

Centrale alarmowe

INTEGRA PLUS

Wersja oprogramowania 1.17

Satel[®] 

INSTRUKCJA UŻYTKOWNIKA



SATEL sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
POLSKA
tel. 58 320 94 00
serwis 58 320 94 30
dz. techn. 58 320 94 20; 604 166 075
www.satel.pl

OSTRZEŻENIA

Przed przystąpieniem do użytkowania centrali należy zapoznać się z niniejszą instrukcją w celu uniknięcia błędów, które mogą skutkować wadliwym działaniem sprzętu.

Wprowadzanie w urządzeniu jakichkolwiek modyfikacji, które nie są autoryzowane przez producenta, lub dokonywanie samodzielnych napraw skutkuje utratą uprawnień wynikających z gwarancji.

Centrale INTEGRA Plus współpracują tylko z analogowymi łączami abonentkimi. W przypadku zmiany analogowej sieci telefonicznej na inną należy skonsultować się z instalatorem systemu alarmowego.

Należy zwrócić szczególną uwagę na częstą zajętość linii telefonicznej wykorzystywanej przez centralę oraz zgłaszanie awarii dotyczących tej linii lub monitoringu. Sytuacje takie należy niezwłocznie zgłaszać instalatorowi systemu alarmowego.

Właściwą ochronę zapewnia tylko sprawny system alarmowy, dlatego firma SATEL zaleca jego regularne testowanie. Centrala wyposażona została w szereg funkcji autodiagnostycznych, które po odpowiednim skonfigurowaniu przez instalatora zapewniają kontrolę nad poprawnością działania systemu.

System alarmowy nie zapobiegnie włamaniu, napadowi lub pożarowi, jednak w przypadku sytuacji alarmowej umożliwia podjęcie działań, które ograniczą potencjalne szkody (poinformowanie o alarmie przy pomocy sygnalizacji optycznej lub dźwiękowej, powiadomienie o alarmie odpowiednich służb itd.). Dzięki temu może odstraszać potencjalnych włamywaczy.

Firma SATEL stawia sobie za cel nieustanne podnoszenie jakości swoich produktów, co może skutkować zmianami w ich specyfikacji technicznej i oprogramowaniu. Aktualna informacja o wprowadzanych zmianach znajduje się na naszej stronie internetowej.

Proszę nas odwiedzić:

<http://www.satel.pl>

Deklaracja zgodności jest dostępna pod adresem www.satel.eu/ce

Hasła fabryczne:

Hasło serwisowe: 12345

Hasło administratora partycji 1: 1111

W instrukcji mogą wystąpić następujące symbole:



- uwaga;



- uwaga krytyczna.

SPIS TREŚCI

1.	Wprowadzenie	3
2.	Sprawność techniczna systemu alarmowego	3
3.	Koszty funkcjonowania systemu alarmowego	3
4.	Autoryzacja użytkowników	4
4.1	Autoryzacja przy pomocy dwóch identyfikatorów	4
4.2	Hasła fabryczne	4
4.3	Działanie pod przymusem	5
5.	Obsługa systemu alarmowego przy pomocy manipulatora	5
5.1	Opis manipulatorów	5
5.1.1	Wyświetlacz LCD	5
5.1.2	Diody LED	7
5.1.3	Klawisze	8
5.1.4	Wbudowany czytnik kart zbliżeniowych	8
5.1.5	Sygnalizacja dźwiękowa	8
5.2	[Hasło]# – menu załączenia / wyłączenia czuwania	9
5.2.1	Menu załączenia czuwania	10
5.2.2	Menu wyłączenia czuwania	10
5.3	[Hasło]* – menu użytkownika	10
5.3.1	Lista funkcji	10
5.3.2	Uruchamianie funkcji	14
5.3.3	Skróty w menu	14
5.3.4	Wprowadzanie danych przy pomocy manipulatora	15
5.3.5	Opis funkcji użytkownika	17
5.4	Załączenie czuwania	22
5.4.1	Załączenie pełnego czuwania bez wybierania stref	22
5.4.2	Załączenie pełnego czuwania w wybranych strefach	23
5.4.3	Załączenie wybranego typu czuwania	23
5.4.4	Szybkie załączenie czuwania	23
5.4.5	Odmowa załączenia czuwania	23
5.4.6	Niepowodzenie procedury załączania czuwania	24
5.4.7	Skrócenie czasu na wyjście	24
5.5	Wyłączenie czuwania i kasowanie alarmu	24
5.5.1	Kasowanie alarmu bez wyłączenia czuwania	24
5.6	Załączanie / wyłączanie czuwania na 2 hasła	24
5.7	Wywołanie alarmu z manipulatora	25
5.8	Użytkownicy	25
5.8.1	Typy użytkowników	27
5.8.2	Dodanie nowego użytkownika	27
5.8.3	Edycja użytkownika	28
5.8.4	Usunięcie użytkownika	28
5.8.5	Dodanie karty zbliżeniowej / pastylki DALLAS	28
5.8.6	Dodanie pilota	29
5.8.7	Usunięcie pilota	30
5.9	Administratorzy	30
5.10	Blokowanie wejść	30
5.10.1	Czasowe blokowanie wejść	31
5.10.2	Trwałe blokowanie wejść	31
5.10.3	Odblokowanie wejść	32
5.11	Przeglądanie zdarzeń	32

5.11.1	Przegląd wszystkich zdarzeń.....	32
5.11.2	Przegląd zdarzeń wymaganych dla Grade 3	32
5.11.3	Przegląd wybranych zdarzeń.....	32
5.11.4	Sposób prezentowania zdarzeń	33
5.12	Programowanie timera strefy	33
5.13	Testowanie wejść	34
5.14	Sterowanie.....	35
5.14.1	Sterowanie wyjściem typu PRZEŁĄCZNIK MONO	36
5.14.2	Sterowanie wyjściem typu PRZEŁĄCZNIK BI	36
5.14.3	Sterowanie wyjściami typu PRZEKAŹNIK TELEFONICZNY	36
5.14.4	Sterowanie wyjściami roletowymi	36
6.	Obsługa klawiatury strefowej	36
6.1	Opis klawiatur strefowych	37
6.1.1	Diody LED	37
6.1.2	Klawisze	38
6.1.3	Wbudowany czytnik kart zbliżeniowych	38
6.1.4	Sygnalizacja dźwiękowa	38
6.2	Funkcje dostępne z klawiatury strefowej	39
6.2.1	[Hasło]*	39
6.2.2	[Hasło]#	39
6.2.3	Szybkie załączenie czuwania	39
6.2.4	Wywołanie alarmu z klawiatury	40
6.2.5	Wyciszenie sygnalizacji alarmu w klawiaturze	40
6.2.6	Zmiana hasła	40
7.	Obsługa klawiatury wejściowej	40
7.1	Diody LED	40
7.2	Sygnalizacja dźwiękowa	40
7.3	Funkcje dostępne z klawiatury wejściowej.....	41
8.	Obsługa zamka szyfrowego	41
8.1	Opis zamków szyfrowych	42
8.1.1	Diody LED	42
8.1.2	Klawisze	42
8.1.3	Sygnalizacja dźwiękowa	42
8.2	Funkcje dostępne z zamka szyfrowego	42
9.	Potwierdzanie powiadamiania głosowego	43
10.	Odpowiadanie na telefon i sterowanie telefoniczne	43
10.1	Odpowiadanie na telefon	43
10.2	Sterowanie telefoniczne.....	44
10.3	Dźwiękowa weryfikacja alarmu	44
11.	Obsługa systemu alarmowego przy pomocy pilota	45
12.	Historia zmian w treści instrukcji	46
13.	Skrócony opis obsługi systemu z manipulatora	50

1. Wprowadzenie

Instrukcja dotyczy central alarmowych z serii INTEGRA Plus:

- INTEGRA 64 Plus
- INTEGRA 128 Plus
- INTEGRA 256 Plus

Miło nam, że wybraliście Państwo oferowany przez nas produkt. Życzymy zadowolenia z dokonanego wyboru i pragniemy zapewnić, że zawsze jesteśmy gotowi służyć fachową pomocą i informacją na temat naszych produktów.

Firma SATEL sp. z o.o. jest producentem szerokiej gamy urządzeń dedykowanych do stosowania w systemach alarmowych. Dodatkowe informacje na ich temat można uzyskać na stronie internetowej **www.satel.pl** lub w punktach sprzedaży oferujących nasze produkty.



Zaleca się, aby instalator przygotował własną instrukcję obsługi systemu alarmowego, który zainstalował. Powinna ona uwzględniać wszystkie zmiany i modyfikacje w stosunku do ustawień fabrycznych.

Instalator powinien przeszkolić użytkowników z zasad obsługi systemu alarmowego.

2. Sprawność techniczna systemu alarmowego

Niesprawność jakiegokolwiek elementu systemu alarmowego skutkuje zmniejszeniem poziomu ochrony. Tymczasem urządzenia montowane na zewnątrz (np. sygnalizatory zewnętrzne) wystawione są na niekorzystny wpływ czynników atmosferycznych. Podczas burz, na skutek wyładowań atmosferycznych, na uszkodzenia narażone są urządzenia podłączone do instalacji elektrycznej lub linii telefonicznej.

Centrala alarmowa jest wyposażona w szereg zabezpieczeń i automatycznych funkcji diagnostycznych testujących sprawność systemu. W przypadku wykrycia awarii, informuje o niej np. dioda  w manipulatorze. **Należy natychmiast reagować na taką sytuację i w razie konieczności konsultować się z instalatorem.**

Dodatkowo, w centrali dostępne są funkcje służące do testowania systemu alarmowego. Pozwalają one sprawdzić, czy prawidłowo działają czujki, sygnalizatory, komunikatory telefoniczne itp. **Tylko regularne testowanie i kontrola systemu alarmowego pozwalają zachować wysoki poziom ochrony przed włamaniem.**

Zalecane jest, aby instalator, na zlecenie użytkownika, przeprowadzał okresowe konserwacje systemu alarmowego.

W interesie użytkownika jest przewidzenie i zaplanowanie zasad postępowania, gdy centrala zasygnalizuje alarm. Istotna jest umiejętność zweryfikowania alarmu i określenia jego źródła oraz podjęcie odpowiednich działań (np. ewakuacja w przypadku alarmu pożarowego).

3. Koszty funkcjonowania systemu alarmowego

Centrala alarmowa może informować użytkowników oraz stację monitorującą o stanie chronionego obiektu. Realizacja tych funkcji przy pomocy linii telefonicznej lub GSM oznacza koszty finansowe. Wysokość ponoszonych kosztów zależy od ilości wysyłanych informacji. Awaria łączy telefonicznych, a także niewłaściwy sposób zaprogramowania centrali, mogą spowodować wzrost kosztów (wykonywanie nadmiernej ilości połączeń).

Należy poinformować instalatora, co jest priorytetem: przekazanie informacji za wszelką cenę, czy zapobieganie nadmiernym kosztom. Przykładowo, kiedy nie udało się przesłać kodu zdarzenia do stacji monitorującej, centrala może wielokrotnie i co kilka minut próbować wysłać kod albo zaniechać prób wysłania kodu do czasu wystąpienia kolejnego zdarzenia.

4. Autoryzacja użytkowników

Obsługa systemu alarmowego jest możliwa po autoryzacji użytkownika, która pozwala centrali alarmowej zweryfikować, czy użytkownik jest uprawniony do wykonania danej operacji. Autoryzacja może odbywać się na podstawie:

- hasła,
- karty zbliżeniowej (transpondera pasywnego 125 kHz, który może mieć formę karty, breloka itd.),
- pastylki DALLAS,
- pilota.



Nie można przydzielić tego samego identyfikatora (hasła, karty zbliżeniowej, pastylki DALLAS lub pilota) dwóm użytkownikom.

Ze względów bezpieczeństwa różne osoby nie powinny posługiwać się tym samym identyfikatorem.

Instalator może tak skonfigurować centralę, że nie będzie ona akceptować haseł, które zawierają mniej niż trzy różne cyfry (np. 1111 lub 1212) lub składają się z kolejnych cyfr (3456).

Instalator może zezwolić na korzystanie z niektórych funkcji bez potrzeby autoryzacji użytkownika.

Trzykrotne użycie nieznanego hasła, karty zbliżeniowej lub pastylki DALLAS może:

- wywołać alarm,
- zablokować klawiaturę / czytnik na 90 sekund.

4.1 Autoryzacja przy pomocy dwóch identyfikatorów

Manipulatory INT-KLCDR i INT-KLFR oraz klawiatura INT-SCR posiadają wbudowany czytnik kart zbliżeniowych. Instalator może tak skonfigurować te urządzenia, że użytkownik w celu autoryzacji musi posłużyć się dwoma identyfikatorami: hasłem i kartą. Realizowana po autoryzacji funkcja zależy od drugiego użytego identyfikatora:

- hasło – czy zostanie zatwierdzone klawiszem #, czy *,
- karta – czy zostanie tylko zbliżona, czy przytrzymana.

4.2 Hasła fabryczne

Fabrycznie w centrali zaprogramowane są następujące hasła:

hasło serwisowe: 12345

hasło administratora partycji 1: 1111

Hasła fabryczne umożliwiają przydzielenie indywidualnych haseł kolejnym osobom, które mają użytkować system alarmowy (patrz: „Użytkownicy” s. 25).



Hasła fabryczne należy zmienić przed rozpoczęciem użytkowania systemu alarmowego (funkcja ZMIANA HASŁA dostępna w menu użytkownika).

Centrala może informować użytkownika o konieczności zmiany hasła, jeżeli hasło jest znane innym użytkownikom.

Hasło administratora nie powinno być używane na co dzień, ponieważ istnieje ryzyko jego podejrzenia. Zaleca się, aby administrator wprowadził dla siebie hasło zwykłego użytkownika.

4.3 Działanie pod przymusem

W przypadku działania pod przymusem, należy zamiast normalnego hasła użytkownika użyć hasła typu PRYMUS (patrz: „Typy użytkowników” s. 27).

5. Obsługa systemu alarmowego przy pomocy manipulatora

Firma SATEL oferuje następujące manipulatory dla central alarmowych INTEGRA Plus:

INT-TSG – manipulator z ekranem dotykowym,

INT-TSH – manipulator z ekranem dotykowym,

INT-TSI – manipulator z ekranem dotykowym,

INT-KSG – manipulator LCD z klawiaturą dotykową,

INT-KLCD – manipulator LCD z klawiaturą mechaniczną,

INT-KLCDR – manipulator LCD z klawiaturą mechaniczną i wbudowanym czytnikiem kart zbliżeniowych,

INT-KLCDK – manipulator LCD z klawiaturą mechaniczną,

INT-KLCDL – manipulator LCD z klawiaturą mechaniczną,

INT-KLCDS – manipulator LCD z klawiaturą mechaniczną,

INT-KLFR – manipulator LCD z klawiaturą mechaniczną i wbudowanym czytnikiem kart zbliżeniowych.

Manipulatory mogą być dostępne z różnymi wariantami kolorystycznymi obudowy, wyświetlacza, czy podświetlenia klawiszy. O wariantach kolorystycznych informuje dodatkowe oznaczenie umieszczane w nazwie manipulatora (np. INT-KLCD-GR – zielony wyświetlacz i podświetlenie klawiszy; INT-KLCD-BL – niebieski wyświetlacz i podświetlenie klawiszy).

