG23 WYŁ.	Sterowniki PG
3684	RO	PG24 WYŁ.	Sterowniki PG
3685	RO	PG25 WYŁ.	Sterowniki PG
3686	RO	PG26 WYŁ.	Sterowniki PG
3687	RO	PG27 WYŁ.	Sterowniki PG
3688	RO	PG28 WYŁ.	Sterowniki PG

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

3689	RO	PG29 WYŁ.	Sterowniki PG
3690	RO	PG30 WYŁ.	Sterowniki PG
3691	RO	PG31 WYŁ.	Sterowniki PG
3692	RO	PG32 WYŁ.	Sterowniki PG
6301	AT	Utrata zasilania sieciowego przez ponad 30 min. (od FW 10 w górę)	Sterowniki PG

	Źródła dla JA 100
001–249	Urządzenia peryferyjne
251–850	Kody użytkownika
250	Kod serwisowy
901	Centrala alarmowa
921	SMA1
922	SMA2
923	SMA3
924	SMA4
925	ARC5
911	Komunikator GSM
912	Komunikator LAN
913	Komunikator PSTN
914	Komunikator GSM zewnętrzny

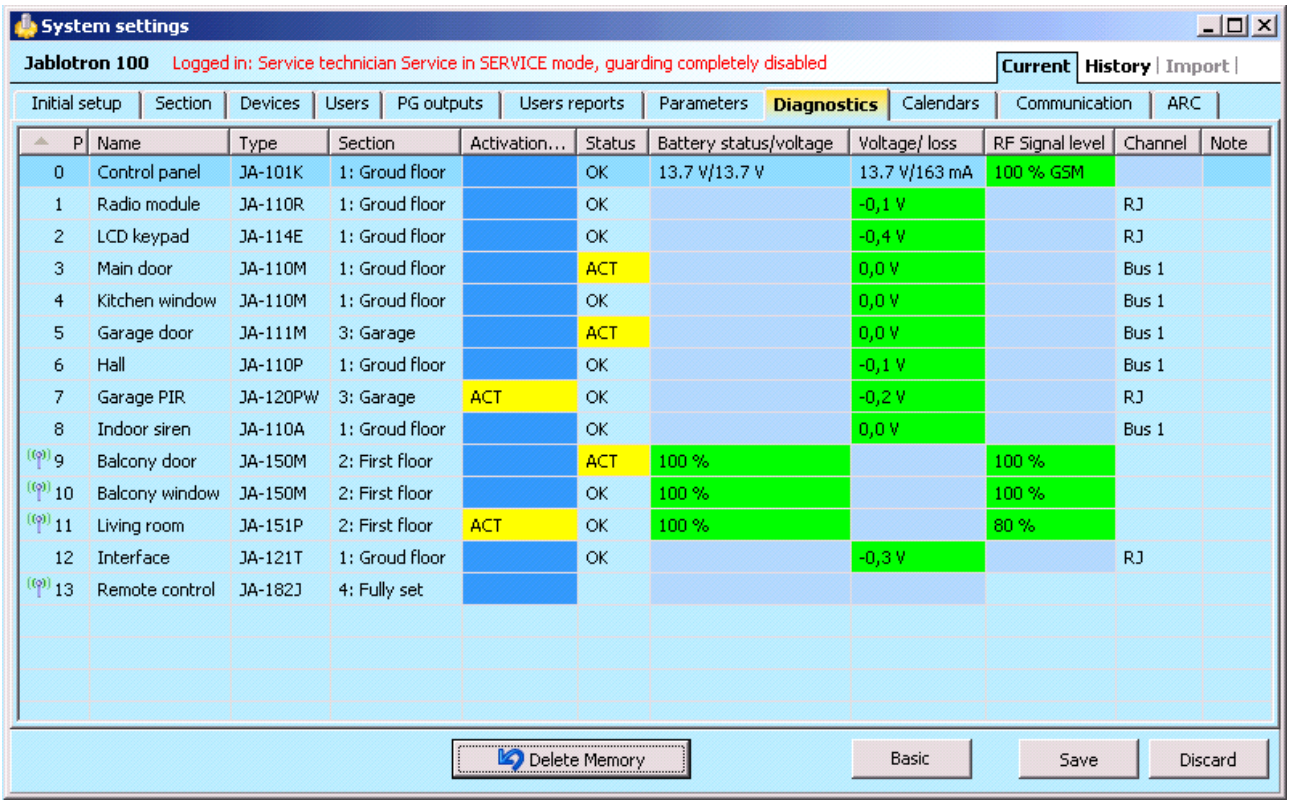
	PG	
	Zakres	**Skład CID**
1. grupa	1–32 PG	Strefa 1 + 1661–1692 / 3661–3692
2. grupa	33–64 PG	Strefa 2 + 1661–1692 / 3661–3692
3. grupa	65–96 PG	Strefa 3 + 1661–1692 / 3661–3692
4. grupa	97–128 PG	Strefa 2 + 1661–1692 / 3661–3692
Przykład: ID obiektu 1234, stałe 18**,** nr **PG WŁ. 33**, 02 to strefa, 901 to centrala alarmowa będąca źródłem zdarzenia = **1234 18 1 661 02 901**		

10.12.2 Ustawianie transmisji zdjęć do magazynowania zewnętrznego

Jeżeli w regionie/kraju aktywowano usługę MyJABLOTRON i użytkownik sprzętu zamierza z niej korzystać, żądane ustawienia zostaną wprowadzone całkowicie automatycznie w chwili rejestracji centrali alarmowej do usługi sieciowej MyJABLOTRON.

10.13 Zakładka Diagnostyka

Służy do sprawdzania i weryfikacji stanu urządzeń i ich właściwości.



P	Name	Type	Section	Activation...	Status	Battery status/voltage	Voltage/ loss	RF Signal level	Channel	Note
0	Control panel	JA-101K	1: Groud floor		OK	13.7 V/13.7 V	13.7 V/163 mA	100 % GSM		
1	Radio module	JA-110R	1: Groud floor		OK		-0,1 V		RJ	
2	LCD keypad	JA-114E	1: Groud floor		OK		-0,4 V		RJ	
3	Main door	JA-110M	1: Groud floor		ACT		0,0 V		Bus 1	
4	Kitchen window	JA-110M	1: Groud floor		OK		0,0 V		Bus 1	
5	Garage door	JA-111M	3: Garage		ACT		0,0 V		Bus 1	
6	Hall	JA-110P	1: Groud floor		OK		-0,1 V		Bus 1	
7	Garage PIR	JA-120PW	3: Garage	ACT	OK		-0,2 V		RJ	
8	Indoor siren	JA-110A	1: Groud floor		OK		0,0 V		Bus 1	
9	Balcony door	JA-150M	2: First floor		ACT	100 %		100 %		
10	Balcony window	JA-150M	2: First floor		OK	100 %		100 %		
11	Living room	JA-151P	2: First floor	ACT	OK	100 %		80 %		
12	Interface	JA-121T	1: Groud floor		OK		-0,3 V		RJ	
13	Remote control	JA-182J	4: Fully set							

* Pozycje oznaczone w ten sposób wyświetlają się przy włączonych **Ustawieniach zaawansowanych**.

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.

Stan — wskazuje aktualny stan 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 niepowodzenie ulepszania (powtórz ulepszanie), INIT = odczyt konfiguracji urządzenia, Disabled = urządzenie jest nieaktywne. Najechanie kursorem myszy na STATUS danego urządzenia pozwala wyświetlić szczegółowe informacje.

Bateria* — jeżeli urządzenie zawiera baterię, wyświetli się jej stan. Dla centrali alarmowej (pozycja 0) wyświetla się napięcie baterii awaryjnej. Jeżeli nie ma danych urządzenia bezprzewodowego, urządzenie nie nawiązało jeszcze komunikacji — aktywacja transmisji (np. za pomocą czujnika sabotażu lub przycisku Załaduj w programie F-Link) lub należy poczekać na automatyczne rozpoczęcie transmisji. Jeżeli klawiatury bezprzewodowe otrzymują zasilanie z zewnętrznego źródła energii, pojawi się komunikat „Zasilanie ze źródła zewnętrznego". Dla urządzeń bezprzewodowych (z wyjątkiem urządzeń serii JA-18x) widoczny jest stan baterii. Kod kolorystyczny stanu baterii: 10% czerwony, 20% żółty, 30% i więcej zielony.

Napięcie* — w pozycji centrali alarmowej (0) wyświetla się napięcie zacisków centrali alarmowej i natężenie pobierane przez urządzenia MAGISTRALI z centrali alarmowej (indywidualnie dla każdego wyjścia MAGISTRALI). 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.

Poziom sygnału RF* — w pozycji centrali alarmowej sygnalizuje jakość sygnału sieci GSM. Aby zapewnić niezawodną komunikację, wartość powinna wynosić co najmniej 50%. Dla urządzeń bezprzewodowych sygnalizuje jakość sygnału RF, która 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. Zakłócenia modułów radiowych i modułu GSM opisano także w rozdziale 6.1 Instalacja modułu radiowego JA-11xR.
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.

Dla urządzeń dwukierunkowych (obsługujących tę funkcję) umieszczenie kursora myszy nad poziomem sygnału urządzenia powoduje wyświetlenie obu kanałów komunikacji między centralą alarmową a urządzeniem.

Kanał* — informuje o MAGISTRALI używanej przez urządzenie do komunikacji. Wyróżnia się trzy kierunki: MAGISTRALA 1, MAGISTRALA 2, 3 (tylko JA-107K) i złączka I-BUS przeznaczona dla modułu radiowego JA-11xR (JA-103K). W przypadku dwukierunkowych urządzeń bezprzewodowych (syreny, klawiatury itp.) kolumna „Kanał" wyświetla moduł radiowy, za którego pośrednictwem urządzenie komunikuje się w danej chwili.

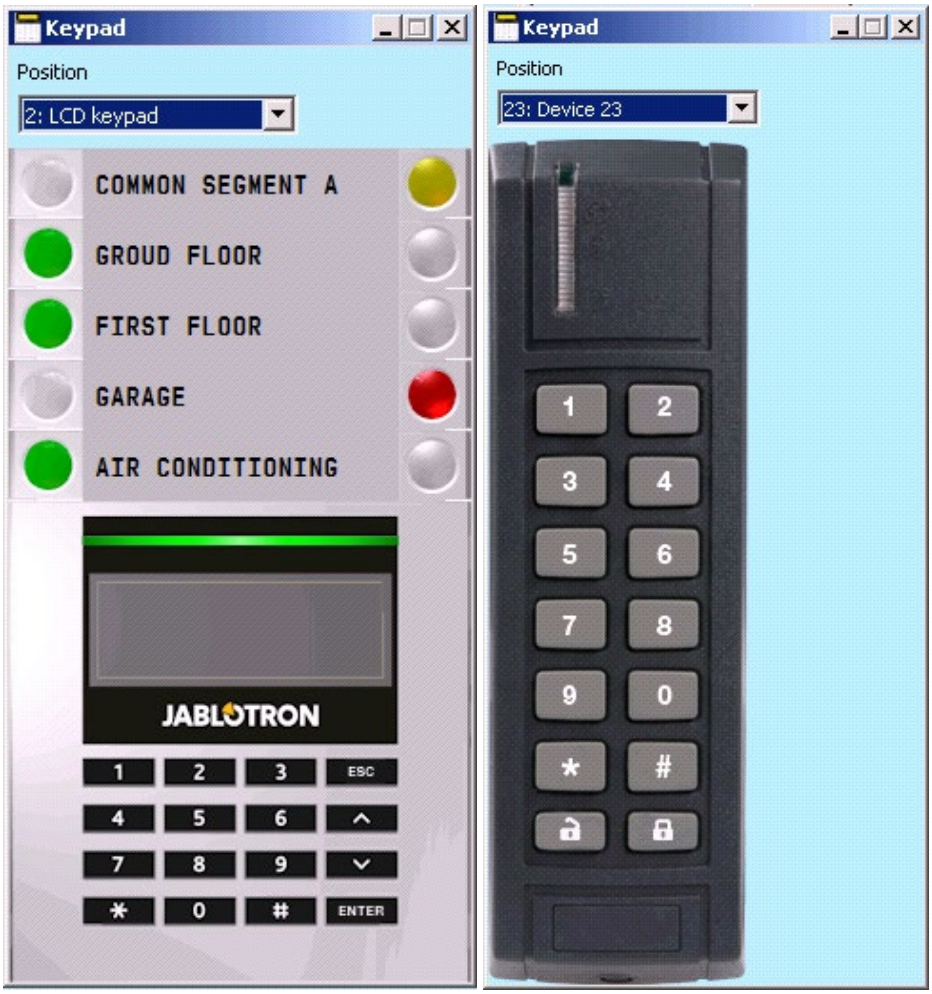
11 Inne opcje programu F-Link

Wersja F-Link zawsze znajduje się w górnym pasku za nazwą.

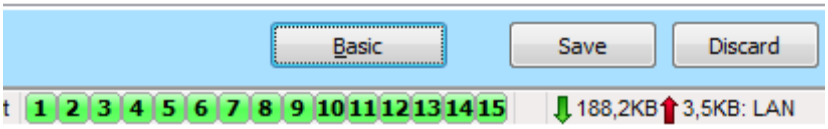
Pasek narzędziowy zapewnia natychmiastowy dostęp do wirtualnych klawiatur, zdarzeń w systemie, ustawień, sygnału RF modułów radiowych, mapy lokalizacji, zmian trybu, dostępu lokalnego i zdalnego do centrali alarmowej.

11.1 Klawiatura (wirtualna)

Klawiatura wirtualna w programie F-Link (teraz także w J-Link) dla wszystkich typów modułów sterujących umożliwia sterowanie (stref, wyjść PG) za pomocą segmentów (nie ponumerowanych klawiszy) przez osobę zalogowaną w F-Link. Oznacza to, że nie można wprowadzać kodów.



Systemem można sterować lokalnie i zdalnie (uzbrajać i rozbrajać), klikając ikony oznaczające stan systemu, które znajdują się na dolnym pasku narzędziowym oraz w zakładce Strefa, korzystając z przycisków.



11.2 Historia zdarzeń

Dostęp do historii zdarzeń można uzyskać w programie F-Link przez naciśnięcie przycisku Zdarzenia 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.

Events from memory

Refresh | Highlight | Filter settings

ID	Time	Source	Section	Event	Channel
50	9/4/2014 9:59:19 AM	Detector 11: Living room	2: First floor	Instant alarm	11: Living room
51	9/4/2014 9:59:20 AM	User 1: Master	2: First floor	Alarm cancelled	USB
52	9/4/2014 9:59:20 AM	Detector 9: Balcony door	2: First floor	Zone is back in arm mode	0: Control panel
53	9/4/2014 9:59:20 AM	User 1: Master	2: First floor	Unset	USB
54	9/4/2014 9:59:22 AM	User 1: Master	3: Garage	Set	USB
55	9/4/2014 9:59:24 AM	Detector 9: Balcony door	2: First floor	Set with active zone	0: Control panel
56	9/4/2014 9:59:24 AM	User 1: Master	2: First floor	Set	USB
57	9/4/2014 9:59:26 AM	User 1: Master	1: Groud floor	Set	USB
58	9/4/2014 9:59:26 AM	Detector 0: Control panel	4: Fully set	Set	0: Control panel
59	9/4/2014 9:59:32 AM	Detector 11: Living room	2: First floor	Instant activation	11: Living room
60	9/4/2014 9:59:32 AM	Detector 11: Living room	2: First floor	Instant Deactivation	11: Living room
61	9/4/2014 9:59:32 AM	Detector 11: Living room	2: First floor	Instant alarm	11: Living room
62	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Groud floor	Instant activation	4: Kitchen window
63	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Groud floor	Instant alarm	4: Kitchen window
64	9/4/2014 9:59:37 AM	Detector 8: Indoor siren	1: Groud floor	Mute	8: Indoor siren
65	9/4/2014 9:59:37 AM	Detector 8: Indoor siren	1: Groud floor	Mute	8: Indoor siren
66	9/4/2014 9:59:43 AM	Detector 11: Living room	2: First floor	Instant activation	11: Living room
67	9/4/2014 9:59:43 AM	Detector 11: Living room	2: First floor	Instant Deactivation	11: Living room
68	9/4/2014 9:59:43 AM	Detector 11: Living room	2: First floor	Instant alarm	11: Living room
69	9/4/2014 9:59:44 AM	Detector 4: Kitchen window	1: Groud floor	Instant Deactivation	4: Kitchen window
70	9/4/2014 9:59:47 AM	User 1: Master	2: First floor	Alarm cancelled	USB
71	9/4/2014 9:59:47 AM	Detector 9: Balcony door	2: First floor	Zone is back in arm mode	0: Control panel
72	9/4/2014 9:59:47 AM	User 1: Master	2: First floor	Unset	USB
73	9/4/2014 9:59:47 AM	Detector 0: Control panel	4: Fully set	Unset	0: Control panel
74	9/4/2014 9:59:49 AM	User 1: Master	1: Groud floor	Alarm cancelled	USB
75	9/4/2014 9:59:49 AM	User 1: Master	1: Groud floor	Unset	USB
76	9/4/2014 9:59:52 AM	User 1: Master	3: Garage	Unset	USB

Zdarzenia z pamięci centrali alarmowej (dostępne także po naciśnięciu F8) — ładuje się około 100 kB zdarzeń (z karty microSD). Jeżeli zakres wczytywania jest niewystarczający, można kilkakrotnie wybrać opcję Załaduj/Następne 100(500) kB, zakres od–do lub Wszystkie. Ostrzeżenie: Po zaznaczeniu Ładuj/Wszystkie w centrali alarmowej o dłuższym czasie działania ładowanie może zająć kilka minut. Historia nie rejestruje zdarzeń, które wystąpią podczas konfiguracji systemu (rejestruje jedynie otwarcie i zamknięcie trybu serwisowego). Załadowane zdarzenia można zapisać w pliku w menu Plik przy pomocy opcji Eksportuj pozycję (Shift + Ctrl + S) w następujących formatach (FDE, PDF, TXT, CSV, XML, HTM lub HTML). Przyrostek FDE pozwala programowi F-Link ponownie pobrać zdarzenia.

Uwaga: *Opcja ładowania zakresu od–do (data) jest dostępna jedynie przy połączeniu zdalnym.*

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

Sygnały online (dostępne także po naciśnięciu 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).

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

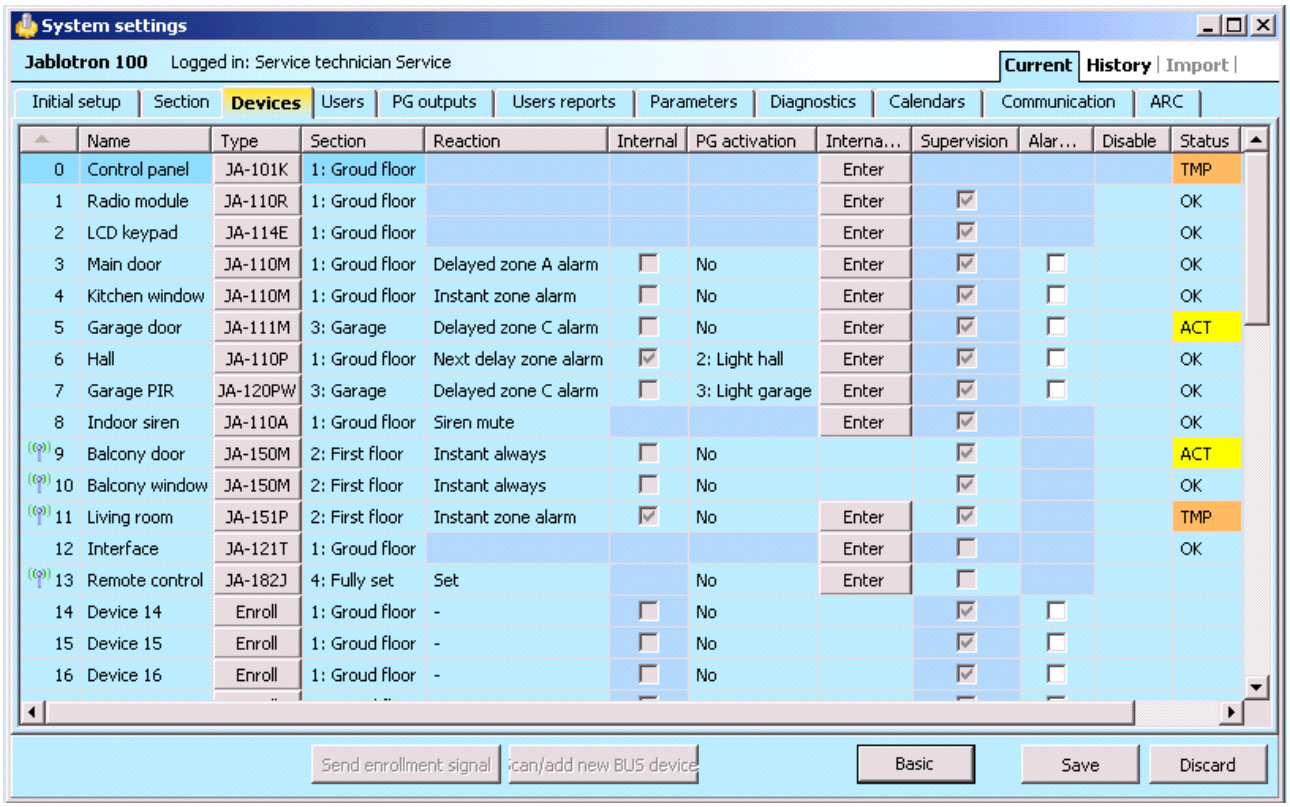
Załaduj — pozwala wczytać większą liczbę zdarzeń z dalszej historii w partiach po 100 kB, 500 kB (100 kB odpowiada około 1200 zdarzeniom) lub wszystkie zdarzenia.