5.1 Opis manipulatorów



Manipulatory INT-TSG, INT-TSH, INT-TSI i INT-KSG opisane są w odrębnych instrukcjach, dodawanych do tych manipulatorów.

5.1.1 Wyświetlacz LCD

Wyświetlacz ułatwia komunikację między użytkownikiem a systemem alarmowym. W przejrzysty sposób informuje o stanie systemu. Prezentowane są na nim funkcje, z których użytkownik może korzystać. Istnieje możliwość podświetlenia wyświetlacza.

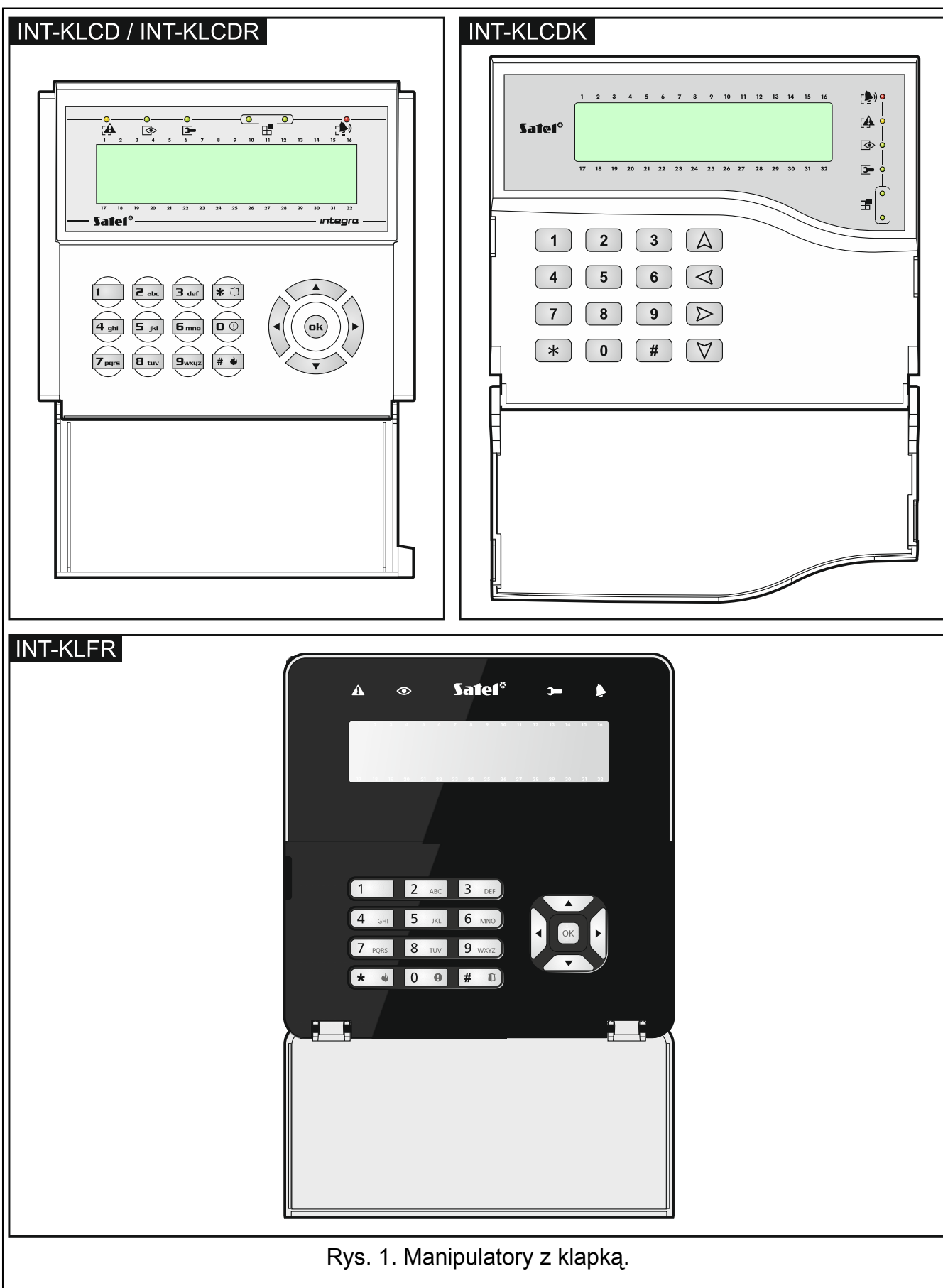
W **trybie gotowości** wyświetlacz prezentuje:

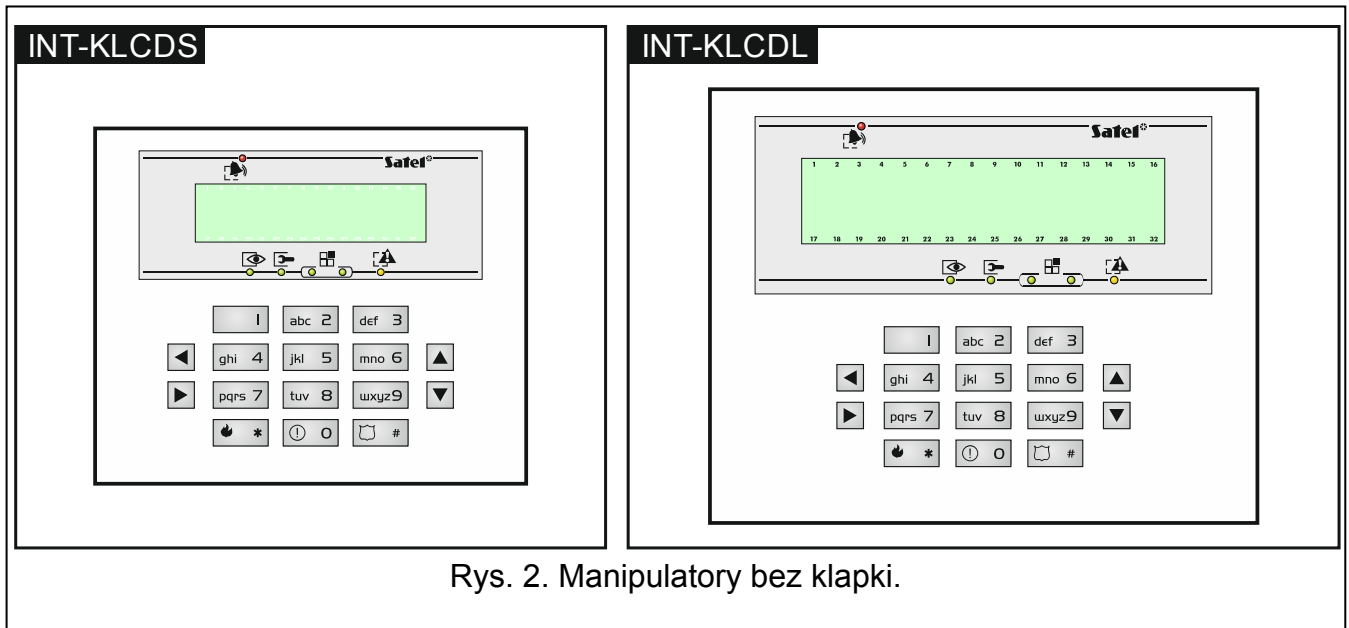
- w górnej linii datę i czas w formacie zdefiniowanym przez instalatora
- w dolnej linii nazwę manipulatora albo stan wybranych stref (określa to instalator).

Instalator może tak skonfigurować manipulator, że naciśnięcie na około 3 sekundy klawisza 9 spowoduje przełączenie wyświetlacza w **tryb wyświetlania stanu stref**. Przy pomocy symboli prezentowany jest stan stref obsługiwanych przez manipulator (obejmuje to także strefy, z których manipulator sygnalizuje alarm). Powrót do trybu gotowości nastąpi po ponownym naciśnięciu na około 3 sekundy klawisza 9.

W przypadku wystąpienia określonych zdarzeń, na wyświetlaczu pojawić się mogą dodatkowe komunikaty (np. załączenie lub wyłączenie czuwania, odliczanie czasu

opóźnienia automatycznego załączenia czuwania, odliczanie czasu na wejście lub wyjście, alarm itd.).





Rys. 2. Manipulatory bez klapy.

Po wprowadzeniu przez użytkownika hasła, czyli autoryzacji użytkownika, wyświetlane jest menu zawierające funkcje, z których użytkownik może korzystać. Funkcje prezentowane są w dwóch liniach. Aktualnie wybrana funkcja wskazywana jest strzałką z lewej strony. Sposób prezentowania informacji w ramach funkcji zależy od specyfiki danej funkcji.

Sposób podświetlania wyświetlacza jest programowany przez instalatora.

5.1.2 Diody LED

Dioda	Kolor	Opis działania
	zielony	świeci – czuwają wszystkie strefy obsługiwane przez manipulator miga – czuwają niektóre strefy obsługiwane przez manipulator lub odliczany jest czas na wyjście
	czerwony	świeci lub miga – alarm lub pamięć alarmu
	żółty	miga – awaria lub pamięć awarii
	zielony	miga – uruchomiony jest tryb serwisowy
	zielony	w przypadku prezentowania stanu wejść lub przełączenia manipulatora w graficzny tryb programowania (patrz: „Wybór z listy wielokrotnego wyboru” s. 15), dwie diody informują, który zestaw danych jest wyświetlany (patrz: tabela 2)

Tabela 1. Opis diod LED manipulatora.

Typ danych	Dioda		Informacja
	lewa / górna	prawa / dolna	
Wejścia / wyjścia	nie świeci	nie świeci	numery 1-32
	nie świeci	świeci	numery 33-64
	świeci	nie świeci	numery 65-96
	świeci	świeci	numery 97-128
Ekspandery	nie świeci	nie świeci	adresy w systemie 0-31 (00-1F HEX)
	nie świeci	świeci	adresy w systemie 32-63 (20-3F HEX)

Tabela 2. Informacje prezentowane przez diody .



Informacja o czuwaniu może być wygaszana po czasie zdefiniowanym przez instalatora.

Jeżeli instalator włączył opcję globalną GRADE 3:

- dioda informuje o alarmach dopiero po wprowadzeniu hasła i zatwierdzeniu klawiszem *,
- miganie diody oznacza, że w systemie jest awaria, są zablokowane wejścia lub miał miejsce alarm.

5.1.3 Klawisze

Klawisze oznaczone cyframi i literami umożliwiają wprowadzanie hasła, a także danych podczas korzystania z funkcji dostępnych w menu. Dodatkowo naciśnięcie na około 3 sekundy wybranych przycisków z cyframi pozwala (o ile instalator skonfigurował tak manipulator):

- 1 - sprawdzić stan wejść,
- 4 - sprawdzić stan stref,
- 5 - przejrzeć pamięć alarmów,
- 6 - przejrzeć pamięć awarii,
- 7 - przejrzeć bieżące awarie,
- 8 - włączyć/wyłączyć sygnalizację GONG w manipulatorze,
- 9 - przełączyć wyświetlacz z trybu gotowości w tryb wyświetlania stanu stref i odwrotnie.

Pozostałe klawisze umożliwiają:

- * - wejście w menu użytkownika (po wprowadzeniu hasła),
- rezygnację z wykonania rozpoczętej operacji.
- # lub **ok** - załączenie lub wyłączenie czuwania oraz skasowanie alarmu (po wprowadzeniu hasła),
- uruchomienie wybranej funkcji,
- zatwierdzenie wprowadzonych danych.
- ◀ ▲ ▼ ▶ - poruszanie się po wyświetlaczu (przewijanie wyświetlanych komunikatów, funkcji i opcji, przesuwanie kursora),
- uruchomienie wybranych przez instalatora funkcji (po wprowadzeniu hasła).
- wywołanie alarmu pożarowego.
- wywołanie alarmu medycznego (pomocniczego).
- wywołanie alarmu napadowego.

5.1.4 Wbudowany czytnik kart zbliżeniowych

Manipulatory INT-KLCDR i INT-KLFR mogą być obsługiwane przy pomocy kart zbliżeniowych (breloków lub innych transponderów pasywnych 125 kHz). Instalator określa, jakie funkcje mogą być realizowane po zbliżeniu lub przytrzymaniu karty.

5.1.5 Sygnalizacja dźwiękowa

Dźwięki generowane w trakcie obsługi



Instalator może wyłączyć sygnalizację dźwiękową.

1 krótki dźwięk – naciśnięcie dowolnego klawisza z cyfrą.

2 krótkie dźwięki – potwierdzenie wykonanie polecenia, sygnalizacja wejścia w menu użytkownika, w podmenu lub w funkcję.

3 krótkie dźwięki – sygnalizacja:

- rozpoczęcia procedury załączenia czuwania (w strefie jest czas na wyjście) lub załączenia czuwania (w strefie nie ma czasu na wyjście),
- wyłączenia czuwania i/lub skasowania alarmu,
- wyłączenia wyjścia,
- wyłączenia sygnalizacji GONG w manipulatorze przy pomocy klawisza 8,
- przełączenia wyświetlacza z trybu gotowości w tryb prezentowania stanu stref i odwrotnie przy pomocy klawisza 9,
- wyjścia z funkcji i powrotu do menu po zatwierdzeniu wprowadzonych danych.

4 krótkie i 1 długi dźwięk – sygnalizacja:

- włączenia wyjścia,
- włączenia sygnalizacji GONG w manipulatorze przy pomocy klawisza 8,
- zakończenia funkcji i wyjścia z menu użytkownika po zatwierdzeniu wprowadzonych danych.

1 długi dźwięk – sygnalizacja:

- naruszonych / zablokowanych wejść podczas załączania czuwania,
- uszkodzenia czujki wibracyjnej (wejście o reakcji typu 10. 24H WIBRACYJNA nie zostało naruszone w trakcie testu czujek wibracyjnych uruchamianego po rozpoczęciu procedury załączenia czuwania).

2 długie dźwięki – nieznane hasło/karta, funkcja niedostępna lub wyjście z funkcji bez zatwierdzenia wprowadzonych danych (np. po użyciu klawisza *).

3 długie dźwięki – funkcja niedostępna.

Zdarzenia sygnalizowane dźwiękiem



Sygnalizowane są tylko te zdarzenia, które wybrał instalator.

Alarmy są sygnalizowane przez czas zaprogramowany przez instalatora.

5 krótkich dźwięków – naruszenie wejścia (sygnalizacja GONG).

Długi dźwięk co 3 sekundy, a następnie seria krótkich dźwięków przez 10 sekund i 1 długi dźwięk – odliczanie czasu na wyjście (jeżeli czas jest krótszy niż 10 sekund, wygenerowana zostanie jedynie końcowa sekwencja krótkich dźwięków).

Sekwencja 7 coraz krótszych dźwięków powtarzana co kilka sekund – odliczanie czasu opóźnienia autouzbrojenia.

2 krótkie dźwięki co sekundę – odliczanie czasu na wyjście.

2 krótkie dźwięki co 3 sekundy – sygnalizacja nowej awarii.

Dźwięk ciągły – alarm.

Długi dźwięk co sekundę – alarm pożarowy.

5.2 [Hasło]# – menu załączenia / wyłączenia czuwania



Informacje podane w rozdziale nie dotyczą użytkownika posiadającego uprawnienie UŻYTKOWNIK PROSTY (patrz: s. 26).