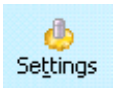
Wyróżnij — wyróżnienie kolorem pozwala odróżnić rodzaje zdarzeń (alarm czerwony, sterowanie zielony, błąd pomarańczowy, sabotaż niebieski, neutralny jasnoniebieski, automatyka lub transmisje szary itp.)

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**: **Konfiguracja początkowa, Strefy, Urządzenia, Użytkownicy, Raporty itp.**
3. Okno wyświetli **aktualną konfigurację centrali alarmowej** załadowaną po otwarciu programu F-Link. Przycisk **Załaduj** na górnym pasku narzędziowym może służyć do ładowania aktualnej treści centrali alarmowej w dowolnej chwili.
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 maks. 10 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. W przypadku prostszych zastosować można ustawić po prostu **podstawowe funkcje** systemu. Jeżeli konieczne jest ustawienie **wszystkich funkcji** systemu, należy użyć przycisku „Zaawansowane" w prawym dolnym rogu. Wielokrotne naciśnięcie tego przycisku pozwala ukryć opcje ustawień zaawansowanych (ich ustawienia pozostają w mocy pomimo ukrycia). Przycisk **Zaawansowane / Podstawowe** jest dostępny także w innych oknach.

7. **Zmiana ustawienia zostanie oznaczona tekstem w kolorze niebieskim** (również nazwa zakładki zmieni kolor na niebieski). Kolor niebieski zniknie natychmiast po zapisaniu zmian.
8. Można **Zapisać ustawienia** przyciskiem **Zapisz** (na dole z prawej strony). Podczas pierwszego zapisywania ustawień w centrali alarmowej program F-Link poprosi o **wprowadzenie nazwy pliku**. W komputerze
zostanie utworzony plik z rozszerzeniem *FDB, w którym stopniowo zapisywana będzie historia ustawień (po każdym zapisaniu ustawień w centrali alarmowej). Jeżeli nie chcą Państwo zapisywać zmian, należy zaznaczyć przycisk **Anuluj**, a w pytaniu potwierdzającym **Ignoruj**. Parametry można zmienić w większej liczbie zakładek, a potem można zapisać wszystkie zmiany.
9. Przycisk **Skanuj/dodaj nowe urządzenia MAGISTRALI** (dolny pasek narzędziowy w zakładce Urządzenia) otworzy okno dialogowe do łącznego przypisywania (bez możliwości wyboru pozycji) urządzeń podłączonych do MAGISTRALI, ale nie połączonych z systemem w inny sposób. Patrz rozdział 8.4.1 Przypisywanie i kasowanie urządzeń.
10. Przycisk **Wyślij sygnał przypisywania** (zakładka Urządzenia i wyjścia PG) zwolni wysyłanie kodu przypisywania centrali alarmowej do urządzeń bezprzewodowych, np. do modułów wyjść bezprzewodowych.
11. **Ustawianie wszystkich parametrów jest możliwe jedynie w trybie serwisowym** (system nie strzeże). Do aktywacji i dezaktywacji trybu serwisowego służy przycisk **Serwis** na górnym pasku narzędzi.
12. **Niektóre parametry można zmienić podczas eksploatacji.** Dlatego też można otworzyć zakładkę Serwis, nie wchodząc w tryb serwisowy. Można ustawić jedynie dostępne opcje.
13. **F-Link zawiera dymki pomocnicze** — po najechaniu kursorem myszy na dany element wyświetli się opis tekstowy. Dymki pomocnicze można wyłączyć w rozwijanym menu programu F-Link.

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

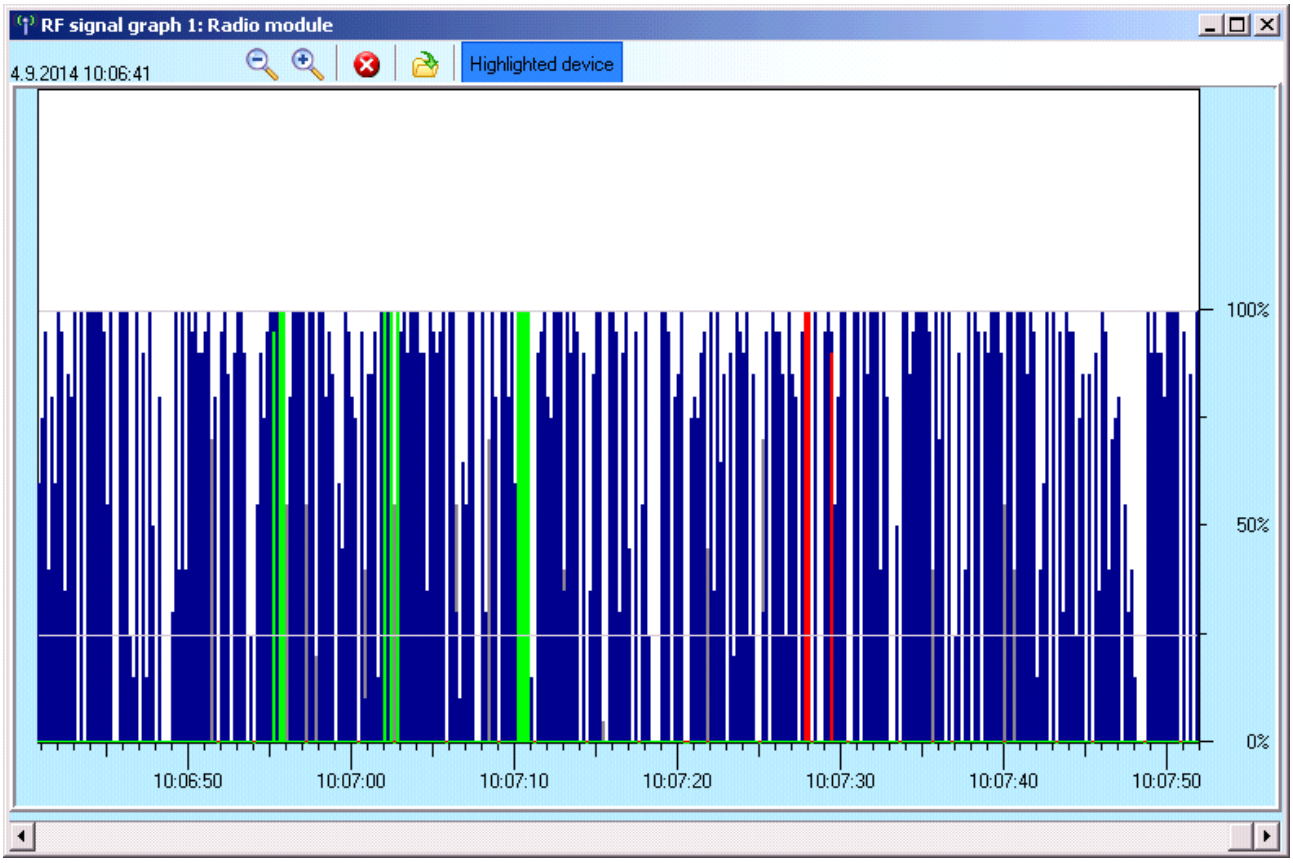
Możliwe problemy podczas użytkowania Ustawień systemu:

Problem	Możliwa przyczyna
Żadnego lub niektórych z wyświetlonych parametrów nie można zmienić	System nie jest w trybie serwisowym i wybrano funkcję, którą można zmienić wyłącznie w kodzie serwisowym. Po uruchomieniu F-Link nie wpisano Kodu serwisowego i nie posiadają Państwo uprawnień. Tego ustawienia nie można zmienić (uwierzytelnienie Serwisanta, pozycja centrali alarmowej, urządzenie nie obsługuje itp.). Serwisant SMA zablokował ustawienie SMA. Są Państwo offline. Aktywowali Państwo parametr w celu zapewnienia zgodności z normą EN 50131.
Nie można znaleźć żądanego parametru	Wyświetlają się jedynie podstawowe opcje, należy użyć przycisku Zaawansowane. Nie widać całego obszaru ustawień na ekranie — należy użyć przycisku przewijania lub powiększyć okno. Dokonali Państwo uwierzytelnienia kodem o innym poziomie dostępu.
Pozycje mają inny układ	Klikając tytuł kolumny, można wybrać, która kolumna będzie używana w charakterze kryterium układania pozycji. Wielokrotne kliknięcie tytułu pozwala wybrać kolejność rosnącą lub malejącą.
Brakuje niektórych zakładek	Jeżeli zakładka Wyjścia PG nie jest dostępna, należy sprawdzić, czy liczba wyjść PG ustawiona w zakładce Konfiguracja początkowa nie wynosi zero. Zakładka SMA nie jest dostępna, jeżeli nie mają Państwo wystarczających uprawnień do tego (mogą być zablokowane przez serwisanta SMA). Może być także niedostępna po rejestracji systemu w aplikacji MyJABLOTRON. Mają Państwo starszą wersję oprogramowania F-Link (J-Link).
Ustawień wewnętrznych nie można zmienić w zakładce Urządzenia	Sprawdzić, czy urządzenie jest prawidłowo podłączone, przypisane i sprawne. Tryb serwisowy nie jest włączony. Niektóre urządzenia nie mają ustawień wewnętrznych. Starsze wersje F-Link mogą nie obsługiwać nowszych typów urządzeń. W przypadku urządzenia bezprzewodowego należy sprawdzić, czy moduł radiowy jest przypisany i sprawny.
Urządzenia nie można przypisać w zakładce Urządzenia	Dla urządzeń bezprzewodowych — nie przypisali Państwo modułu radiowego JA-11xR. W przypadku urządzenia MAGISTRALI żółta dioda musi regularnie migać. Jeżeli nie miga, element nie jest prawidłowo podłączony lub nie nastąpiła jego stabilizacja po aktywacji zasilania (może to zająć do 180 sek.). Tryb serwisowy nie jest włączony. Starsze wersje F-Link mogą nie obsługiwać nowszych typów urządzeń.
Wyjście PG nie reaguje na aktywację urządzenia	Sprawdzić, czy system nie jest w trybie serwisowym. W zakładce Diagnostyka sprawdzić, czy urządzenie przesyła informację do centrali alarmowej. W zakładce Wyjścia PG sprawdzić, czy wyjście nie jest zablokowane stanem strefy, urządzeniem lub kalendarzem. Sprawdzić poprawność ustawień w kolumnie Funkcje. W JA-11xN moduły JA-15xN sprawdzają przełączniki DIP pod kątem odpowiedniego ustawienia binarnego adresu i funkcji modułu.