Po wpisaniu hasła i zatwierdzeniu klawiszem #:

- na wyświetlaczu może pojawić się komunikat o potrzebie zmiany hasła lub notatka serwisowa,

- zostanie skasowany alarm – jeżeli użytkownik posiada uprawnienie do kasowania alarmu i w systemie jest alarm,
- zostanie wyłączone czuwanie w jednej strefie – jeżeli użytkownik posiada uprawnienie do wyłączenia czuwania, dostęp tylko do jednej strefy obsługiwanej z manipulatora i strefa ta czuwa albo dostęp do wielu stref, ale tylko jedna strefa czuwa,
- zostanie załączone czuwanie w jednej strefie – jeżeli użytkownik posiada uprawnienie do załączenia czuwania, dostęp tylko do jednej strefy obsługiwanej z manipulatora i strefa ta nie czuwa,
- na wyświetlaczu pojawi się menu załączenia lub wyłączenia czuwania.

5.2.1 Menu załączenia czuwania

Menu załączenia czuwania zostanie wyświetlone jeżeli:

- użytkownik posiada uprawnienie do załączenia czuwania,
- użytkownik posiada dostęp do kilku stref obsługiwanych z manipulatora,
- żadna ze stref, do których użytkownik ma dostęp, nie czuwa,
- nie ma alarmu.

W menu dostępne są 2 funkcje:

Załącz wszystko	<i>załączenie czuwania we wszystkich strefach</i>
Załącz wybrane	<i>załączenie czuwania w wybranych strefach</i>

5.2.2 Menu wyłączenia czuwania

Menu wyłączenia czuwania zostanie wyświetlone jeżeli:

- użytkownik posiada uprawnienie do wyłączenia czuwania,
- użytkownik posiada dostęp do kilku stref obsługiwanych z manipulatora,
- co najmniej dwie strefy, do których użytkownik ma dostęp, czuwają.

W menu dostępne są 2 funkcje:

Wyłącz wszystko	<i>wyłączenie czuwania we wszystkich strefach</i>
Wyłącz wybrane	<i>wyłączenie czuwania w wybranych strefach</i>

5.3 [Hasło]* – menu użytkownika

Po wpisaniu hasła i zatwierdzeniu klawiszem * wyświetlane jest menu użytkownika. Lista dostępnych funkcji zależy od uprawnień użytkownika, stanu i konfiguracji systemu. W celu wyjścia z menu użytkownika należy nacisnąć klawisz *. Manipulator automatycznie wyjdzie z menu, jeżeli od naciśnięcia ostatniego klawisza upłynęły 2 minuty.



Po wpisaniu hasła i zatwierdzeniu klawiszem * na wyświetlaczu może pojawić się komunikat o potrzebie zmiany hasła lub notatka serwisowa.

5.3.1 Lista funkcji



Funkcje dostępne po wprowadzeniu hasła serwisowego zostały wyróżnione białym tekstem na czarnym tle. Ramką wyróżniono funkcje, które są dostępne dla administratorów.

Przeł.skas.al.	<i>przegląd skasowanych alarmów z wejść z wybranej strefy</i>
Przywróć system	<i>przywracanie systemu po alarmie zweryfikowanym</i>
Wyłącz czuwanie	<i>wyłączenie czuwania w wybranych strefach</i>
Kasuj alarm	<i>skasowanie alarmu</i>

Kasuj al.innych	<i>skasowanie alarmu w innych partycjach</i>
Kas.powiad.tel.	<i>skasowanie powiadamiania telefonicznego</i>
Załącz czuwanie	<i>załączenie czuwania w wybranych strefach</i>
Zał. na 2 hasła	<i>rozpoczęcie załączenia czuwania na dwa hasła</i>
Wył. na 2 hasła	<i>rozpoczęcie wyłączenia czuwania na dwa hasła</i>
Odrocz. zał.cz.	<i>odroczenie automatycznego załączenia czuwania</i>
Ustaw odroczen.	<i>program. czasu odroczenia automatycznego załączenia czuwania</i>
Tryb załączenia	<i>wybór trybu załączenia czuwania</i>
Anuluj 1 hasło	<i>anulowanie zgody na zał./wył. czuwania na dwa hasła</i>
Zmiana hasła	<i>zmiana własnego hasła</i>
Zmiana has.tel	<i>zmiana własnego hasła telefonicznego</i>

Zmiana prefiksów

Prefix normalny	<i>programowanie prefiksu używanego normalnie</i>
Prefix przymus	<i>programowanie prefiksu używanego w sytuacji zagrożenia</i>
Czas przypomin.	<i>programowanie czasu przypominania o potrzebie zmiany prefiksu</i>

Użytkownicy

Nowy użytkownik

Hasło	<i>dodanie nowego użytkownika</i>
Hasło telefon.	<i>programowanie hasła</i>
Strefy	<i>programowanie hasła telefonicznego</i>
Typ	<i>przydział stref, do których użytkownik ma mieć dostęp</i>
Schemat użyt.	<i>wybór typu hasła</i>
Czas istnienia	<i>wybór schematu czasowego</i>
Czas blokady	<i>programowanie czasu istnienia hasła</i>
Uprawnienia	<i>programowanie czasu blokady</i>
Klawiatury itp.	<i>przydział uprawnień</i>
Nowa karta	<i>przydział modułów, do których użytkownik ma mieć dostęp</i>
Usuń kartę	<i>dodanie karty zbliżeniowej</i>
Nowa pastylka	<i>usunięcie karty zbliżeniowej</i>
Usuń pastylkę	<i>dodanie pastylki DALLAS</i>
Nowy pilot RX	<i>usunięcie pastylki DALLAS</i>
Usuń pilota RX	<i>dodanie pilota 433 MHz</i>
Przycisk 1	<i>usunięcie pilota 433 MHz</i>
Przycisk 2	<i>przypisanie funkcji do przycisku 1 w pilocie</i>
Przycisk 3	<i>przypisanie funkcji do przycisku 2 w pilocie</i>
Przycisk 4	<i>przypisanie funkcji do przycisku 3 w pilocie</i>
Przycisk 1 i 2	<i>przypisanie funkcji do przycisku 4 w pilocie</i>
Przycisk 1 i 3	<i>przypisanie funkcji do kombinacji przycisków 1 i 2 w pilocie</i>
Zdarzenia RX	<i>przypisanie funkcji do kombinacji przycisków 1 i 3 w pilocie</i>
Nowy pilot ABAX	<i>programowanie zasad generowania zdarzeń</i>
Usuń pilot.ABAX	<i>dodanie pilota obsługiwanego przez system ABAX</i>
Przycisk 1	<i>usunięcie pilota obsługiwanego przez system ABAX</i>
Przycisk 2	<i>przypisanie funkcji do przycisku 1 w pilocie</i>
Przycisk 3	<i>przypisanie funkcji do przycisku 2 w pilocie</i>
	<i>przypisanie funkcji do przycisku 3 w pilocie</i>

Przycisk 4	<i>przypisanie funkcji do przycisku 4 w pilocie</i>
Przycisk 5	<i>przypisanie funkcji do przycisku 5 w pilocie</i>
Przycisk 1 i 5	<i>przypisanie funkcji do kombinacji przycisków 1 i 5 w pilocie</i>
Zdarzenia ABAX	<i>programowanie zasad generowania zdarzeń</i>
Potwierdz. ABAX	<i>programowanie zasad potwierdzania</i>
Nazwa	<i>programowanie nazwy użytkownika</i>
Edycja użyt.	<i>edycja istniejącego użytkownika</i>
[wybór użytkownika]	
[lista parametrów identyczna jak w przypadku nowego użytkownika]	
Usunięcie użyt.	<i>usunięcie użytkownika</i>
Administratorzy	
Nowy admin.	<i>dodanie nowego administratora</i>
Hasło	<i>programowanie hasła</i>
Uprawnienia	<i>przydział uprawnień</i>
Klawiatury itp.	<i>przydział modułów, do których administrator ma mieć dostęp</i>
Nowa karta	<i>dodanie karty zbliżeniowej</i>
Usuń kartę	<i>usunięcie karty zbliżeniowej</i>
Nowa pastylka	<i>dodanie pastylki DALLAS</i>
Usuń pastylkę	<i>usunięcie pastylki DALLAS</i>
Nowy pilot RX	<i>dodanie pilota 433 MHz</i>
Usuń pilota RX	<i>usunięcie pilota 433 MHz</i>
Przycisk 1	<i>przypisanie funkcji do przycisku 1 w pilocie</i>
Przycisk 2	<i>przypisanie funkcji do przycisku 2 w pilocie</i>
Przycisk 3	<i>przypisanie funkcji do przycisku 3 w pilocie</i>
Przycisk 4	<i>przypisanie funkcji do przycisku 4 w pilocie</i>
Przycisk 1 i 2	<i>przypisanie funkcji do kombinacji przycisków 1 i 2 w pilocie</i>
Przycisk 1 i 3	<i>przypisanie funkcji do kombinacji przycisków 1 i 3 w pilocie</i>
Zdarzenia RX	<i>programowanie zasad generowania zdarzeń</i>
Nowy pilot ABAX	<i>dodanie pilota obsługiwanego przez system ABAX</i>
Usuń pilot.ABAX	<i>usunięcie pilota obsługiwanego przez system ABAX</i>
Przycisk 1	<i>przypisanie funkcji do przycisku 1 w pilocie</i>
Przycisk 2	<i>przypisanie funkcji do przycisku 2 w pilocie</i>
Przycisk 3	<i>przypisanie funkcji do przycisku 3 w pilocie</i>
Przycisk 4	<i>przypisanie funkcji do przycisku 4 w pilocie</i>
Przycisk 5	<i>przypisanie funkcji do przycisku 5 w pilocie</i>
Przycisk 1 i 5	<i>przypisanie funkcji do kombinacji przycisków 1 i 5 w pilocie</i>
Zdarzenia ABAX	<i>programowanie zasad generowania zdarzeń</i>
Potwierdz. ABAX	<i>programowanie zasad potwierdzania</i>
Nazwa	<i>programowanie nazwy administratora</i>
Edycja admin.	<i>edycja istniejącego administratora</i>
[wybór administratora]	
[lista parametrów identyczna jak w przypadku nowego administratora]	
Usunięcie adm.	<i>usunięcie administratora</i>

Blokowanie wej.

Blokady czasowe

czasowe blokowanie wejść

Blokady trwałe

trwałe blokowanie wejść

Program. zegara

programowanie zegara centrali

Stan systemu

*sprawdzenie awarii / sprawdzenie stanu systemu***Przegl. zdarzeń****Wybrane**

Wybór zdarzeń

wybór typu zdarzeń, które mają być przeglądane

Wybór stref

wybór stref, z których zdarzenia mają być przeglądane

Przegląd

przegląd wybranych zdarzeń

Przegląd Grade3

przegląd zdarzeń wymaganych dla Grade 3

Wszystkie

przegląd wszystkich zdarzeń

Zdarz. Grade3

przegląd zdarzeń wymaganych dla Grade 3

Reset czujek

reset wyjść typu 43. ZASILANIE Z RESETEM

Wył.zatrz.wyjść

wyłączenie zatrzaśniętych wyjść centrali

Kon.otwar.drzwi

*koniec otwarcia pożarowego drzwi***Zmiana opcji**

Gong w manipul.

włączenie/wyłączenie sygnalizacji GONG w manipulatorze

Gong wyjść

blokowanie sygn. naruszeń wejść na wyjściach typu 11. GONG

Timery

edycja timerów

Temperatury

edycja prog. temp. i histerezy dla wyjść typu 120. TERMOSTAT

Timery stref

*programowanie timerów stref***Blok. sab.eksp.***blokowanie sabotaży ekspanderów***Stały dost.ser.***włączenie/wyłączenie stałego dostępu serwisu***Serwis edytuje***udostępnianie serwisowi edycji użytkowników***Serw. ZałWył...***udostępnianie serwisowi sterowania systemem***Stał. dos. DLOADX***włączenie/wyłączenie stałego dostępu programu DLOADX*

Adres DLOADX

programowanie adresu komputera z programem DLOADX

Adres GUARDX

programowanie adresu komputera z programem GUARDX

Skasowanie not.

*kasowanie notatki serwisowej***Testy**

Stan stref

sprawdzenie aktualnego stanu stref

Stan wejść

*sprawdzenie aktualnego stanu wejść***Napięcia zasil.***sprawdzenie napięcia zasilania modułów*

Urządzenia rad.

sprawdzenie poziomu sygnału radiowego urządzeń bezprzew.

Temperatury

*sprawdzenie temperatur mierzonych przez czujki ATD-100***Test wejść****Nowy**

Wej. właman.

uruchomienie nowego testu wejść włamaniowych

Wej. poż./tech.

uruchomienie nowego testu wejść pożarowych i technicznych

Wybrane wejście

uruchomienie nowego testu pojedynczego wejścia

Przegląd testu

przegląd wyników testu

Koniec testu

wcześniejsze zakończenie testu

Skasow. wyników

skasowanie wyników testu

Test akumulat.

Ręczna tr.test.

Test stacji 1A

Test stacji 1B

Test stacji 2A

Test stacji 2B

Test powiadam.

Test odb. tel.

Test karty

Test CA-64 PTSA

Przegląd admin.

Nazwa manipul.

Plik w DLOADX

Wersja centrali

Wersja prog.STM

IP/MAC ETHM-1

Wersje modułów

Synchron. czasu

Dostęp serwisu

Otwórz drzwi

Sterowanie

Tryb serwisowy**Przejęcie TS****Downloading****Start DWNL-RS****Koniec DWNL-RS**

Start DWNL-MOD.

Start DWNL-TEL

ETHM-1 – DLOADX

ETHM-1 – GUARDX

*test akumulatora i wejść 60. TECHNICZNA - AWARIA AKUMULATORA**uruchomienie ręcznej transmisji testowej**uruchomienie transmisji testowej do stacji 1 – podst. numer tel.**uruchomienie transmisji testowej do stacji 1 – zapasowy numer tel.**uruchomienie transmisji testowej do stacji 2 – podst. numer tel.**uruchomienie transmisji testowej do stacji 2 – zapasowy numer tel.**uruchomienie testu powiadamiania**wyświetlenie informacji na temat odbieranego połączenia tel.**sprawdzenie numeru karty zbliżeniowej**uruchomienie testu tablicy synoptycznej**przegląd administratorów**wyświetlenie nazwy manipulatora**wyświetlenie inf. o pliku programu DLOADX z danymi centrali**wyświetlenie informacji o wersji oprogramowania centrali**wyśw. inf. o wersji programu obsługującego zasilacz i wejścia**wyśw. inf. o adresie IP i MAC modułu ETHM-1 / ETHM-1 Plus**wyświetlenie informacji o wersji oprogramowania modułów**uruchomienie synchronizacji czasu**programowanie czasu dostępu serwisu**otwarcie wybranych drzwi kontrolowanych przez system**sterowanie wyjściami**uruchomienie trybu serwisowego**przejęcie trybu serwisowego**uruchomienie programowania lokalnego**zakończenie programowania lokalnego**uruchomienie komunikacji przez modem zewnętrzny**uruchomienie komunikacji przez modem 300 bps**uruchomienie komunikacji przez Ethernet z programem DLOADX**uruchomienie komunikacji przez Ethernet z programem GUARDX***5.3.2 Uruchamianie funkcji**

1. Przy pomocy klawiszy ▼ i ▲ znaleźć żądane podmenu lub funkcję. Aktualnie wybrane podmenu lub funkcja wskazywana jest strzałką (→) z lewej strony.
2. Naciśnąć klawisz ► lub #, żeby wejść w podmenu (klawisz ◀ umożliwia wyjście z podmenu) lub uruchomić funkcję.

5.3.3 Skróty w menu

Instalator może wyłączyć obsługę skrótów w menu użytkownika.

Do niektórych elementów menu (podmenu, funkcje) można uzyskać szybki dostęp dzięki skrótom. Naciśnięcie klawisza oznaczonego cyfrą (lub sekwencji klawiszy) spowoduje wejście w podmenu lub uruchomienie funkcji. Lista podmenu i funkcji dostępnych przy pomocy skrótów przedstawiona została poniżej. Skróty podane zostały w nawiasach kwadratowych.

[1] Zmiana hasła

- [2] Użytkownicy
 - [21] Nowy użytkownik
 - [22] Edycja użytkownika
 - [23] Usunięcie użytkownika
- [4] Blokowanie wejść
 - [41] Blokady czasowe
 - [42] Blokady trwałe
- [5] Przegląd zdarzeń
 - [51] Przegląd wybranych zdarzeń
 - [52] Przegląd wszystkich zdarzeń
- [6] Programowanie zegara
- [7] Stan systemu
- [8] Sterowanie
- [9] Tryb serwisowy
- [0] Downloading
 - [01] Start DWNL-RS
 - [02] Koniec DWNL-RS
 - [03] Start DWNL-MOD.
 - [04] Start DWNL-TEL
 - [07] ETHM-1 – DLOADX
 - [08] ETHM-1 – GUARDX



Jeżeli serwis nie może edytować użytkowników, skróty zaczynające się od cyfry 2 umożliwiają serwisowi uruchamianie funkcji z podmenu ADMINISTRATORZY.

5.3.4 Wprowadzanie danych przy pomocy manipulatora

Dane są zapisywane w centrali po naciśnięciu klawisza # (w niektórych manipulatorach dostępny jest dodatkowo klawisz , pełniący identyczną funkcję). Klawisz * umożliwia wyjście z funkcji bez zapisania zmian.

Poniżej opisano ogólne zasady wprowadzania danych, jednak w przypadku niektórych funkcji mogą one być inne.

Wybór z listy pojedynczego wyboru

W górnej linii wyświetlacza znajduje się opis funkcji, a w dolnej aktualnie wybrana pozycja. Listę przewija się przy pomocy klawisza ▼ (w dół) lub ▲ (w górę). Klawisze ► i ◀ nie są wykorzystywane.

Wybór z listy wielokrotnego wyboru

Funkcje, które pozwalają dokonać wielokrotnego wyboru, można rozpoznać po tym, że po prawej stronie wyświetlacza znajduje się dodatkowy symbol:

 – wyświetlana pozycja jest wybrana / opcja jest włączona,

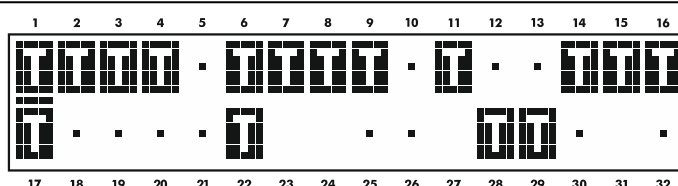
• – wyświetlana pozycja nie jest wybrana / opcja jest wyłączona.

Naciśnięcie klawisza z dowolną cyfrą (w niektórych funkcjach nie dotyczy to klawisza 0) powoduje zmianę wyświetlanego aktualnie symbolu na drugi. Listę przewija się przy pomocy klawisza ▼ (w dół) lub ▲ (w górę). W przypadku niektórych funkcji, po naciśnięciu klawisza 0 można wprowadzić numer pozycji, która ma być edytowana (np. numer wejścia, które ma zostać zablokowane / odblokowane). Przyśpiesza to wyszukiwanie.

W przypadku niektórych funkcji, naciśnięcie klawisza ► lub ◄ przełącza manipulator w **graficzny tryb programowania**. Przy pomocy symboli ■ i · prezentowany jest na wyświetlaczu bieżący status do 32 dostępnych w ramach funkcji pozycji (mogą to być np. wejścia, strefy itp.). W przypadku blokowania wejść, dodatkowo używany jest symbol ■. Klawisz ► przesuwa kursor w prawo, a klawisz ◄ w lewo. Jeżeli lista pozycji jest dłuższa niż 32, naciśnięcie klawisza ►, gdy kursor jest na ostatniej pozycji spowoduje wyświetlenie następnej listy, a naciśnięcie klawisza ◄, gdy kursor jest na pierwszej pozycji – poprzedniej listy (patrz też opis diod LED ■ s. 7). W trybie graficznym trzykrotne naciśnięcie w ciągu 3 sekund klawisza 0, 1 lub 2 spowoduje:

- 000** - wyświetlenie na wszystkich dostępnych pozycjach symbolu · ,
- 111** - wyświetlenie na wszystkich dostępnych pozycjach symbolu ■,
- 222** - odwrócenie dokonanego wyboru: na wszystkich pozycjach, gdzie wyświetlany był symbol · pojawi się ■, a gdzie był ■ – będzie · .

Po naciśnięciu klawisza ▼ lub ▲ manipulator wraca do trybu tekstowego.



Rys. 3. Przykład prezentowania informacji w graficznym trybie programowania. Pola puste są niedostępne do edycji.

Wprowadzanie liczb dziesiętnych i szesnastkowych

Cyfry wpisuje się poprzez naciśnięcie odpowiednich klawiszy. Znaki od A do F dostępne są pod klawiszami oznaczonymi cyframi 2 i 3. Klawisze te należy naciskać tak długo, aż pojawi się żądany znak.

Wprowadzanie nazw

Poszczególne klawisze należy naciskać tak długo, aż pojawi się żądany znak. Znaki dostępne w manipulatorze prezentowane są w tabeli 3. Dłuższe przytrzymanie klawisza spowoduje wyświetlenie cyfry przypisanej do klawisza.

Klawisz	Znaki dostępne po kolejnym naciśnięciu klawisza																		
1	!	?	'	`	←	"	{	}	\$	%	&	@	\	^		↵	#	1	
2	a	ą	b	c	ć	2													
3	d	e	ę	f	3														
4	g	h	i	4															
5	j	k	l	ł	5														
6	m	n	ń	o	ó	6													
7	p	q	r	s	ś	7													
8	t	u	v	·	■	■	↑	←	→	↓	8								
9	w	x	y	z	ż	ż	9												
0		.	,	:	;	+	-	*	/	=	_	<	>	(	)	[	]	0	

Tabela 3. Znaki dostępne podczas wprowadzania nazw. Duże litery dostępne są pod tymi samymi klawiszami (zmiana wielkości liter: klawisz ▼).

W górnej linii wyświetlacza, po lewej stronie, wyświetlana jest informacja o wielkości liter: [Abc], [ABC] lub [abc] (zostanie wyświetlona po naciśnięciu dowolnego klawisza i będzie wyświetlana przez kilka sekund od ostatniego naciśnięcia klawisza).

Klawisz ► przesuwa kursor w prawo, a klawisz ◀ w lewo. Klawisz ▲ kasuje znak z lewej strony kursora.

5.3.5 Opis funkcji użytkownika

Przegląd skasowanych alarmów – dostępna, jeśli po skasowaniu alarmu użytkownik nie dokonał przeglądu naruszonych wejść. Pozwala sprawdzić, które wejścia wywołały alarm. Po zakończeniu przeglądu funkcja jest niedostępna.

Przywróć system – dostępna dla serwisu, jeżeli w centrali włączona jest opcja NIE ZAŁĄCZAJ CZUWANIA PO ALARMIE ZWERYFIKOWANYM i miał miejsce alarm zweryfikowany. Po wystąpieniu alarmu zweryfikowanego konieczne jest przywrócenie systemu przy pomocy tej funkcji, zanim możliwe będzie ponowne załączenie czuwania.

Wyłącz czuwanie – pozwala wyłączyć czuwanie w strefach dostępnych dla użytkownika z danego manipulatora.

Kasuj alarm – umożliwia zakończenie sygnalizacji alarmu w systemie.

Kasuj alarmy innych partycji – umożliwia skasowanie sygnalizacji alarmów z innych partycji, do których użytkownik normalnie nie ma dostępu.

Kasuj powiadamianie telefoniczne – przerywa powiadamianie telefoniczne.



Powiadamianie może być kasowane automatycznie razem z kasowaniem alarmu. Zasady kasowania powiadamiania określa instalator.

Załącz czuwanie – umożliwia załączenie czuwania w strefach dostępnych dla użytkownika z danego manipulatora.

Załącz na 2 hasła – umożliwia zainicjowanie załączania czuwania w strefach wymagających podania 2 haseł.

Wyłącz na 2 hasła – umożliwia zainicjowanie wyłączania czuwania w strefach wymagających podania 2 haseł.

Odroczenie załączenia czuwania – dostępna, gdy trwa odliczanie opóźnienia autouzbrojenia. Pozwala odroczyć o zaprogramowany czas automatyczne załączenie czuwania w strefie, w której trwa odliczanie opóźnienia autouzbrojenia. Wpisanie samych zer oznacza zablokowanie autouzbrojenia (do następnego terminu autouzbrojenia).

Ustaw odroczenie załączenia czuwania – dostępna, jeżeli co najmniej dla jednej strefy zaprogramowany jest czas opóźnienia autouzbrojenia i w strefie tej nie jest on aktualnie odliczany. Pozwala odroczyć o zaprogramowany czas automatyczne załączenie czuwania w strefie.

Tryb załączenia – umożliwia wybór typu czuwania, który ma zostać załączony (w nawiasie kwadratowym podano klawisz skrótu):

- [0] **pełne czuwanie** (do stosowania, gdy wszyscy opuścili chroniony obszar),
- [1] **pełne czuwanie + blokady** (umożliwia pozostanie w chronionym obszarze) – zablokowane zostaną wejścia, dla których instalator włączył opcję BLOKOWANE PRZY BRAKU WYJŚCIA Z OBIEKTU,
- [2] **czuwanie bez wewnętrznych** (umożliwia pozostanie w chronionym obszarze):
 - wejścia wewnętrzne (typ reakcji 3. OPÓŹNIONA WEWNĘTRZNA) nie będą czuwać,
 - naruszenie wejścia zewnętrznego (typ reakcji 8. ZEWNĘTRZNA) wywoła cichy alarm,
 - naruszenie innego wejścia alarmowego wywoła głośny alarm.
- [3] **czuwanie bez wewnętrznych i bez czasu na wejście** (umożliwia pozostanie w chronionym obszarze – do stosowania, gdy nikt już nie będzie wchodził do

chronionego obszaru) – typ czuwania analogiczny do poprzedniego, ale wejścia opóźnione działają jak natychmiastowe (nie ma czasu na wejście).

Anuluj 1 hasło – jeżeli czuwanie jest załączane / wyłączane przy pomocy dwóch haseł i pierwsze hasło zostało wprowadzone, można jeszcze anulować zgodę na załączenie / wyłączenie czuwania.

Zmiana hasła – pozwala użytkownikowi na zmianę własnego hasła.

Zmiana hasła telefonicznego – pozwala użytkownikowi na zmianę własnego hasła telefonicznego.

Zmiana prefiksów – dostępna dla administratora, jeżeli instalator przewidział stosowanie prefiksów w systemie (określił długość prefiksów). Umożliwia programowanie prefiksów oraz czasu przypominania o potrzebie zmiany prefiksu. Każde hasło będzie musiało zostać poprzedzone prefiksem:

normalny – do codziennego użytku. Fabrycznie składa się z cyfr 0 w odpowiedniej liczbie (np. jeśli długość prefiksu ustalona została na 4, domyślny prefiks ma postać: 0000),

PRZYMUS – do stosowania, gdy użytkownik został zmuszony do wprowadzenia hasła. Jego użycie wywoła cichy alarm. Fabrycznie składa się z cyfr 4 w odpowiedniej liczbie (np. jeśli długość prefiksu ustalona została na 3, domyślny prefiks ma postać: 444).

Użytkownicy – w podmenu dostępne są następujące funkcje:

Nowy użytkownik – umożliwia utworzenie nowego użytkownika (patrz: „Dodanie nowego użytkownika” s. 27).

Edycja użytkownika – umożliwia edycję istniejących użytkowników (patrz: „Edycja użytkownika” s. 28).

Usunięcie użytkownika – umożliwia kasowanie istniejących użytkowników (patrz: „Usunięcie użytkownika” s. 28).



Administrator określa, czy serwis ma dostęp do podmenu UŻYTKOWNICY (opcja SERWIS EDYTUJE w podmenu ZMIANA OPCJI).

Administratorzy – w podmenu dostępne są dla serwisu następujące funkcje:

Nowy administrator – umożliwia utworzenie nowego administratora.

Edycja administratora – umożliwia edycję istniejących administratorów.

Usunięcie administratora – umożliwia kasowanie istniejących administratorów.

Blokowanie wejść – w podmenu dostępne są następujące funkcje:

Blokady czasowe – umożliwia czasowe blokowanie wejść (patrz: „Czasowe blokowanie wejść” s. 31).

Blokady trwałe – umożliwia trwałe blokowanie wejść (patrz: „Trwałe blokowanie wejść” s. 31).



Jeżeli instalator włączył opcję globalną GRADE 3, funkcja BLOKADY TRWAŁE dostępna jest tylko dla serwisu.

Programowanie zegara – pozwala zaprogramować zegar centrali. Dane wprowadzane są w formacie:

czas – godzina:minuta:sekunda,

data – dzień:miesiąc:rok.

Stan systemu – pozwala przejrzeć awarie, a jeżeli instalator włączył opcję GRADE 3, dodatkowo alarmy i zablokowane wejścia oraz sprawdzić stan stref.

Przegląd zdarzeń – w podmenu dostępne są funkcje umożliwiające przegląd zdarzeń zapisanych w pamięci centrali (patrz: „Przeglądanie zdarzeń” s. 32).

Reset czujek – uruchomienie funkcji spowoduje chwilowe wyłączenie wyjść typu 43. ZASILANIE Z RESETEM, co pozwala skasować pamięć alarmu czujek zasilanych z tych wyjść (np. czujek pożarowych).

Wyłączenie zatrzaśniętych wyjść – umożliwia wyłączenie niektórych wyjść centrali, dla których włączona jest opcja ZATRZASK, oraz wyjść typu 9. ALARM DAY, 12. CICHY ALARM i 116. SYGNALIZATOR WEWNĘTRZNY.

Koniec otwarcia pożarowego drzwi – przywraca normalny tryb pracy wszystkich modułów realizujących funkcje kontroli dostępu (w przypadku pożaru drzwi kontrolowane przez te moduły mogą być automatycznie odblokowywane).

Zmiana opcji – w podmenu dostępne są następujące funkcje:

Gong w manipulatorze – umożliwia włączenie lub wyłączenie sygnalizacji GONG w manipulatorze. Sygnalizacja GONG to pięć krótkich dźwięków, przy pomocy których manipulator informuje np. o otwarciu drzwi lub okna, gdy system nie czuwa. Instalator określa, które wejścia systemu alarmowego mogą wyzwoić sygnalizację GONG.