11.4 Sygnał RF

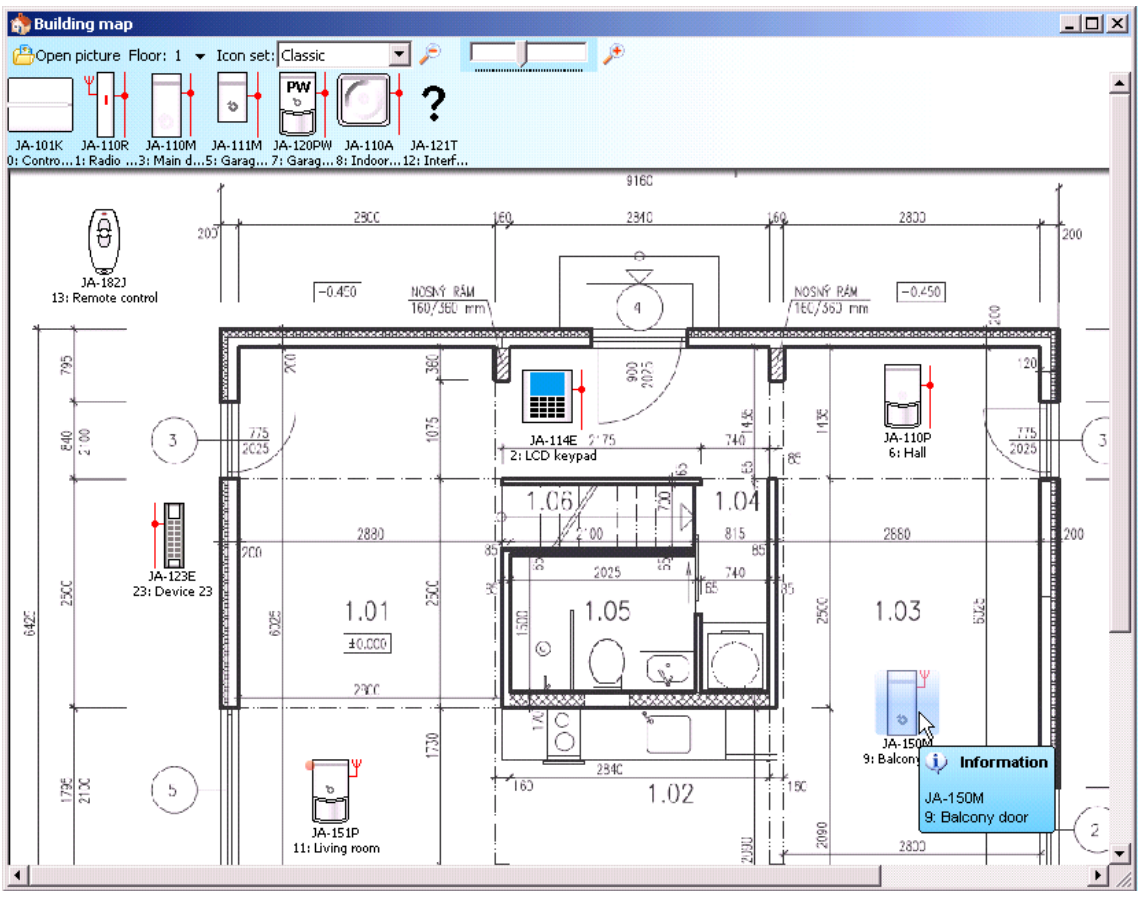
Okno zawierające przedstawienie graficzne intensywności zakłóceń pasma radiowego z możliwością wyboru z używanych modułów radiowych. Obecność nieznanych sygnałów w paśmie sygnalizuje kolor czerwony. Kolor zielony oznacza sygnały komunikacji systemu (urządzenia przypisane), a niebieski służy do wyświetlania wybranego urządzenia z listy pozycji **Urządzenie zaznaczone** (patrz ilustracja). Kolor szary oznacza tło (tłumienie). Za pomocą opcji **Dezaktywuj nieznane urządzenia** można przefiltrować nieznane urządzenia i wyświetlić jedynie urządzenia przypisane w systemie.

Rejestrację monitorowanych zakłóceń (gdy otwarte jest okno Sygnał RF) można wyeksportować z menu głównego do pliku z rozszerzeniem FDR, a przycisk  można wykorzystać do ich ponownego importu w celu wyświetlenia.



11.5 Mapa budynku

Można włożyć widok z góry (jpg, gif, bmp, tif, png itp.) do mapy budynku dla każdego piętra oddzielnie albo użyć linii prostych do narysowania własnego planu. Na każdym piętrze można umieścić jedynie ikony przypisanych urządzeń z panelu ikon za pomocą funkcji Drag & Drop (przeciągnij i upuść). Można wydrukować mapę budynku z ikonami albo można zapisać ją jako obraz BMP przy pomocy pozycji Drukuj lub Eksportuj w menu głównym.



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

11.6 Serwis

Przełączanie trybu centrali alarmowej między stanem 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).

11.7 Konserwacja

Przełączanie trybu centrali alarmowej między stanem Rozbrojona a trybem konserwacji.

11.8 Odśwież

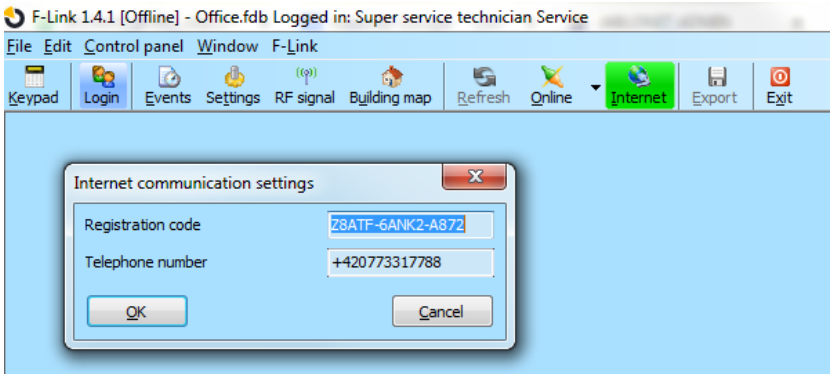
Aktualizacja ustawień wewnętrznych urządzeń po zmianie sprzętu, np. dodaniu segmentów do modułów dostępu lub klawiatur.

11.9 Online

Połączenie z programem F-Link lub rozłączenie z nim z centrali alarmowej za pomocą przewodu USB. Po połączeniu program automatycznie znajdzie port, którego centrala alarmowa używa do komunikacji.

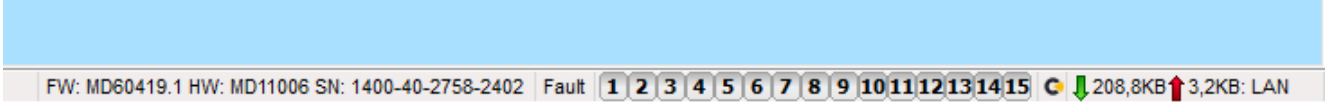
11.10 Internet

Zdalne połączenie z programem F-Link lub rozłączenie z nim z 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 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. W przypadku korzystania z karty SIM Security ta opcja jest wyłączona.



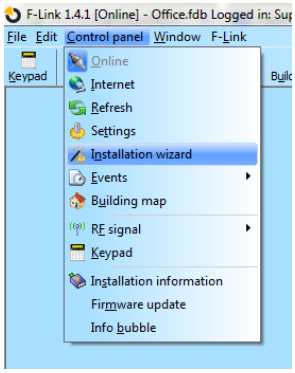
Kliknięcie przycisku Internet wyświetli okno dialogowe z wcześniej wprowadzonymi danymi. Jeśli łączą się Państwo z nowej, „pustej" bazy danych, należy wprowadzić kod rejestracji i numer telefonu. W przypadku korzystania z karty SIM Security i połączenia LAN nie trzeba wprowadzać numeru telefonu. Ustanowienie połączenia trwa zaledwie kilka sekund, ale pobranie konfiguracji zależy od wielkości systemu i zwykle może potrwać od 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.*



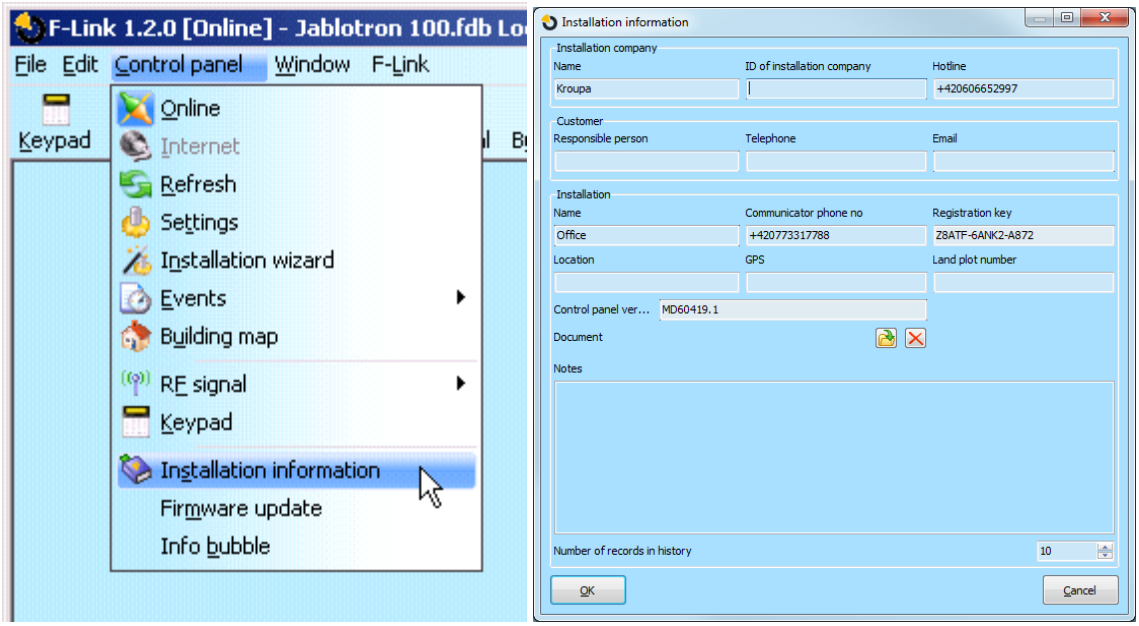
11.11 Kreator instalacji

Asystent stopniowego przechodzenia przez zakładki Ustawienia, co ułatwia procedurę programowania systemu. Kreatora aktywuje się w menu głównym Centrala alarmowa, a dezaktywuje przyciskiem Zamknij w prawym dolnym rogu okna Kreator.