Gong wyjść – umożliwia zablokowanie sygnalizacji naruszeń wejść z wybranych stref na wyjściu typu 11. GONG.

Timery – pozwala programować parametry timerów sterujących wyjściami typu 120. TERMOSTAT i innych timerów, na których edycję zezwolił instalator.

Temperatury – umożliwia edycję progów temperatury i histerezy dla wyjść typu 120. TERMOSTAT.

Timery stref – pozwala zaprogramować timery stref (patrz: „Programowanie timera strefy” s. 33).

Blokowanie sabotaży ekspanderów – umożliwia tymczasowe wyłączenie kontroli sabotaży ekspanderów. W przypadku jakichkolwiek problemów z modułami rozszerzającymi, należy o tym poinformować serwis.

Stały dostęp serwisu – opcja dostępna dla administratora. Jeżeli jest włączona, serwis ma stały dostęp do systemu alarmowego, co m.in. pozwala programować centralę przy pomocy manipulatora LCD lub programu DLOADX.



Włączenie opcji STAŁY DOSTĘP SERWISU kasuje czas dostępu serwisu zaprogramowany przy pomocy funkcji DOSTĘP SERWISU. Z kolei zaprogramowanie czasu dostępu serwisu wyłączy opcję STAŁY DOSTĘP SERWISU.

Serwis edytuje – opcja dostępna dla administratora. Jej włączenie umożliwi serwisowi dodawanie, edycję i usuwanie użytkowników w partycji administratora.

Serwis załącza/wyłącza/kasuje/blokuje – opcja dostępna dla administratora. Jeżeli jest włączona, serwis może załączać i wyłączać czuwanie, kasować alarmy oraz blokować wejścia w partycji administratora.

Stały dostęp DLOADX – opcja dostępna dla administratora. Jeżeli jest włączona, możliwe jest programowanie centrali przy pomocy programu DLOADX niezależnie od tego, czy serwis ma dostęp do systemu alarmowego.

Adres DLOADX – pozwala zaprogramować adres komputera, na którym zainstalowany jest program DLOADX. Adres należy zaprogramować, jeżeli centrala ma inicjować komunikację z programem DLOADX przez sieć Ethernet z wykorzystaniem protokołów TCP/IP (patrz: opis funkcji ETHM-1 – DLOADX dostępnej w podmenu DOWNLOADING). Może zostać wprowadzony w formie nazwy lub adresu IP.

Adres GUARDX – pozwala zaprogramować adres komputera, na którym zainstalowany jest program GUARDX. Adres należy zaprogramować, jeżeli centrala ma inicjować komunikację z programem GUARDX przez sieć Ethernet z wykorzystaniem protokołów TCP/IP (patrz: opis funkcji ETHM-1 – GUARDX dostępnej w podmenu DOWNLOADING). Może zostać wprowadzony w formie nazwy lub adresu IP.

Skasowanie notatki – pozwala skasować notatkę serwisową.

Testy – w podmenu dostępne są następujące funkcje:

Stan stref – pozwala sprawdzić stan stref dostępnych dla użytkownika i obsługiwanych przez manipulator. Stan strefy jest prezentowany przy pomocy symbolu. Liczby umieszczone na szybcie umożliwiają identyfikację numerów stref. Fabrycznie stan stref przedstawiany jest przy pomocy następujących symboli (instalator może je zmienić):

- b - czasowa blokada strefy,
- ? - czas na wejście,
- W - czas na wyjście (mniejszy od 10 sekund),
- w - czas na wyjście (większy od 10 sekund),
- P - alarm pożarowy,
- A - alarm,
- p - pamięć alarmu pożarowego,
- a - pamięć alarmu,
- c - strefa czuwa,
- - naruszone wejścia,
- - strefa nie czuwa, wejścia OK.

Stan wejść – pozwala sprawdzić stan wejść w strefach dostępnych dla użytkownika i obsługiwanych przez manipulator. Stan wejścia jest prezentowany przy pomocy symbolu. Liczby umieszczone na szybcie umożliwiają identyfikację numerów wejść. Po uruchomieniu funkcji wyświetlany jest stan wejść 1-32. Klawisze ► i ◄ pozwalają wyświetlić stan innych wejść (patrz też opis diod LED ■ s. 7). Fabrycznie stan wejść przedstawiany jest przy pomocy następujących symboli (instalator może je zmienić):

- b - blokada wejścia,
- l - awaria "długie naruszenie",
- f - awaria "brak naruszenia",
- S - alarm sabotażowy,
- A - alarm,
- - sabotaż wejścia,
- M - maskowanie,
- - naruszenie wejścia,
- s - pamięć alarmu sabotażowego,
- m - pamięć maskowania,
- a - pamięć alarmu,
- - wejście OK.

Napięcia zasilania – dostępna dla serwisu. Pozwala sprawdzić napięcie zasilania poszczególnych ekspanderów.

Temperatury – umożliwia sprawdzenie temperatur mierzonych przez czujki bezprzewodowe ATD-100.

Urządzenia radiowe – pozwala sprawdzić poziom sygnału radiowego urządzeń bezprzewodowych systemu ABAX współpracujących z centralą.

Test wejść – w podmenu dostępne są funkcje umożliwiające przetestowanie czujek podłączonych do wejść (patrz: „Testowanie wejść” s. 34).

Test akumulatora – dostępna dla serwisu. Po jej uruchomieniu centrala wygeneruje zdarzenia informujące o stanie akumulatorów płyty głównej i ekspanderów przewodowych z zasilaczem. Dodatkowo analizowany jest stan wejść o reakcji 60. TECHNICZNA - AWARIA AKUMULATORA.

Ręczna transmisja testowa – generuje zdarzenie, które uruchamia procedurę przesłania komunikatu do stacji monitorującej (kod wysyłany z identyfikatorem systemowym).

Test stacji monitorującej (1A, 1B, 2A, 2B) – umożliwia wysłanie transmisji testowej do stacji monitorującej (osobne funkcje dla każdego z numerów telefonu). W trakcie wysyłania transmisji komunikaty na wyświetlaczu informują o aktualnie wykonywanej czynności. Funkcja przydatna podczas uruchamiania monitoringu lub w przypadku awarii monitorowania.

Test powiadamiania – pozwala przetestować powiadamianie. Po uruchomieniu funkcji należy:

1. Wpisać numer telefonu (numer porządkowy na liście telefonów).
2. Nacisnąć klawisz ▼.
3. Wpisać numer komunikatu głosowego.
4. Nacisnąć klawisz #. Centrala zadzwoni pod wskazany numer i odtworzy komunikat.

Test odbierania telefonu – po uruchomieniu funkcji, w trakcie odbierania połączenia telefonicznego wyświetlane są informacje o ilości dzwonek i o odebraniu połączenia telefonicznego.

Test karty – pozwala sprawdzić numer karty zbliżeniowej oraz ustalić, do kogo ona należy (o ile karta należy do użytkownika systemu).

Test CA-64 PTSA – pozwala przetestować tablicę synoptyczną.

Przegląd administratorów – dostępna dla administratora. Pozwala sprawdzić, w których partycjach są utworzeni administratorzy.

Nazwa manipulatora – umożliwia sprawdzenie nazwy danego manipulatora.

Plik w DLOADX – wyświetla datę i czas zapisania danych w centrali przy pomocy programu DLOADX oraz nazwę pliku z danymi centrali.

Wersja centrali – wyświetla informacje o wersji oprogramowania centrali.

Wersja programu STM – wyświetla informacje o wersji oprogramowania procesora obsługującego zasilacz i wejścia centrali.

IP/MAC ETHM-1 – wyświetla kolejno następujące informacje dotyczące modułu ethernetowego podłączonego do centrali:

- adres lokalny,
- numer MAC,
- adres publiczny,
- indywidualny numer identyfikacyjny na potrzeby komunikacji przez serwer SATEL [ID].

Przewijanie informacji umożliwiają klawisze ► i ◀. Jeżeli do centrali podłączonych jest kilka modułów ethernetowych, listę modułów można przewijać przy pomocy klawiszy ▼ i ▲.

Wersje modułów – pozwala sprawdzić wersje oprogramowania urządzeń podłączonych do magistral komunikacyjnych centrali.

Synchronizacja czasu – pozwala ręcznie uruchomić synchronizację zegara centrali z serwerem czasu. Dotyczy centrali, do której podłączony jest moduł ETHM-1 / ETHM-1 Plus. W centrali musi być zaprogramowany adres serwera synchronizacji czasu.



Funkcja jest niedostępna, jeżeli trwa synchronizacja czasu. Automatyczna synchronizacja czasu odbywa się codziennie o 05:30 i po restarcie centrali.

Dostęp serwisu – dostępna dla administratora. Umożliwia określenie czasu dostępu serwisu do systemu alarmowego. Czas programuje się w godzinach. Zaprogramowanie wartości 0 oznacza wyłączenie dostępu serwisu.

Otwórz drzwi – umożliwia otwarcie drzwi kontrolowanych przez system alarmowy (moduły realizujące funkcje kontroli dostępu) lub włączenie wyjść typu 101. Wczytanie karty w module.

Sterowanie – umożliwia sterowanie urządzeniami podłączonymi do wyjść typu PRZELĄCZNIK MONO, PRZELĄCZNIK BI, PRZEKAŹNIK TELEFONICZNY, ROLETA W GÓRĘ i ROLETA W DÓŁ (patrz: „Sterowanie” s. 35).

Tryb serwisowy – dostępna dla serwisu. Uruchamia tryb serwisowy.

Przejęcie TS – dostępna dla serwisu. Jeżeli tryb serwisowy uruchomiony został przy pomocy innego manipulatora, można go przejąć, tzn. wyświetlić menu serwisowe w manipulatorze, na którym uruchomiona została funkcja PRZEJĘCIE TS.

Downloading – w podmenu dostępne są następujące funkcje:

Start DWNL-RS – dostępna dla serwisu. Umożliwia programowanie lokalne centrali przy pomocy programu DLOADX.

Koniec DWNL-RS – dostępna dla serwisu. Kończy programowanie lokalne centrali.

Start DWNL-MOD. – umożliwia programowanie zdalne przez modem zewnętrzny (analogowy, GSM lub ISDN) przy pomocy programu DLOADX.

Start DWNL-TEL – umożliwia programowanie zdalne przez wbudowany modem 300 bps przy pomocy programu DLOADX.

ETHM-1 – DLOADX – umożliwia programowanie zdalne przez sieć Ethernet (TCP/IP) przy pomocy programu DLOADX. Do centrali musi być podłączony moduł ETHM-1 (wersja oprogramowania 1.03 lub nowsza) / ETHM-1 Plus.

ETHM-1 – GUARDX – umożliwia zdalną obsługę i administrowanie przez sieć Ethernet (TCP/IP) przy pomocy programu GUARDX. Do centrali musi być podłączony moduł ETHM-1 (wersja oprogramowania 1.03 lub nowsza) / ETHM-1 Plus.

5.4 Załączenie czuwania

W rozdziale opisane zostały operacje, które wykonać musi użytkownik przy pomocy manipulatora, aby rozpocząć procedurę załączenia czuwania. Procedura załączenia czuwania kończy się równocześnie z końcem czasu na wyjście (jeśli kończy się powodzeniem, zostaje załączone czuwanie – patrz też „Niepowodzenie procedury załączania czuwania” s. 24). Jeżeli czas na wyjście jest równy 0, czuwanie zostanie załączone natychmiast.



Instalator może tak skonfigurować system alarmowy, że funkcje służące do załączenia czuwania będą niedostępne po sabotażu. Komunikat na wyświetlaczu będzie informował, że należy wezwać serwis. Dopiero po wpisaniu hasła serwisowego i zatwierdzeniu klawiszem #, funkcje służące do załączenia czuwania będą znowu dostępne.

5.4.1 Załączenie pełnego czuwania bez wybierania stref

Załączenie czuwania bez wyboru stref jest możliwe, gdy żadna ze stref, do których użytkownik ma dostęp, nie czuwa i manipulator nie sygnalizuje alarmu.

1. Wpisać hasło i zatwierdzić klawiszem #.
2. Gdy zostanie wyświetlona funkcja ZAŁĄCZ WSZYSTKO, nacisnąć klawisz #. We wszystkich strefach, do których użytkownik ma dostęp i które obsługiwane są przez manipulator, rozpocznie się procedura załączenia czuwania.



Jeżeli użytkownik może załączyć czuwanie tylko w jednej strefie, już po wprowadzeniu hasła i zatwierdzeniu klawiszem # rozpocznie się procedura załączenia czuwania.

5.4.2 Załączenie pełnego czuwania w wybranych strefach

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Przy pomocy klawisza ▼ przewijać menu aż znaleziona zostanie funkcja ZAŁĄCZ CZUWANIE.
3. Nacisnąć klawisz #. Zostanie wyświetlona lista stref, w których można załączyć czuwanie.
4. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście strefę, w której ma zostać załączone czuwanie (albo nacisnąć klawisz 0 i wprowadzić numer strefy).
5. Nacisnąć jeden z klawiszy z cyframi od 1 do 9. Symbol * w prawym górnym rogu zostanie zastąpiony symbolem  (patrz też „Wybór z listy wielokrotnego wyboru” s. 15).
6. Czynności z punktów 4 i 5 powtórzyć dla kolejnych stref, w których ma zostać załączone czuwanie.
7. Po wybraniu stref, w których ma zostać załączone czuwanie, nacisnąć klawisz #.

Czuwanie w wybranych strefach można też załączyć przy pomocy funkcji ZAŁĄCZ WYBRANE, dostępnej po wpisaniu hasła i zatwierdzeniu klawiszem #, jednak tylko wówczas, gdy żadna ze stref, do których użytkownik ma dostęp, nie czuwa i manipulator nie sygnalizuje alarmu.

5.4.3 Załączenie wybranego typu czuwania

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Przy pomocy klawisza ▼ przewijać menu aż znaleziona zostanie funkcja TRYB ZAŁĄCZENIA.
3. Nacisnąć klawisz #. Zostanie wyświetlona lista typów czuwania (patrz: opis funkcji TRYB ZAŁĄCZENIA s. 17).
4. Przy pomocy klawiszy ▲ i ▼ znaleźć typ czuwania, który ma zostać załączony, a następnie nacisnąć klawisz #.
5. Gdy zostanie wyświetlona funkcja ZAŁĄCZ CZUWANIE, nacisnąć klawisz #. Postępować analogicznie, jak w przypadku załączania pełnego czuwania w wybranych strefach (punkty 4-7).

5.4.4 Szybkie załączenie czuwania

Instalator może zezwolić na załączanie czuwania bez autoryzacji użytkownika. Czuwanie jest załączane w strefach wskazanych przez instalatora.

1. Wybrać typ czuwania, który ma zostać załączony (nacisnąć jeden z klawiszy: 0 – pełne czuwanie; 1 – pełne czuwanie + blokady; 2 – czuwanie bez wewnętrznych; 3 – czuwanie bez wewnętrznych i bez czasu na wejście).
2. Nacisnąć klawisz #. Rozpocznie się procedura załączania czuwania.

5.4.5 Odmowa załączenia czuwania

Instalator może zaprogramować centralę w taki sposób, że nie uda się rozpocząć procedury załączenia czuwania, jeśli:

- w strefie naruszone jest wejście,
- w systemie jest awaria (w tym sabotaż),
- miał miejsce alarm zweryfikowany.

Manipulator poinformuje o odmowie załączenia czuwania przy pomocy komunikatu precyzującego przyczynę odmowy.



Jeżeli po alarmie zweryfikowanym załączenie czuwania jest niemożliwe, należy wezwać serwis. Dopiero po interwencji serwisu możliwe będzie załączenie czuwania (patrz: opis funkcji PRZYWRÓĆ SYSTEM s. 17).

Blokowanie naruszonych wejść przy załączaniu czuwania

Jeżeli nie udało się załączyć czuwania, a komunikat na wyświetlaczu informuje, że są naruszone wejścia, można przejrzeć listę tych wejść po naciśnięciu klawisza 2. Listę można przewijać przy pomocy klawiszy ▼ i ▲. Po naciśnięciu klawisza 4 dane wejście można zablokować. Komunikat na wyświetlaczu poprosi o naciśnięcie klawisza 1 w celu potwierdzenia, że wejście ma zostać zablokowane.

Wymuszone załączenie czuwania

Jeśli nie udało się załączyć czuwania, komunikat na wyświetlaczu może dopuszczać wymuszenie załączenia czuwania (1=Zał.). Po naciśnięciu klawisza 1, czuwanie zostanie załączone pomimo naruszonego wejścia lub awarii.

5.4.6 Niepowodzenie procedury załączania czuwania

Jeżeli instalator włączył opcję globalną GRADE 3, procedura załączania czuwania może się zakończyć niepowodzeniem. Czuwanie nie zostanie załączone, jeśli w chwili zakończenia odliczania czasu na wyjście:

- w strefie jest naruszone wejście, które nie było naruszone, gdy rozpoczęta została procedura załączenia czuwania,
- ma miejsce awaria, której nie było, gdy rozpoczęta została procedura załączenia czuwania.

5.4.7 Skrócenie czasu na wyjście

Jeżeli instalator dopuścił taką możliwość, czas na wyjście ze strefy może zostać skrócony po naciśnięciu kolejno klawiszy 9 i #. Czas na wyjście można skrócić używając tego samego manipulatora, przy pomocy którego załączone zostało czuwanie.

5.5 Wyłączenie czuwania i kasowanie alarmu

Wpisać hasło i zatwierdzić klawiszem # (patrz: „[Hasło]# – menu załączenia / wyłączenia czuwania” s. 9). Jeżeli czuwanie ma zostać wyłączone tylko w wybranych strefach (funkcja WYŁĄCZ WYBRANE), wyboru stref dokonuje się w analogiczny sposób, jak w przypadku załączania czuwania w wybranych strefach.

5.5.1 Kasowanie alarmu bez wyłączenia czuwania

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Przy pomocy klawisza ▼ przewijać menu aż znaleziona zostanie funkcja KASUJ ALARM.
3. Nacisnąć klawisz #.

5.6 Załączanie / wyłączenie czuwania na 2 hasła

Jeżeli czuwanie w strefie jest załączane / wyłączane na 2 hasła, użytkownik wprowadzający pierwsze hasło powinien:

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Przy pomocy klawisza ▼ przewijać menu aż znaleziona zostanie funkcja ZAŁ. NA 2 HASŁA / WYŁ. NA 2 HASŁA.
3. Nacisnąć klawisz #. Postępować analogicznie, jak w przypadku załączania pełnego czuwania w wybranych strefach (punkty 3-7).

4. Jeżeli instalator nie ustalił czasu ważności hasła na 30 sekund, podać czas ważności hasła i zatwierdzić klawiszem #.

Przed upływem czasu ważności hasła, użytkownik wprowadzający drugie hasło powinien załączyć / wyłączyć czuwanie przy pomocy:

- manipulatora (patrz: „Załączenie czuwania” lub „Wyłączenie czuwania i kasowanie alarmu”),
- klawiatury strefowej ([hasło]#),
- czytnika (wczytanie karty zbliżeniowej lub pastylki DALLAS).



Instalator może tak skonfigurować system alarmowy, że drugie hasło musi zostać wpisane na innym manipulatorze, klawiaturze strefowej itd.

5.7 Wywołanie alarmu z manipulatora

Instalator może zezwolić na wywoływanie alarmów z manipulatora. W celu wywołania alarmu należy:

alarm pożarowy – nacisnąć na około 3 sekundy klawisz 🔥,

alarm medyczny (pomocniczy) – nacisnąć na około 3 sekundy klawisz ⚠,

alarm napadowy – nacisnąć na około 3 sekundy klawisz 🛡. Instalator określa, czy wywołany zostanie alarm napadowy głośny (uruchamiający głośną sygnalizację alarmu) czy cichy (bez głośnej sygnalizacji).

5.8 Użytkownicy

Dodawanie, edytowanie i usuwanie użytkowników mogą:

- administrator,
- serwis (jeżeli administrator włączył opcję SERWIS EDYTUJE),
- użytkownik (jeżeli posiada uprawnienie EDYCJA UŻYTKOWNIKÓW).

Dla użytkownika można zdefiniować:

Hasło – ciąg cyfr służący do autoryzacji użytkownika podczas korzystania z manipulatorów, klawiatur strefowych i zamków szyfrowych. Centrala obsługuje hasła liczące od 4 do 8 znaków, jednak instalator może określić, jaka powinna być minimalna długość hasła.

Hasło telefoniczne – ciąg cyfr służący do autoryzacji użytkownika podczas korzystania z funkcji odpowiadania na telefon i sterowania telefonicznego (patrz: „Odpowiadanie na telefon i sterowanie telefoniczne” s. 43).

Strefy – strefy, do których użytkownik ma dostęp (tzn. może w nich załączać i wyłączać czuwanie, kasować alarm itd.).

Typ – patrz: „Typy użytkowników” s. 27.

Schemat użytkownika – parametr dla hasła typu SCHEMATOWY (patrz: „Typy użytkowników” s. 27).

Czas istnienia – parametr dla haseł typu NA CZAS – ODNAWIALNY, NA CZAS – NIEODNAWIALNY lub SCHEMATOWY (patrz: „Typy użytkowników” s. 27).

Czas blokady – parametr programowany dla hasła typu WŁĄCZA BLOKADĘ CZASOWĄ STREF (patrz: „Typy użytkowników” s. 27).

Uprawnienia – określają, z jakich funkcji może korzystać użytkownik. Dostępne są następujące uprawnienia:

- Załączanie czuwania
- Wyłączanie czuwania

- Wyłącza, gdy kto inny załączył [Wył.za innego] – jeżeli użytkownik nie posiada tego uprawnienia, może wyłączyć czuwanie tylko, jeśli je załączył
- Kasowanie alarmu strefy [Kas.al.strefy]
- Kasowanie alarmu partycji [Kas.al.part]
- Kasowanie alarmu innych partycji [Kas.al.innych]
- Kasowanie powiadamiania telefonicznego [Kas. pow. tel.]
- Odraczanie auto-uzbrojenia [Odrocz.zał.cz.]
- Hasło pierwsze dla strefy na 2 hasła [Pod.pier.hasła]
- Hasło drugie dla strefy na 2 hasła [Pod.drug.hasła]
- Dostęp do stref zablokowanych czasowo [Dost.str.blok.]
- Zmiana hasła
- Edycja użytkowników
- Blokowanie wejść
- Trwałe blokowanie wejść [Blok. trwałe]
- Programowanie czasu [Prog. zegara]
- Sprawdzanie aktualnych awarii
- Przeglądanie zdarzeń
- Resetowanie czujek
- Zmiana opcji
- Dostęp do testów [Testy]
- Uruchamianie funkcji DOWNLOAD [Downloading]
- Sterowanie wyjściami
- Przegląd stanu systemu w programie GUARDX [Obsługa GUARDX]
- Wyłączanie zatrzaśniętych wyjść [Wył.zatrz.wyj.]
- Użytkownik prosty – po wpisaniu hasła i zatwierdzeniu klawiszem # użytkownik nigdy nie wybiera stref, w których chce załączyć / wyłączyć czuwanie. Czuwanie jest od razu załączane / wyłączane we wszystkich strefach, do których ma dostęp.
- Administrator – użytkownik ma dostęp w menu do funkcji zastrzeżonych dla administratora

Klawiatury itd. – moduły dodatkowe, z których użytkownik będzie mógł obsługiwać system (moduły sterowania strefami, klawiatury strefowe, zamki szyfrowe, ekspanderów czytników).

Karty zbliżeniowe / pastylki DALLAS – jeśli w systemie pracuje czytnik kart zbliżeniowych / pastylek DALLAS, użytkownikowi można przypisać kartę zbliżeniową / pastylkę DALLAS, która umożliwi obsługę systemu przy pomocy czytników.

Piloty – w przypadku centrali, do której podłączony jest moduł obsługujący piloty (ACU-120, ACU-270, ACU-100, ACU-250, INT-RX lub INT-RX-S), użytkownikowi może zostać przydzielony pilot, który umożliwi obsługę systemu. Użytkownik może posiadać maksymalnie 2 piloty: pilot APT-100 (obsługiwany przez system ABAX) i pilot 433 MHz (obsługiwany przez moduły INT-RX lub INT-RX-S).

Przyciski – funkcje dotyczące przycisków są dostępne, jeżeli użytkownikowi przypisany został pilot. Do przycisków lub kombinacji przycisków pilota można przypisać wejście, które zostanie naruszone po naciśnięciu przycisku / kombinacji przycisków. Przypisane wejście nie powinno istnieć fizycznie.



Do przycisków / kombinacji przycisków nie można przypisać wejścia 256.

Zdarzenia RX / Zdarzenia ABAX – jeżeli użytkownikowi przydzielony został pilot, można określić, czy naciśnięcie odpowiedniego przycisku pilota będzie skutkowało zapisaniem zdarzenia informującego o użyciu pilota.

Potwierdzanie ABAX – jeżeli użytkownikowi przydzielony został pilot systemu ABAX, można określić, stan których wyjść prezentowany będzie na diodach LED w pilocie po naciśnięciu dowolnego przycisku.

Nazwa – indywidualna nazwa użytkownika.

5.8.1 Typy użytkowników

W nawiasie kwadratowym podana jest nazwa prezentowana w manipulatorze. W opisie uwzględnione zostały jedynie hasła, ale podane informacje dotyczą wszystkich identyfikatorów przydzielonych użytkownikowi.

Normalny – podstawowy typ użytkownika.

Jednorazowy – użytkownik uzyska jednorazowy dostęp.

Na czas – odnawialny [Czasowy odnaw.] – użytkownik ma dostęp do systemu przez określony czas. Czas ważności użytkownika należy zdefiniować. Przed upłynięciem czasu ważności centrala przypomina użytkownikowi o konieczności zmiany hasła. Po zmianie hasła czas ważności będzie liczony od nowa.

Na czas – nieodnawialny [Czasowy nieodn.] – użytkownik ma dostęp do systemu przez określony czas. Czas ważności użytkownika należy zdefiniować. Po upływie czasu ważności użytkownik nie będzie miał dostępu do systemu.

Przymus – hasło przeznaczone do stosowania w przypadku napadu i działania pod przymusem. Jego użycie wywoła cichy alarm i spowoduje wysłanie kodu zdarzenia do stacji monitorującej.

Steruje wyjściami „mono” stref [Wyjścia monost.] – hasło przeznaczone do sterowania wyjściami typu PRZELĄCZNIK MONO.

Steruje wyjściami „bi” stref [Wyjścia bistab.] – hasło przeznaczone do sterowania wyjściami typu PRZELĄCZNIK BI.

Włącza blokadę czasową stref [Czas.blok.stref] – hasło umożliwia dostęp do stref, które czuwają. Użycie hasła blokuje czuwającą strefę/strefy (wejścia w strefie nie wywołają alarmu włamania). Czas blokady definiuje się indywidualnie dla każdego użytkownika w zakresie od 1 do 109 minut. Jeżeli jednak dla strefy zdefiniowany jest czas blokady na obchód wartownika i jest on dłuższy, blokada będzie trwała dłużej.

Odblokowuje dostęp do bankomatu [Dostęp do bank.] – hasło przeznaczone do odblokowania dostępu do bankomatu (w strefie zostaną zablokowane czasowo wejścia o typie reakcji 24H BANKOMATOWE).

Wartownik – posłużenie się hasłem oznacza dokonanie obchodu (dodatkowo może spowodować czasową blokadę strefy na czas obchodu wartownika). Instalator wyznacza moduły, które wykorzystywane są do potwierdzania wykonania obchodu oraz określa czas między kolejnymi obchodami. Przydzielenie takiemu użytkownikowi dostępu do stref daje mu takie same możliwości, jak użytkownikowi typu NORMALNY.

Schematowy – użytkownik ma dostęp do systemu według schematu czasowego przez określony czas. Należy wybrać schemat czasowy (schemat czasowy programuje instalator) i określić czas ważności użytkownika.

5.8.2 Dodanie nowego użytkownika

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Naciśnąć kolejno klawisze 2 i 1. Zostanie wyświetlona lista funkcji służących do definiowania parametrów użytkownika.



Jeżeli wpisane zostało hasło serwisowe, zanim wyświetlona zostanie lista funkcji wymagane jest określenie, w której partycji ma zostać utworzony nowy użytkownik (hasło serwisowe umożliwia dostęp do wszystkich partycji).

3. Przy pomocy odpowiednich funkcji zdefiniować parametry użytkownika.



Użytkownikowi musi zostać przydzielony co najmniej jeden identyfikator: hasło, karta zbliżeniowa, pastylka DALLAS lub pilot.

Nowy użytkownik nie może otrzymać większych uprawnień niż posiada osoba, która dodaje go do systemu.

4. Nacisnąć klawisz *.

5. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.

6. Komunikat poinformuje o utworzeniu nowego użytkownika. Nacisnąć klawisz *, aby wrócić do podmenu UŻYTKOWNICY.

5.8.3 Edycja użytkownika



Użytkownik może edytować tych użytkowników, wobec których jest nadrzędny. Przykładowo, jeżeli użytkownik A utworzył użytkownika B, a użytkownik B utworzył użytkownika C, to użytkownik A może edytować użytkowników B i C.

Edytowany użytkownik nie może otrzymać większych uprawnień niż posiada osoba, która go edytuje.

1. Wpisać hasło i zatwierdzić klawiszem *.

2. Dwukrotnie nacisnąć klawisz 2. Zostanie wyświetlona lista użytkowników.

3. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście użytkownika, który ma być edytowany.

4. Nacisnąć klawisz #. Zostanie wyświetlona lista funkcji służących do definiowania parametrów użytkownika.

5. Przy pomocy odpowiednich funkcji zmodyfikować parametry użytkownika.

6. Nacisnąć klawisz *.

7. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.

8. Komunikat poinformuje o zmodyfikowaniu użytkownika. Nacisnąć klawisz *, aby wrócić do listy użytkowników.

5.8.4 Usunięcie użytkownika



Użytkownik może kasować użytkowników, wobec których jest nadrzędny. Przykładowo, jeżeli użytkownik A utworzył użytkownika B, a użytkownik B utworzył użytkownika C, to użytkownik A może usunąć użytkowników B i C.