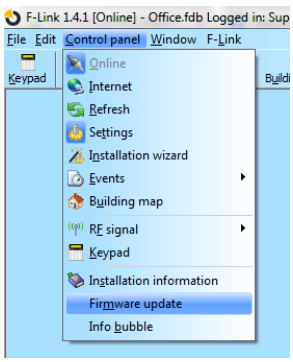
11.12 Informacje o instalacji

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.



11.13 Aktualizacje oprogramowania

Aktualizacja lub zmiana oprogramowania umożliwia zmianę zachowania urządzeń z możliwością aktualizacji (centrala alarmowa, moduły radiowe, klawiatury, czujki itp.) o pakiet, który producent oficjalnie umieszcza na serwerze JABLOTRON. F-Link automatycznie pobiera z serwera JABLOTRON (po zapytaniu), jeżeli w menu F-Link aktywna jest pozycja Automatyczne aktualizacje (w ustawieniu domyślnym jest aktywna). Jeżeli ta pozycja nie jest aktywna, przed aktualizacją F-Link umożliwi ręczne znalezienie plików FWP w komputerze.

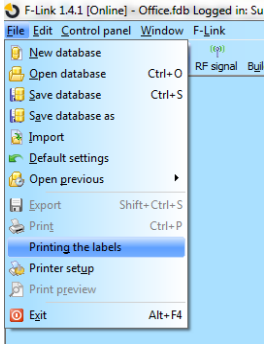


JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

11.14 Drukowanie etykiet

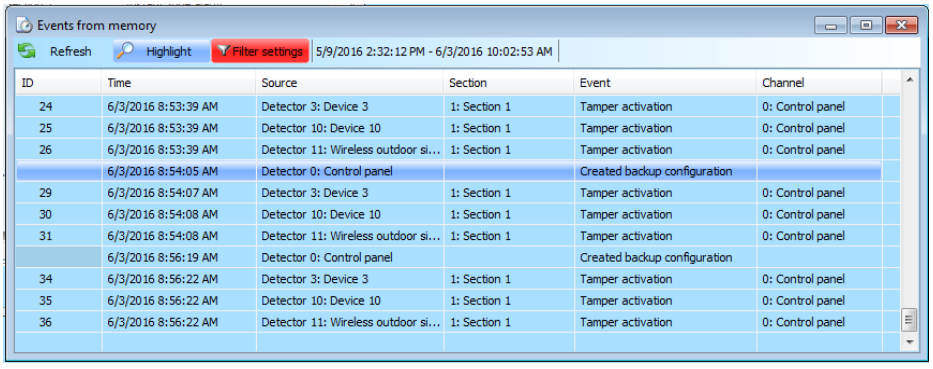
Aby wydrukować etykiety z nazwami faktycznie używanego segmentu modułów dostępowych, można korzystać z funkcji Drukuj etykiety w oknie Ustawienia wewnętrzne każdego z używanych modułów dostępowych, patrz rozdział 10.5.1.1 Zakładka Segmenty.

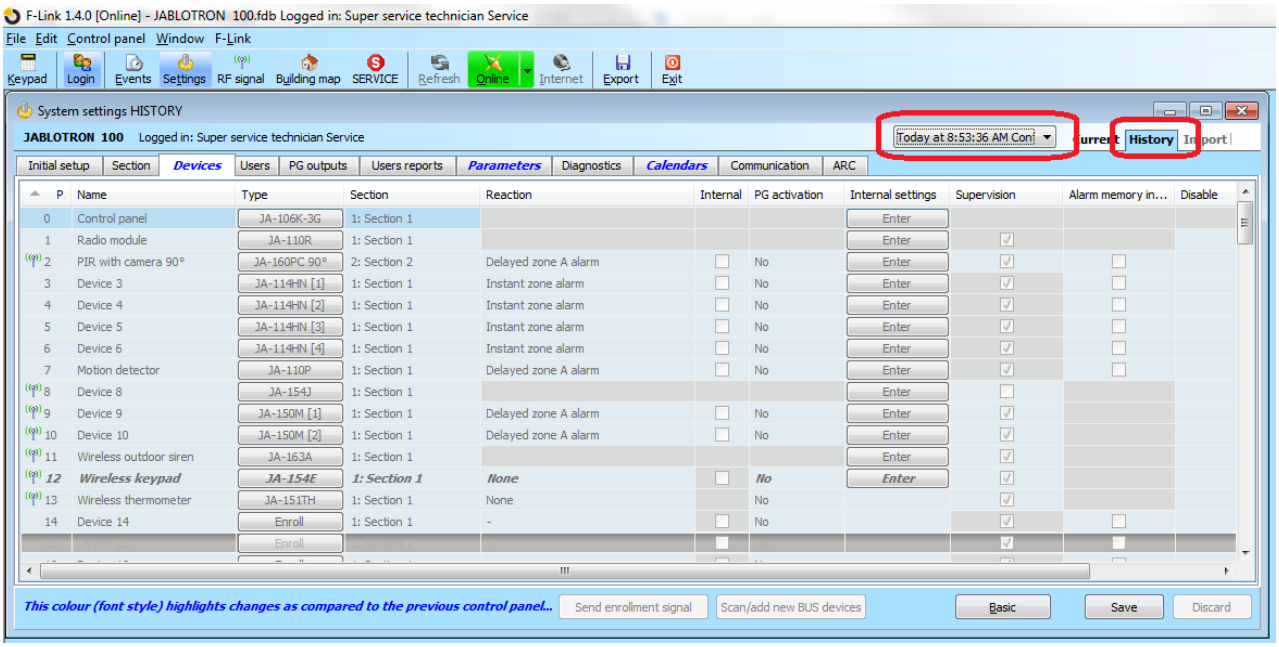
Można wprowadzić własny tekst do wydruku. Po wydruku oprogramowanie nie zapisuje tekstów poddanych edycji, w związku z czym nie ma możliwości ich wydrukowania po raz kolejny. Tekst na etykietach można wyrównać do lewej lub wyśrodkować.



11.15 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 wyszukać zdarzenia zmiany konfiguracji na podstawie daty i godziny, do porównania z aktualnym programowaniem systemu, załadować je i zajrzeć do zakładki „Historia” w prawym górnym rogu w oknie „Ustawienia systemu”. Zmiany w konfiguracji są zaznaczone niebieską kursywą. Z zapisanego pliku kopii zapasowej można akceptować zmiany, a przyciskiem „Zapisz” 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 poniższy sposób w programie F-Link w zakładce Parametry, gdy zaznaczono pozycję Reset dozwolony. Jeżeli Reset nie jest dozwolony i nie znają Państwo kodu serwisowego, nie mogą Państwo zresetować centrali alarmowej, a płytę centrali trzeba wysłać do dystrybutora.

Procedura:

1. Przełączyć centralę alarmową w tryb serwisowy (nieobowiązkowe).
2. Otworzyć pokrywę centrali alarmowej: Reset wymaga aktywności styku sabotażu. Jeżeli nie spełniono warunku w punkcie 1, 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 kabla złączowego dostarczonego w opakowaniu).
6. Najpierw podłączyć baterię, a następnie zasilanie centrali alarmowej i poczekać. Zaświecą się zielona, żółta i czerwona kontrolka przy kablu złączowym (jeśli pozostanie włączona tylko czerwona kontrolka, ustawienie Parametry / Reset dozwolony nie jest aktywne).
7. Odczekać około 15 sekund, a następnie odłączyć kabel złączowy.
8. Po upływie kilku sekund wszystkie kontrolki zaczną migać na potwierdzenie ukończenia resetowania centrali alarmowej. Później nastąpi ponowne uruchomienie napięcia centrali alarmowej i urządzeń MAGISTRALI, co zostanie potwierdzone miganiem wszystkich segmentów na klawiaturze.
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 pamięci SD. Jeżeli procedury resetowania nie przeprowadzono poprawnie, centrala alarmowa zachowa niezmienione pierwotne ustawienia.

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

13 Aktualizacje oprogramowania

Centrale alarmowe i niektóre inne urządzenia w systemie JABLOTRON 100+ umożliwiają zmianę oprogramowania. Oprogramowanie zwykle zmienia się w zakresie dozwolonym parametrami sprzętu.

13.1 Ogólne zasady aktualizacji oprogramowania (FW)

1. Zmianę można wprowadzić jedynie za pomocą komputera z zainstalowanym oprogramowaniem **F-Link** przy użyciu dostępu zdalnego za pomocą przewodu USB lub zdalnego, gdzie możliwość zmiany oprogramowania ogranicza się do urządzeń MAGISTRALI.
2. Oprogramowanie (FW) może zmienić użytkownik z upoważnieniem serwisowym.
3. Prosimy sprawdzić, czy korzystają Państwo z aktualnej wersji F-Link. Najnowsza wersja jest dostępna wyłącznie na stronie www.myjablotron.com, **MyCOMPANY / MySTORAGE / Oprogramowanie**, do której dostęp mają wyłącznie upoważnieni serwisanci po zalogowaniu. W przypadku zainstalowanego oprogramowania F-Link i dostępu do internetu F-Link automatycznie oferuje aktualizacje oprogramowania po uruchomieniu, a jednocześnie samodzielnie pobiera aktualny pakiet FW.
4. Podłączyć komputer do centrali alarmowej przewodem USB (w zestawie z centralą alarmową).
5. Uruchomić program **F-Link** z podłączoną centralą alarmową.
6. Przełączyć centralę alarmową w tryb **Serwis**.
7. Uruchomić **Centrala alarmowa / Aktualizacja firmware**
   Jeżeli w menu **F-Link** jest dozwolona **Automatyczna aktualizacja** (włączona w ustawieniu domyślnym), wyświetli się wykaz urządzeń, które można aktualizować. 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. Jego aktualność jest gwarantowana automatycznie w czasie pobierania programu F-Link.