1. Wpisać hasło i zatwierdzić klawiszem *.

2. Nacisnąć kolejno klawisze 2 i 3. Zostanie wyświetlona lista użytkowników.

3. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście użytkownika, który ma zostać usunięty.

4. Nacisnąć klawisz #. Komunikat poinformuje o usunięciu użytkownika.

5. Nacisnąć klawisz *, aby wrócić do listy użytkowników.

5.8.5 Dodanie karty zbliżeniowej / pastylki DALLAS

1. W trakcie dodawania lub edycji użytkownika uruchomić funkcję NOWA KARTA / NOWA PASTYLKA.

2. Przy pomocy klawiszy ▼ i ▲ wybrać sposób dodania karty / pastylki. Numer karty / pastylki może zostać odczytany przez wybrany czytnik (urządzenie posiadające czytnik) lub wpisany ręcznie.
3. Nacisnąć klawisz #.
4. Jeżeli numer karty / pastylki ma zostać odczytany, zgodnie z poleceniami pojawiającymi się na wyświetlaczu manipulatora dwukrotnie wczytać kartę / pastylkę. Kiedy wyświetlony zostanie odczytany numer karty / pastylki, nacisnąć klawisz #.
5. Jeżeli numer karty / pastylki ma zostać wpisany, wpisać go przy pomocy klawiatury, a następnie nacisnąć klawisz #.
6. Nastąpi powrót do listy funkcji służących do definiowania parametrów użytkownika. Zamiast funkcji NOWA KARTA / NOWA PASTYLKA dostępna będzie funkcja USUŃ KARTĘ / USUŃ PASTYLKĘ. Nacisnąć klawisz *.
7. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.



Analogicznie dodaje się kartę zbliżeniową / pastylkę DALLAS administratorom.

5.8.6 Dodanie pilota

1. W trakcie dodawania lub edycji użytkownika uruchomić funkcję NOWY PILOT RX / NOWY PILOT ABAX (zależnie od tego, jaki pilot ma zostać dodany).
2. Przy pomocy klawiszy ▼ i ▲ wybrać sposób dodania pilota. Numer pilota może zostać odczytany w czasie transmisji przez urządzenie obsługujące piloty lub wpisany ręcznie.
3. Nacisnąć klawisz #.
4. Jeżeli numer pilota ma zostać odczytany, zgodnie z poleceniami pojawiającymi się na wyświetlaczu manipulatora dwukrotnie nacisnąć przycisk w pilocie. Kiedy wyświetlony zostanie numer pilota, nacisnąć klawisz #.
5. Jeżeli numer pilota ma zostać wpisany, wpisać go przy pomocy klawiatury, a następnie nacisnąć klawisz #.
6. Nastąpi powrót do listy funkcji służących do definiowania parametrów użytkownika. Zamiast funkcji NOWY PILOT RX / NOWY PILOT ABAX dostępna będzie funkcja USUŃ PILOTA RX / USUŃ PILOT.ABAX. Pojawia się ponadto funkcje umożliwiające konfigurację pilota.



Przed przypisaniem wejść do przycisków / kombinacji przycisków należy skonsultować się z instalatorem.

Numeracja przycisków i diod LED w pilotach przedstawiona została w rozdziale „Obsługa systemu alarmowego przy pomocy pilota” (s. 45).

7. Przy pomocy klawisza ▼ znaleźć na liście funkcję PRZYCISK 1, a następnie nacisnąć klawisz #.
8. Przy pomocy klawiszy ▼ i ▲ wybrać, które wejście ma zostać naruszone po naciśnięciu przycisku 1 w pilocie (można też wpisać numer wejścia z klawiatury), a następnie nacisnąć klawisz #.
9. Czynności z punktów 7 i 8 powtórzyć dla innych przycisków / kombinacji przycisków, które mają być używane.
10. Przy pomocy klawisza ▼ znaleźć na liście funkcję ZDARZENIA RX / ZDARZENIA ABAX.
11. Nacisnąć klawisz #. Wyświetlona zostanie lista przycisków / kombinacji przycisków. W górnym prawym rogu wyświetlacza znajduje się dodatkowy symbol:
 - naciśnięcie przycisku / kombinacji przycisków jest zapisywane w pamięci zdarzeń (ustawienie domyślne),
 - – naciśnięcie przycisku / kombinacji przycisków nie jest zapisywane w pamięci zdarzeń.

12. Określić, czy naciśnięcie przycisku / kombinacji przycisków będzie zapisywane w pamięci zdarzeń (patrz: „Wybór z listy wielokrotnego wyboru” s. 15), a następnie nacisnąć klawisz #.
 13. W przypadku pilotów APT-100 (ABAX), przy pomocy klawisza ▼ znaleźć na liście funkcję POTWIERDZ. ABAX, a następnie nacisnąć klawisz #.
 14. Wyświetlona zostanie lista wyjść, które instalator przeznaczył do potwierdzania (maksymalnie 8). Należy wybrać maksymalnie 3 z nich (patrz: „Wybór z listy wielokrotnego wyboru” s. 15). Po naciśnięciu dowolnego przycisku pilota, na diodach LED pilota przez kilka sekund prezentowana będzie informacja o stanie wybranych wyjść. Pozwala to uzyskać potwierdzenie wykonania funkcji lub informację o aktualnym stanie systemu.
- i** Instalator może zdefiniować listę wyjść przy pomocy manipulatora (funkcja ABAX-POTWIERDZ. [TRYB SERWISOWY ► STRUKTURA ► SPRZĘT ► EKSPANDERY ► ABAX-POTWIERDZ.]) lub komputera z programem DLOADX (okno „Piloty ABAX”).
15. Nacisnąć klawisz #.
 16. Nacisnąć klawisz *.
 17. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.

i Analogicznie dodaje się piloty administratorom.

5.8.7 Usunięcie pilota

1. W trakcie dodawania lub edycji użytkownika uruchomić funkcję USUŃ PILOTA RX / USUŃ PILOT.ABAX (zależnie od tego, jaki pilot ma zostać usunięty). Odpowiednia funkcja jest wyświetlana tylko, gdy użytkownikowi został wcześniej przydzielony pilot.
2. Gdy wyświetli się numer pilota i pytanie, czy go usunąć, nacisnąć klawisz 1. Nastąpi powrót do listy funkcji służących do definiowania parametrów użytkownika.
3. Nacisnąć klawisz *.
4. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.

i Usunięcie pilota nie kasuje jego ustawień (zależności między przyciskami a wejściami, zasad potwierdzania itd.). Po dodaniu użytkownikowi nowego pilota, będzie on miał takie same ustawienia, jak usunięty pilot.

Instalator może usunąć wszystkie piloty łącznie z ich ustawieniami przy pomocy funkcji dostępnych w trybie serwisowym (► STRUKTURA ► SPRZĘT ► EKSPANDERY ► USUŃ PILOTY RX / USUŃ PILOT.ABAX).

Analogicznie usuwa się piloty administratorom.

5.9 Administratorzy

Dodawanie, edytowanie i usuwanie administratorów może serwis. W każdej partycji może być 1 administrator. Administrator ma dostęp do wszystkich stref swojej partycji, a także decyduje o dostępie do systemu hasła serwisowego. Dla administratora można zdefiniować większość parametrów, które definiowane są dla zwykłego użytkownika (patrz: „Użytkownicy” s. 25).

5.10 Blokowanie wejść

Jeśli wejście nie ma wywoływać alarmu, można je zablokować, gdy strefa, do której wejście należy, nie czuwa. Blokowanie wejść jest przydatne np. gdy ma pozostać otwarte okno

w czasie czuwania lub gdy czujka podłączona do wejścia jest uszkodzona i wywołuje niepotrzebne alarmy.



Blokowanie wejść obniża poziom ochrony. Zablokowane wejście może pozwolić intruzowi na wdarcie się do chronionego obszaru pomimo załączenia czuwania.

W przypadku blokowania wejścia z powodu uszkodzenia czujki, należy natychmiast wezwać serwis w celu usunięcia usterki.

Ze względów bezpieczeństwa instalator może ograniczyć liczbę wejść, które użytkownik będzie mógł blokować.

5.10.1 Czasowe blokowanie wejść

Wejścia mogą być blokowane czasowo przez użytkowników posiadających uprawnienie BLOKOWANIE WEJŚĆ. Wejście zablokowane czasowo pozostanie zablokowane do momentu wyłączenia czuwania w strefie, do której należy, albo do chwili odblokowania przez użytkownika.

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Nacisnąć kolejno klawisze 4 i 1. Zostanie wyświetlona lista wejść. W górnym prawym rogu wyświetlacza znajduje się dodatkowy symbol informujący o statusie danego wejścia:
 - – wejście nie jest zablokowane,
 - wejście jest zablokowane czasowo,
 - wejście jest zablokowane trwale.
3. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście wejście, które ma zostać czasowo zablokowane (albo nacisnąć klawisz 0 i wprowadzić numer wejścia).
4. Naciskać jeden z klawiszy z cyframi od 1 do 9, aż w górnym prawym rogu wyświetlacza pojawi się symbol .
5. Czynności z punktów 3 i 4 powtórzyć dla kolejnych wejść, które mają zostać zablokowane czasowo.
6. Nacisnąć klawisz #. Komunikat poinformuje o zablokowaniu wejść.



Po uruchomieniu funkcji BLOKADY CZASOWE (punkt 2), można nacisnąć klawisz ► lub ◀, aby przełączyć manipulator w graficzny tryb programowania (patrz: „Wybór z listy wielokrotnego wyboru” s. 15).

5.10.2 Trwale blokowanie wejść

Wejścia mogą być blokowane trwale przez użytkowników posiadających uprawnienia BLOKOWANIE WEJŚĆ i TRWAŁE BLOKOWANIE WEJŚĆ. Wejście zablokowane trwale pozostanie zablokowane do chwili odblokowania przez użytkownika.

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Nacisnąć kolejno klawisze 4 i 2. Zostanie wyświetlona lista wejść. W górnym prawym rogu wyświetlacza znajduje się dodatkowy symbol informujący o statusie danego wejścia:
 - – wejście nie jest zablokowane,
 - wejście jest zablokowane czasowo,
 - wejście jest zablokowane trwale.
3. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście wejście, które ma zostać trwale zablokowane (albo nacisnąć klawisz 0 i wprowadzić numer wejścia).
4. Naciskać jeden z klawiszy z cyframi od 1 do 9, aż w górnym prawym rogu wyświetlacza pojawi się symbol .

5. Czynności z punktów 3 i 4 powtórzyć dla kolejnych wejść, które mają zostać zablokowane trwale.
6. Nacisnąć klawisz **#**. Komunikat poinformuje o zablokowaniu wejść.



Po uruchomieniu funkcji BLOKADY TRWAŁE (punkt 2), można nacisnąć klawisz ► lub ◀, aby przełączyć manipulator w graficzny tryb programowania (patrz: „Wybór z listy wielokrotnego wyboru” s. 15).

5.10.3 Odblokowanie wejść

Wejścia mogą odblokować użytkownicy posiadający uprawnienie BLOKOWANIE WEJŚĆ. Należy postępować analogicznie, jak w przypadku czasowego lub trwałego blokowania wejść (punkty 1-3), ale w górnym prawym rogu wyświetlacza musi być wyświetlany symbol *****, jeśli wejście ma zostać odblokowane po naciśnięciu klawisza **#**.

5.11 Przeglądanie zdarzeń



Funkcja przeglądu zdarzeń uruchomiona przez administratora lub zwykłego użytkownika nie informuje o:

- alarmach napadowych,
- alarmach wywołanych użyciem hasła typu PRZYMUS.

5.11.1 Przegląd wszystkich zdarzeń

1. Wpisać hasło i zatwierdzić klawiszem *****.
2. Nacisnąć kolejno klawisze 5 i 2. Zostanie wyświetlone ostatnie zdarzenie, które miało miejsce w systemie.
3. Przy pomocy klawisza **▲** przewijać listę wcześniejszych zdarzeń.

5.11.2 Przegląd zdarzeń wymaganych dla Grade 3

Jeżeli w systemie włączona jest opcja globalna GRADE 3, dostępna jest funkcja umożliwiająca serwisowi i administratorom przegląd zdarzeń wymaganych przez normę EN 50131 dla Grade 3.

1. Wpisać hasło i zatwierdzić klawiszem *****.
2. Nacisnąć klawisz 5. Zostaną wyświetlone funkcje dostępne w podmenu PRZEGL. ZDARZEŃ.
3. Przy pomocy klawisza **▼** przewijać menu aż znaleziona zostanie funkcja ZDARZ. GRADE3.
4. Nacisnąć klawisz **#**. Zostanie wyświetlone ostatnie zdarzenie wymagane dla Grade 3, które miało miejsce w systemie.
5. Przy pomocy klawisza **▲** przewijać listę wcześniejszych zdarzeń.

5.11.3 Przegląd wybranych zdarzeń

1. Wpisać hasło i zatwierdzić klawiszem *****.
2. Nacisnąć kolejno klawisze 5 i 1.
3. Gdy zostanie wyświetlona funkcja WYBÓR ZDARZEŃ, nacisnąć klawisz **#**. Zostanie wyświetlona lista typów zdarzeń.
4. Wybrać, które typy zdarzeń mają zostać wyświetlone (patrz: „Wybór z listy wielokrotnego wyboru” s. 15).
5. Nacisnąć klawisz **#**. Nastąpi powrót do podmenu WYBRANE.
6. Przy pomocy klawisza **▼** przewijać menu aż znaleziona zostanie funkcja PRZEGLĄD.

7. Nacisnąć klawisz **#**. Zostanie wyświetlone ostatnie z wybranych zdarzeń, które miało miejsce w systemie.
8. Przy pomocy klawisza **▲** przewijać listę wcześniejszych zdarzeń.



Oprócz określenia, jakie typy zdarzeń mają zostać wyświetlone, przy pomocy funkcji WYBÓR STREF można dodatkowo wskazać strefy, których mają dotyczyć zdarzenia.

Jeżeli w systemie włączona jest opcja globalna GRADE 3, serwis lub administrator mogą zamiast funkcji PRZEGLĄD użyć funkcji PRZEGLĄD GRADE3. Zostaną wówczas wyświetlone wybrane zdarzenia spośród wymaganych przez normę EN 50131 dla Grade 3.

5.11.4 Sposób prezentowania zdarzeń

W górnej linii wyświetlane są:

- data i czas wystąpienia zdarzenia,
- dodatkowe informacje na temat zdarzenia w formie skróconej np. numer strefy, wejścia, użytkownika, timera, ekspandera, manipulatora itp.

W dolnej linii wyświetlany jest opis zdarzenia.

Jeśli przez parę sekund nie zostanie naciśnięty żaden klawisz, wyświetlone zostaną dodatkowe informacje na temat zdarzenia np. nazwa strefy, wejścia, użytkownika, timera, ekspandera, manipulatora itp. Po paru sekundach ponownie wyświetlony zostanie opis zdarzenia itd.

Naciśnięcie klawisza **►** umożliwia ręczne przełączanie między opisem zdarzenia a dodatkowymi informacjami na jego temat.

Naciśnięcie klawisza **◄**, gdy wyświetlany jest opis zdarzenia, pozwala zobaczyć kolejne dodatkowe informacje na temat zdarzenia podawane w formie skróconej.

Użycie klawisza **◄** lub **►** blokuje automatyczne przełączanie między opisem zdarzenia a dodatkowymi informacjami na jego temat.