Lokalizacja parametru Automatyczna aktualizacja:

13.2 Aktualizacje FW dla centrali alarmowej i urządzeń połączonych z MAGISTRALĄ

1. W oknie wyboru Aktualizacji firmware wyświetlają się jedynie urządzenia MAGISTRALI z możliwością aktualizacji oraz centrala alarmowa. F-Link automatycznie wybiera urządzenia, dla których konieczna jest aktualizacja (ich oprogramowanie jest starsze od oprogramowania FW w pakiecie).
2. F-Link ostrzega, kiedy można zaktualizować urządzenia bezprzewodowe. Informacje na temat procedury aktualizacji urządzeń bezprzewodowych podano w rozdziale 13.3 Aktualizacja FW dla urządzeń bezprzewodowych.
3. Bardziej szczegółowe informacje na temat istniejącej i nowej wersji poszczególnych urządzeń wyświetlają się w formie podpowiedzi w dymkach po najechaniu kursorem myszy na poszczególne urządzenia.
4. W polach wyboru należy zaznaczyć urządzenia, dla których chcą Państwo zmienić FW. Jeżeli w zaoferowanych opcjach znajduje się centrala alarmowa z propozycją nowszej wersji FW, zalecamy, by pozostawić jej zaznaczenie. Niektóre pozycje mogą być obowiązkowe, a tym samym niedostępne (wyszarzone) do anulowania aktualizacji.
5. Jeżeli zaznaczona jest opcja aktualizacji centrali alarmowej, wyświetla się możliwość zachowania zmodyfikowanego menu głosowego użytkownika. Jeżeli możliwość zachowania menu jest nieaktywna, zostanie przywrócone domyślne ustawienie menu głosowego.
6. Kliknąć OK, aby rozpocząć aktualizację FW 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 FW może zmienić się część kodu rejestracji. Jego zmiana nie wpłynie na możliwość dostępu zdalnego (przy pomocy F-Link) lub ewentualną komunikację centrali alarmowej z usługą MyJABLOTRON.
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. Choć aktualizacja FW nie zmienia zachowania systemu, należy przeprowadzić kontrolę zgodnie z opisem w rozdziale Kontrola po aktualizacji 13.4 Check after a FW FW.

13.3 Aktualizacje FW dla urządzeń bezprzewodowych.

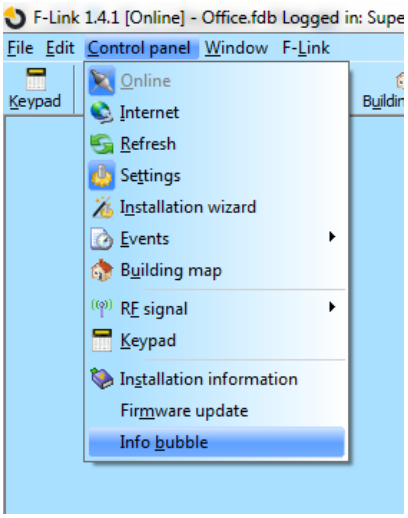
1. Aktualizację FW urządzeń bezprzewodowych wykonuje się w ten sam sposób, co w przypadku urządzeń MAGISTRALI. W przypadku niepowodzenia tego sposobu aktualizacji należy wykonać poniższe czynności:
2. Otworzyć urządzenie bezprzewodowe do aktualizacji (np. JA-152E, JA-153E, JA-154E, JA-160PC, AC-160DIN itp.), naciskając zaczep.
3. Jeżeli zawiera baterie, należy je usunąć i odłączyć ewentualne zewnętrzne źródło zasilania.
4. Uruchomić program F-Link, otworzyć bazę danych i podłączyć przewód USB do komputera (miniUSB lub microUSB zależnie od używanego urządzenia).

   ***Ostrzeżenie**: Przewody USB nie wchodzą w zakres dostawy poszczególnych urządzeń. Zalecamy korzystanie z bezpośredniego połączenia USB z komputerem, ponieważ ewentualne połączenie z HUBEM USB może zmniejszyć niezawodność.*
5. Aktualizację FW urządzeń bezprzewodowych należy prowadzić stopniowo, nie można jej wykonać jednocześnie przy użyciu większej liczby przewodów USB.
6. W urządzeniu bezprzewodowym do aktualizacji wejść w tryb do wczytywania nowego FW. W przypadku innych urządzeń przestrzegać zaleceń w poszczególnych instrukcjach.
7. Następnie postępować tak samo, jak w przypadku aktualizacji systemu za pomocą programu **F-Link: Centrala alarmowa → Aktualizacja firmware.**
8. W tabeli wyboru urządzeń należy wybrać pozycję USB (zwykle na pierwszym miejscu).
9. Bardziej szczegółowe informacje na temat istniejącej i nowej wersji poszczególnych urządzeń wyświetlają się w formie podpowiedzi w dymkach po najechaniu kursorem myszy na poszczególne urządzenia.
10. Naciśnięcie przycisku OK pozwoli zaktualizować wszystkie urządzenia.
11. Po ukończeniu aktualizacji odłączyć przewód USB, ponownie włożyć baterie lub podłączyć zasilanie i złożyć moduł.
12. Przeprowadzić kontrolę zgodnie z opisem w rozdziale 13.4 Check after a FW .
13. Przejść do aktualizacji kolejnego urządzenia bezprzewodowego.

13.4 Kontrola po aktualizacji 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. Jeżeli przeprowadzono reset 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 posiadały ustawienia domyślne. Sprawdzić je i dostosować ustawienia do potrzeb instalacji.
3. Sprawdzić ustawienia i przetestować działanie zaktualizowanych urządzeń.

13.5 Dymek informacyjny



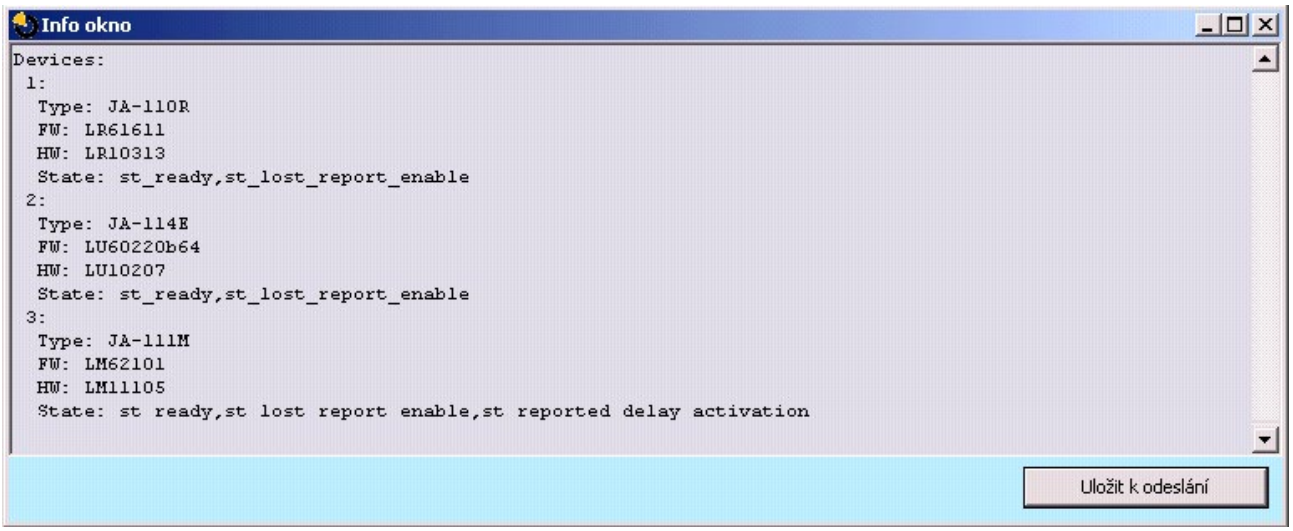
Otwiera się go z menu głównego **Centrala alarmowa / Dymek informacyjny.** Podczas generowania Dymku informacyjnego centrala alarmowa kontaktuje się z wszystkimi podłączonymi urządzeniami i urządzeniami bezprzewodowymi, prosząc o aktualne informacje.

Dymek **informacyjny** oferuje ogólny przegląd danych technicznych całego systemu, w tym centrali alarmowej (numer seryjny, kod rejestracji, wersja FW i sprzętu, napięcie i natężenie zasilania MAGISTRALI, zakres ustawień: urządzeń, stref, wyjść PG), wszystkich używanych komunikatorów (GSM: numer telefonu, numer sygnału BTS lub LAN: stan, MAC, IP, PSTN, stan linii telefonicznej), a także wszystkich urządzeń MAGISTRALI i bezprzewodowych (jedno- i dwukierunkowych): typ urządzenia,

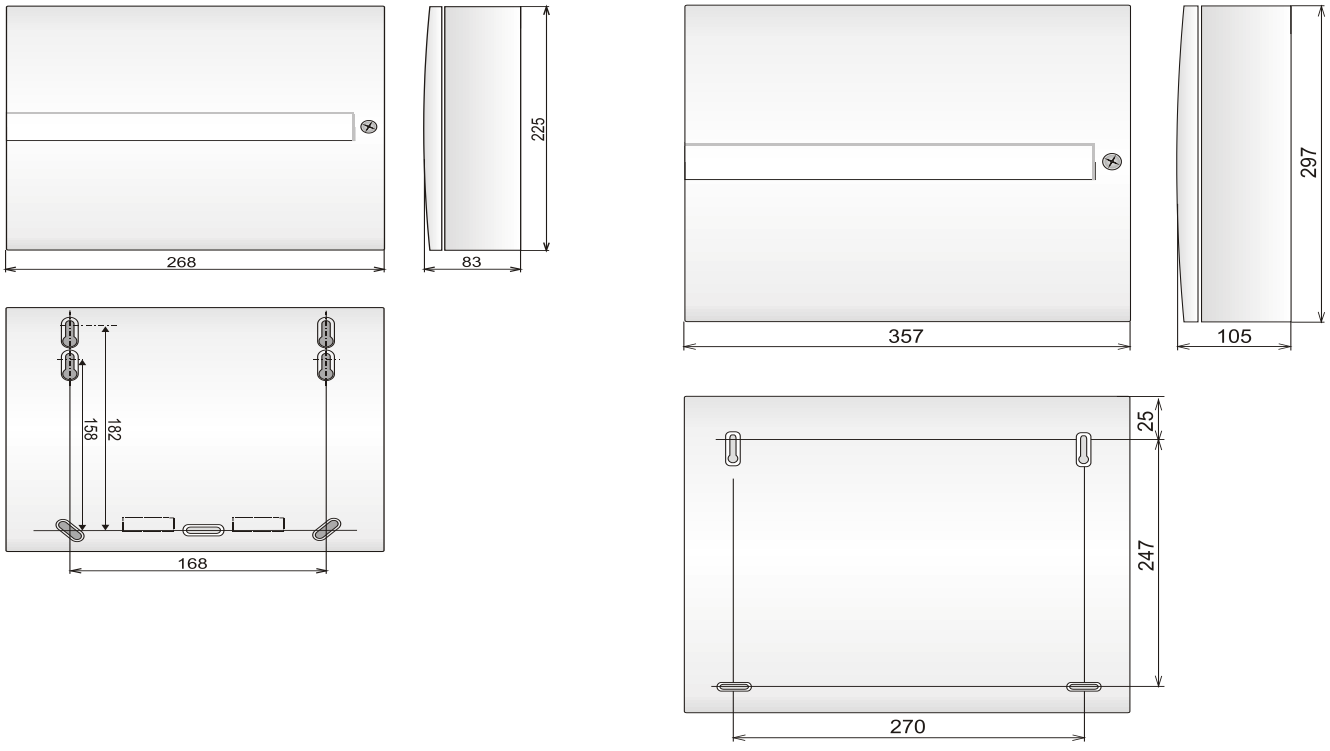
JABLOTRON ALARMS a.s.
Pod Skalkou 4567/33 | 46601 | Jablonec n. Nisou
Czech Republic | www.jablotron.com

identyfikacja wersji FW / sprzętu poszczególnych urządzeń i ich stanu. Jest dostępny we wszystkich stanach systemu (uzbrojony/rozbrojony/serwis).

Te dane są niezbędne np. do komunikacji z konsultantem technicznym, do czego przeznaczony jest przycisk Zapisz do wysłania znajdujący się w prawym dolnym rogu. Plik jest skompresowany, zawiera dane numeryczne instalacji, w tym część historii zdarzeń (100 kB), ale nie zawiera żadnych danych wrażliwych, jak numery telefonów użytkowników czy ich kody dostępu, ani innych danych poufnych. Zapisany plik osiąga rozmiar rzędu setek kB, dzięki czemu można go rozsyłać zwykłymi sposobami, np. pocztą elektroniczną.



13.6 Wymiary centrali alarmowej



14 Aplikacja sieciowa MyJABLOTRON

Aplikacja sieciowa MyJABLOTRON jest unikalną usługą, która zapewnia użytkownikom i instalatorom dostęp online do urządzeń produkowanych przez firmę Jablotron. Klienci firmy Jablotron mogą z niej korzystać w celu administrowania swoimi systemami. Użytkownicy końcowi alarmów mogą używać jej do sterowania i monitorowania swojego urządzenia. Zapewnia instalatorom potężne narzędzie, które pozwala im monitorować wszystkie zainstalowane alarmy i nimi administrować, a także wygodnie tworzyć oferty cenowe na nowe instalacje.

Wszystkie dane dotyczące alarmów lub instalacji są dostępne w jasnym formacie w jednej aplikacji dostępnej z dowolnego miejsca.

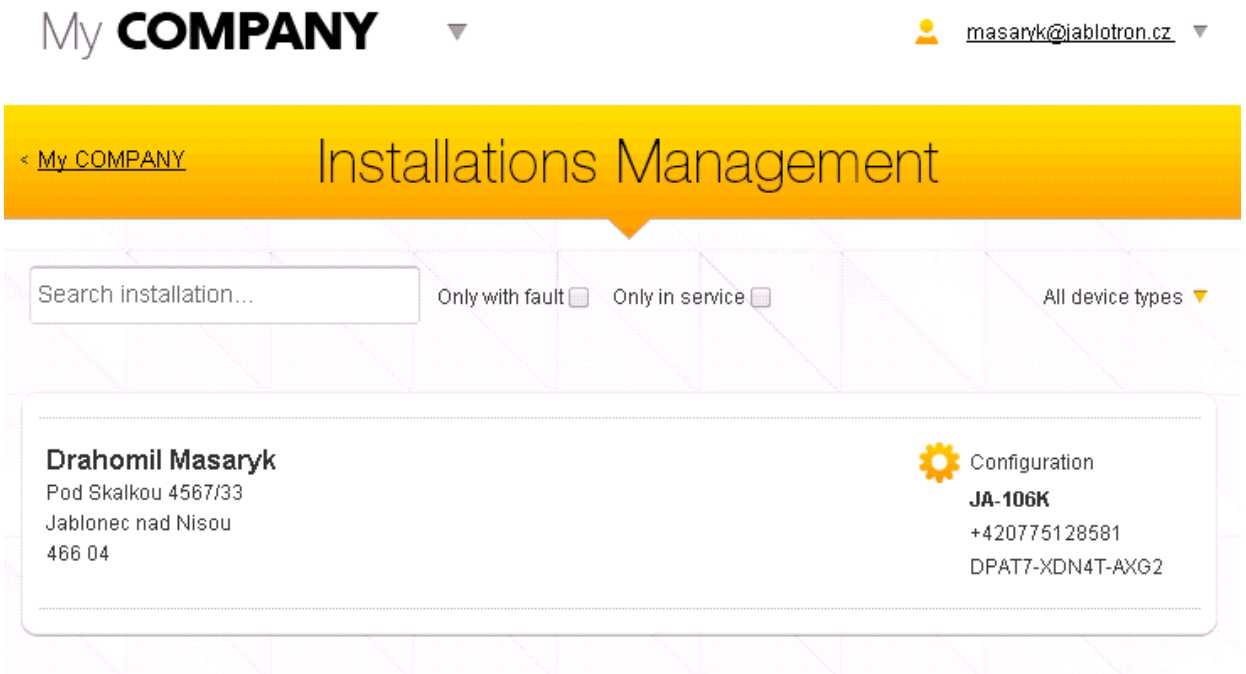
Aplikacja MyJABLOTRON pozwala użytkownikom:

- Sprawdzać **aktualny stan alarmu** (w kreatorze wstępnym zarejestrowane urządzenia są widoczne wraz z ostatnim zarejestrowanym zdarzeniem i liczbą stref w stanie rozbrojonym i uzbrojonym).
- **Uzbroić/rozbroić alarm** lub jego część.
- **Sterować wyjściami** programowalnymi (najczęściej do sterowania urządzeniami).
- Wyświetlać historię zdarzeń z możliwością eksportu jej do pliku.
- **Wyświetlać, i jeżeli możliwe, robić zdjęcia** za pomocą urządzeń do weryfikacji.
- **Monitorować przebieg temperatury** w budynku lub na zewnątrz (z powiadomieniem o przekroczeniu górnego lub dolnego limitu zdanych temperatur o określonej porze dnia).
- **Monitorować zużycie elektryczności** (w tym ustawienie powiadomienia w przypadku przekroczenia zużycia godzinnego/dobowego/miesięcznego).
- **Wysyłać wiadomości** do wybranych osób do kontaktu w formie SMS, poczty elektronicznej, standardowych powiadomień PUSH na telefony komórkowe.
- Oraz inne przydatne funkcje.

14.1 Zarządzanie instalacjami i ofertami dla instalatora

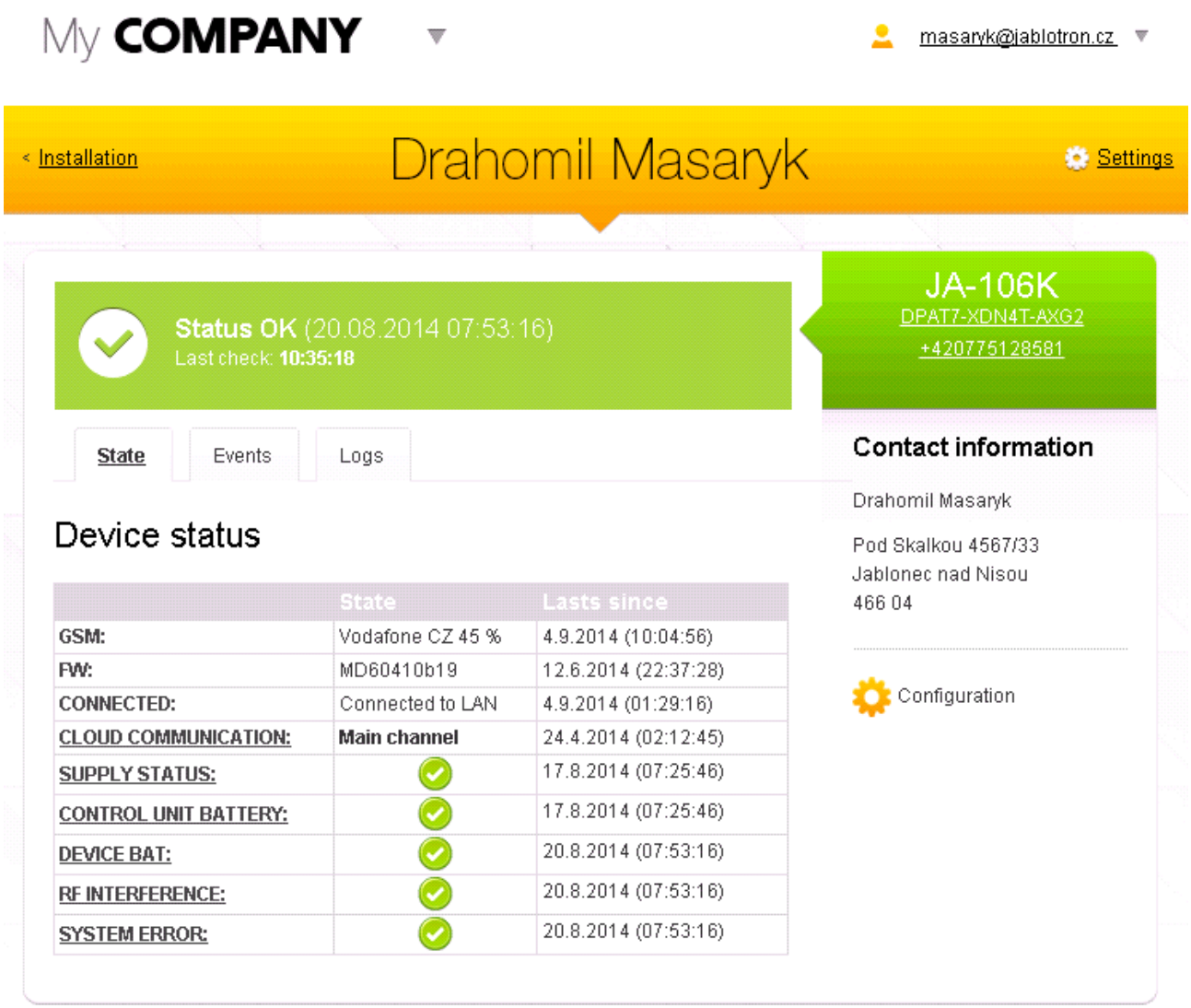
Przegląd wszystkich zainstalowanych urządzeń zarejestrowanych w MyJABLOTRON — Moduł do zarządzania instalacją

Jest to unikalne narzędzie dla instalatorów, którzy zarządzają wszystkimi zainstalowanymi przez siebie systemami w jednym miejscu, w tym pełnym przeglądem ich aktualnego stanu technicznego, widokiem historii i diagnostyką działania. Moduł **Zarządzanie instalacją** znajdą Państwo na swoim koncie w aplikacji MyJABLOTRON w części **MyCOMPANY** (jeżeli jest obsługiwana w Państwa regionie).



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

Własne instalacje można przefiltrować na podstawie typu alarmu lub w oparciu o ich aktualny stan. Tym samym można wstępnie ustawić powiadomienie dla problemu technicznego i szybko na nie odpowiedzieć w formie interwencji serwisowej. W ten sposób można zapewnić klientowi usługę o podwyższonym standardzie, ponieważ skontaktują się z nim Państwo, zanim klient zacznie rozwiązywać problem związany z systemem.



W danych każdej centrali alarmowej instalator ma ogólny przegląd w formie wyświetlania stanu poszczególnych grup błędów (stany zasilania, komunikacji, stan baterii w urządzeniach, zakłócenia lub inne błędy, typ karty SIM w urządzeniu i aktualna jakość sygnału GSM, aktualna wersja FW) z datą, od kiedy stan jest aktywny. Oprócz tego technik ma dostęp do przeglądu kompletnej historii zdarzeń, lecz wymaga ona dopuszczenia przez właściciela budynku w jego własnych ustawieniach.

W aplikacji **Zarządzanie instalacją** znajdą Państwo także kompletny rejestr zdarzeń technicznych alarmu z przedstawieniem graficznym jakości połączenia GSM, historii zmian oprogramowania lub komunikacji.

14.2 Aplikacja WEB-Link (konfiguracja)

WEB-Link jest niezwykle przydatną aplikacją dla instalatora w ramach usługi sieciowej MyJABLOTRON. Jest ona bardzo podobna do oprogramowania F-Link, ale różnica polega na tym, że ta aplikacja działa na serwerze i jest dostępna z dowolnej lokalizacji za pośrednictwem dowolnej przeglądarki sieciowej. Należy uruchomić aplikację, klikając ikonę Konfiguracja w Zarządzanie instalacją w MyCOMPANY. Instalator jest w stanie z dowolnego komputera zmienić niemal wszystkie ustawienia w systemie przypisanym do jego profilu niezależnie od miejsca, w którym się znajduje i platformy, z której korzysta. Zmiany wprowadzone przez instalatora zapisują się na serwerze i mogą zostać zapisane w systemie natychmiast lub po upływie określonego czasu, który można ustawić, lub po rozbrojeniu systemu przez użytkownika. Instalator może otrzymać informacje o zmianach za pomocą wiadomości SMS lub poczty elektronicznej.

15 Odbiór systemu przez użytkownika

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

1. Sterowanie z klawiatury systemu. Uzbrajanie i rozbrajanie stref (z segmentów kontrolnych 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 takie opcje, jak kody z prefiksem i bez niego, breloki RFID itp.
4. Częściowe uzbrojenie w domu. Różnice sygnalizacji uzbrojenia częściowego i pełnego.
5. Sterowanie automatyką domową przy pomocy segmentów kontrolnych 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 za pomocą aplikacji MyJABLOTRON ze smartfonów lub ze strony internetowej.
11. Edycja kodów użytkownika przez użytkownika za pomocą klawiatury i programu J-Link.

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. Zbliżającą się coroczną kontrolę można automatycznie sygnalizować klientowi za pomocą klawiatury LCD.

16 Specyfikacja techniczna

<table>
<tr><th>Parametr</th><th colspan="2">JA-103K</th><th colspan="2">JA-107K</th></tr>
<tr><td>Zasilanie centrali alarmowej</td><td colspan="2">~ 110–230 V / 50–60 Hz, maks. 0,28 A
z bezpiecznikiem F 1,6 A/250 V
Klasa ochronności II</td><td colspan="2">~ 110–230 V / 50–60 Hz, maks. 0,85 A
z bezpiecznikiem F 1,6 A/250 V
Klasa ochronności II</td></tr>
<tr><td>Bateria awaryjna</td><td colspan="2">12 V; 2,6 Ah (ołowiowo-żelowa)</td><td colspan="2">12 V; 7 do 18 Ah (ołowiowo-żelowa)</td></tr>
<tr><td>Maksymalny czas ładowania baterii</td><td colspan="2">72 h</td><td colspan="2">72 h</td></tr>
<tr><td>Napięcie magistrali BUS
(czerwono–czarna)</td><td colspan="2">od 12,0 V do 13,8 V</td><td colspan="2">od 12,0 V do 13,8 V</td></tr>
<tr><td>Maksymalne ciągłe zużycie mocy z centrali alarmowej</td><td colspan="2">1000 mA</td><td colspan="2">2000 mA stałe
3000 mA przez 60 minut
(maks. 2000 mA dla jednej MAGISTRALI)</td></tr>
<tr><td rowspan="3">Maks. ciągłe zużycie prądu do zasilania awaryjnego
12 godzin</td><td colspan="2">JA-103K — bateria awaryjna 2,6 Ah</td><td colspan="2">JA-107K — bateria awaryjna 18 Ah</td></tr>
<tr><td>Bez komunikatora GSM</td><td>LAN OFF (sieć LAN wył.)
115 mA
LAN ON (sieć LAN wł.)
88 mA</td><td>Bez komunikatora GSM</td><td>LAN OFF (sieć LAN wył.)
1135 mA
LAN ON (sieć LAN wł.)
1107 mA</td></tr>
<tr><td>Z komunikatorem GSM</td><td>LAN OFF (sieć LAN wył.)
80 mA
LAN ON (sieć LAN wł.)
53 mA</td><td>Z komunikatorem GSM</td><td>LAN OFF (sieć LAN wył.)
1100 mA
LAN ON (sieć LAN wł.)
1072 mA</td></tr>
<tr><td>Maksymalna liczba urządzeń</td><td colspan="2">50</td><td colspan="2">230</td></tr>
<tr><td>Komunikator LAN</td><td colspan="2">Interfejs ethernetowy, 10/100BASE</td><td colspan="2">Interfejs ethernetowy, 10/100BASE</td></tr>
<tr><td>Wymiary (mm)</td><td colspan="2">268 x 225 x 83</td><td colspan="2">357 x 297 x 105</td></tr>
<tr><td>Masa z/bez AKU</td><td colspan="2">1844 g / 970 g</td><td colspan="2">7027 g / 1809 g</td></tr>
<tr><td>Reakcja na wprowadzenie nieprawidłowego kodu</td><td colspan="4">Alarm po 10 próbach wprowadzenia nieprawidłowego kodu</td></tr>
<tr><td>Pamięć zdarzeń</td><td colspan="4">Około 7 milionów najnowszych zdarzeń, z datą i godziną</td></tr>
<tr><td>Zasilacz</td><td colspan="4">Typ A zgodnie z EN 50131-6</td></tr>
<tr><td>Komunikator GSM</td><td colspan="4">850 / 900 / 1800 / 1900 MHz</td></tr>
<tr><td>Klasyfikacja</td><td colspan="4">Klasa ochronności 2 wg EN 50131-1</td></tr>
<tr><td>Środowisko pracy</td><td colspan="4">Klasa środowiskowa II (wewnętrzne ogólne) wg EN 50131-1</td></tr>
<tr><td>Zakres temperatur pracy</td><td colspan="4">od -10°C do +40°C</td></tr>
<tr><td>Średnia wilgotność pracy</td><td colspan="4">75% (bez kondensacji)</td></tr>
<tr><td>Spełnia wymogi:</td><td colspan="4">EN 50131-1 wyd. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1,
EN 50131-6 wyd. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN 50581</td></tr>
<tr><td>Robocza częstotliwość radiowa
(z modułem JA-11xR)</td><td colspan="4">868,1 MHz</td></tr>
<tr><td>Emisje radiowe</td><td colspan="4">ETSI EN 300 220-1, -2 (moduł R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)</td></tr>
<tr><td>Kompatybilność elektromagnetyczna</td><td colspan="4">EN 50130-4 wyd. 2+A1, EN 55032 wyd. 2, ETSI EN 301 489-7</td></tr>
<tr><td>Zgodność w zakresie bezpieczeństwa</td><td colspan="4">EN 62368-1+A11</td></tr>
<tr><td>Identyfikacja rozmówcy (CLIP)</td><td colspan="4">ETSI EN 300 089</td></tr>
<tr><td>Warunki pracy</td><td colspan="4">ERC REC 70-03</td></tr>
<tr><td>Organ certyfikujący</td><td colspan="4">Trezor Test s.r.o. (nr 3025)</td></tr>
</table>

Firma JABLOTRON ALARMS a.s. oświadcza niniejszym, że urządzenia JA-103K oraz JA-107K zaprojektowano i wyprodukowano zgodnie z wymaganymi przepisami harmonizacyjnymi Unii Europejskiej: Dyrektywy nr: 2014/53/UE, 2014/35/UE, 2014/30/UE, 2011/65/UE w przypadku używania zgodnie z przeznaczeniem. Oryginał oceny zgodności znajduje się na stronie www.jablotron.com w sekcji *Do pobrania*.

Uwaga: Choć te produkty nie zawierają żadnych szkodliwych materiałów, sugerujemy, by zużyte produkty oddać do komunalnego punktu odbioru odpadów elektronicznych lub do dystrybutora, lub bezpośrednio do producenta. Bardziej szczegółowe informacje znajdują się na stronie www.jablotron.com w sekcji *Do pobrania*.

UWAGI:

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