Po przewinięciu listy zdarzeń przy pomocy klawisza **▲** lub **▼**, przywrócone zostanie automatyczne przełączanie między opisem zdarzenia a dodatkowymi informacjami na jego temat.

5.12 Programowanie timera strefy

Timer strefy automatycznie załącza / wyłącza czuwanie w strefie.

1. Wpisać hasło i zatwierdzić klawiszem *****.
2. Przy pomocy klawisza **▼** przewijać menu aż znalezione zostanie podmenu ZMIANA OPCJI.
3. Nacisnąć klawisz **#**.
4. Przy pomocy klawisza **▼** przewijać menu aż znaleziona zostanie funkcja TIMERY STREF.
5. Nacisnąć klawisz **#**. Zostanie wyświetlona lista stref.
6. Przy pomocy klawiszy **▼** i **▲** znaleźć na liście strefę, dla której ma zostać zaprogramowany timer.
7. Nacisnąć klawisz **#**.
8. Gdy zostanie wyświetlona opcja AKTYWNOŚĆ, upewnić się, że jest włączona (obok opcji wyświetla się symbol ). Jeżeli nie jest włączona (obok opcji wyświetla się symbol *****), nacisnąć dowolny klawisz z cyfrą.
9. Przy pomocy klawisza **▼** przewijać menu aż znaleziona zostanie funkcja TYP.
10. Nacisnąć klawisz **#**.

11. Przy pomocy klawiszy ▼ i ▲ wybrać typ timera:
codzienny – jeżeli czuwanie ma być załączane / wyłączane codziennie o tej samej porze,
tygodniowy – jeżeli czuwanie ma być załączane / wyłączane o różnych porach w różne dni tygodnia.
 12. Nacisnąć klawisz #.
 13. Jeżeli wybrany został wariant codzienny, funkcja od razu pozwoli zaprogramować czas załączenia czuwania, a po naciśnięciu klawisza ▲ lub ▼ – czas wyłączenia czuwania. Po zatwierdzeniu klawiszem #, nastąpi powrót do listy opcji i funkcji.
 14. Jeżeli wybrany został wariant tygodniowy, nastąpi powrót do listy opcji i funkcji, gdzie pojawiają się funkcje umożliwiające zaprogramowanie czasu załączenia i wyłączenia czuwania dla każdego dnia tygodnia (w analogiczny sposób jak dla timera codziennego).
-  *Zaprogramowanie wartości 99:99 oznacza, że czuwanie w strefie nie zostanie załączone / wyłączone.*
15. Po zaprogramowaniu czasu załączenia czuwania, wyświetlona zostanie dodatkowa funkcja pozwalająca określić, jaki typ czuwania będzie załączany przez dany timer. Domyślnie timer załącza pełne czuwanie. Jeżeli ma załączać inny typ czuwania, należy uruchomić tę funkcję (dla timera codziennego albo indywidualnie dla każdego dnia tygodnia), przy pomocy klawiszy ▲ i ▼ wybrać inny typ czuwania i zatwierdzić klawiszem #.
 16. Po zaprogramowaniu wszystkich parametrów, nacisnąć klawisz *.
 17. Gdy wyświetli się pytanie, czy zapisać zmiany, nacisnąć klawisz 1.

5.13 Testowanie wejść

W ramach okresowych przeglądów systemu alarmowego należy sprawdzać, czy czujki działają poprawnie. Dzięki funkcji testowania wejść można to zrobić bez wywołania reakcji przewidzianej na wypadek naruszenia, co jest szczególnie istotne w przypadku wejść czuwających stale.

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Przy pomocy klawisza ▼ przewijać menu aż znalezione zostanie podmenu TESTY.
3. Nacisnąć klawisz #.
4. Przy pomocy klawisza ▼ przewijać menu aż znalezione zostanie podmenu TEST WEJŚĆ.
5. Nacisnąć klawisz #.
6. Gdy zostanie wyświetlona funkcja NOWY, nacisnąć klawisz #.
7. Wybrać, czy testowane będą wejścia włamaniowe, czy pożarowe i techniczne, czy pojedyncze wejścia, a następnie nacisnąć klawisz #.
8. Wybrać, w których strefach będą testowane wejścia (patrz: „Wybór z listy wielokrotnego wyboru” s. 15).
9. Określić czas trwania testu (maksymalnie 50 minut) i nacisnąć klawisz #.
10. Określić, czy naruszenie wejścia ma wywołać sygnalizację GONG w manipulatorze (jeśli tak, nacisnąć dowolny klawisz z cyfrą – wyświetli się symbol .
11. Nacisnąć klawisz #. Rozpocznie się test wejść.

 *Rozpoczęcie testu wejść w dowolnej strefie uruchamia tryb testowy we wszystkich urządzeniach bezprzewodowych systemu ABAX współpracujących z centralą (czujki bezprzewodowe będą sygnalizować naruszenia przy pomocy diod LED).*

Jeżeli do centrali podłączone są czujki z funkcją zdalnego włączania / wyłączania diody LED, na czas testu można włączyć w nich diody LED (instalator może tak skonfigurować centralę, że nastąpi to automatycznie w momencie rozpoczęcia testu).

Test wejść można zakończyć przed upływem zaprogramowanego czasu przy pomocy funkcji KONIEC TESTU (► TESTY ► TEST WEJŚĆ ► KONIEC TESTU). Od chwili uruchomienia funkcji do faktycznego zakończenia testu może upłynąć do 6 sekund (przez ten czas funkcja KONIEC TESTU będzie nadal dostępna).

12. W zależności od typu testowanej czujki:

- czujki magnetyczne – otworzyć i zamknąć drzwi lub okno chronione przy pomocy czujki,
- czujki ruchu – przejść przed czujką,
- inne czujki – postępować zgodnie z zaleceniami producenta dotyczącymi testowania czujki.

13. Przejrzeć wyniki testu. W tym celu należy ponownie wejść w podmenu TEST WEJŚĆ (patrz: punkty 1-5) i uruchomić funkcję PRZEGLĄD TESTU. Listę wyników można przewijać przy pomocy klawiszy ▲ i ▼. Naciśnięcie klawisza ► lub ◀ przełączy wyświetlacz w tryb graficzny, w którym informacje przekazywane są przy pomocy symboli:

- - wejście nie zostało naruszone,
- - wejście zostało naruszone.

Naciśnięcie klawisza ► lub ◀ w trybie graficznym spowoduje wyświetlenie informacji o innym zestawie wejść (patrz też opis diod LED s. 7).



Wyniki testu można skasować przy pomocy funkcji SKASOW. WYNIKÓW (► TESTY ► TEST WEJŚĆ ► SKASOW. WYNIKÓW).

5.14 Sterowanie



Jeżeli zezwoli na to instalator, funkcja sterowania może być uruchamiana bez autoryzacji użytkownika, po naciśnięciu kolejno klawiszy 8 i #.

1. Wpisać hasło i zatwierdzić klawiszem *.
2. Nacisnąć klawisz 8. W zależności od sposobu skonfigurowania centrali przez instalatora:
 - wyświetlona zostanie lista grup wyjść – przy pomocy klawiszy ▼ i ▲ należy znaleźć grupę, w której znajduje się wyjście, a następnie nacisnąć klawisz #, żeby wyświetlona została lista wyjść,
 - wyświetlona zostanie od razu lista wyjść, którymi można sterować.
3. Przy pomocy klawiszy ▼ i ▲ znaleźć na liście wyjście, którego stan chcemy zmienić, aby sterować urządzeniem podłączonym do wyjścia. Stan wyjścia prezentowany jest przy pomocy symboli:
 - - wyjście nieaktywne (wyłączone),
 - - wyjście aktywne (włączone).



Stan wyjścia może być przedstawiany według stanu wejścia. Wyświetlane symbole należy wówczas interpretować następująco:

- - wejście nienaruszone (urządzenie sterowane przez wyjście nieaktywne),
- - wejście naruszone (urządzenie sterowane przez wyjście aktywne).

Sposób prezentowania stanu wyjść roletowych różni się od sposobu prezentowania stanu innych wyjść (patrz: „Sterowanie wyjściami roletowymi”).

5.14.1 Sterowanie wyjściem typu PRZELĄCZNIK MONO

Gdy wyjście jest nieaktywne:

- naciśnięcie klawisza ► włączy wyjście na czas zaprogramowany przez instalatora,
- naciśnięcie klawisza # pozwoli zaprogramować czas, na który wyjście zostanie włączone po kolejnym naciśnięciu klawisza #.

Gdy wyjście jest aktywne, naciśnięcie dowolnego klawisza z cyfrą wyłączy wyjście.

5.14.2 Sterowanie wyjściem typu PRZELĄCZNIK BI

Naciśnięcie klawisza # lub ► przełączy stan wyjścia. Ponadto, gdy wyjście jest aktywne, naciśnięcie dowolnego klawisza z cyfrą wyłączy wyjście.

5.14.3 Sterowanie wyjściami typu PRZEKAŹNIK TELEFONICZNY

W zależności od sposobu zaprogramowania wyjścia, naciśnięcie klawisza # lub ► włączy wyjście na czas zaprogramowany przez instalatora albo przełączy stan wyjścia. Ponadto, gdy wyjście jest aktywne, naciśnięcie dowolnego klawisza z cyfrą wyłączy wyjście.

5.14.4 Sterowanie wyjściami roletowymi

Wyjścia typu ROLETA W GÓRĘ i ROLETA W DÓŁ zawsze są programowane jako kolejne i tworzą parę. Na liście wyjść wyświetlana jest tylko nazwa wyjścia zaprogramowanego jako ROLETA W GÓRĘ. Stan wyjść prezentowany jest przy pomocy symboli:

- - wyjścia nieaktywne (wyłączone),
- ↑ - wyjście typu ROLETA W GÓRĘ aktywne (włączone),
- ↓ - wyjście typu ROLETA W DÓŁ aktywne (włączone).

Po naciśnięciu klawisza # lub ►, pod symbolem informującym o stanie wyjścia wyświetlony zostanie kursor w postaci poziomej kreski. Naciśnięcie klawisza ▲ włączy wyjście typu ROLETA W GÓRĘ (jeżeli oba wyjścia były nieaktywne) lub wyłączy wyjście typu ROLETA W DÓŁ (jeżeli było ono aktywne). Naciśnięcie klawisza ▼ włączy wyjście typu ROLETA W DÓŁ (jeżeli oba wyjścia były nieaktywne) lub wyłączy wyjście typu ROLETA W GÓRĘ (jeżeli było ono aktywne). Niezależnie od tego, które wyjście jest aktualnie aktywne, naciśnięcie dowolnego klawisza z cyfrą wyłączy je. Po zakończeniu sterowania należy nacisnąć klawisz # lub ◀, aby wrócić do listy wyjść, którymi można sterować (kursor pod symbolem zniknie).

6. Obsługa klawiatury strefowej

Podstawowym zadaniem klawiatury strefowej jest sterowanie czuwaniem jednej strefy. Ponadto oferuje szereg innych funkcji, w tym m.in. funkcje kontroli dostępu (nadzorowanie pojedynczego przejścia).

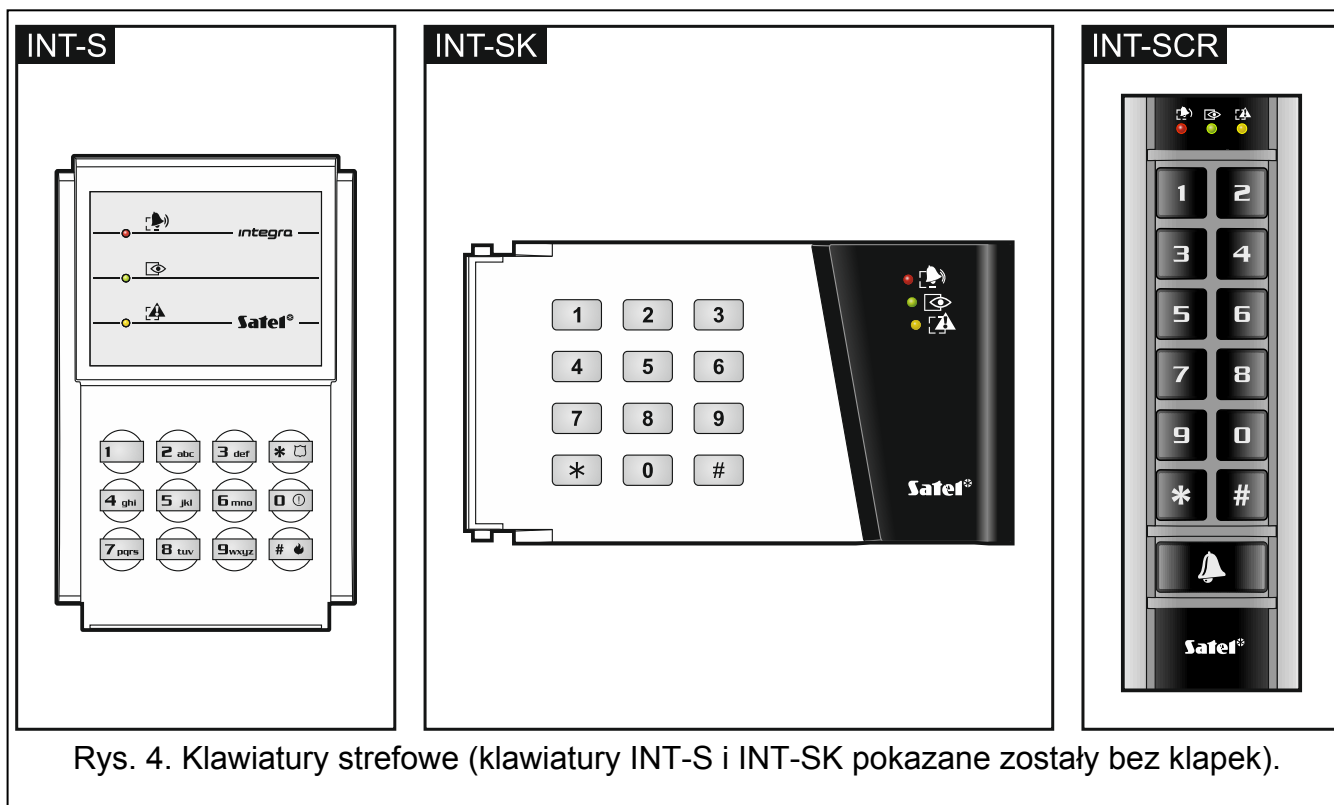
Firma SATEL oferuje następujące klawiatury strefowe:

INT-S,

INT-SK,

INT-SCR (klawiatura wielofunkcyjna z możliwością pracy w trybie klawiatury strefowej).

Klawiatury mogą być dostępne z różnymi wariantami kolorystycznymi podświetlenia klawiszy. O wariacie kolorystycznym informuje dodatkowe oznaczenie umieszczane w nazwie klawiatury (np. INT-S-GR – zielone podświetlenie, INT-S-BL – niebieskie podświetlenie).



Rys. 4. Klaviatury strefowe (klaviatury INT-S i INT-SK pokazane zostały bez kłapek).

6.1 Opis klaviatur strefowych

6.1.1 Diody LED

Dioda	Kolor	Opis działania
	zielony	świeci – strefa czuwa
	czerwony	świeci lub miga – alarm lub pamięć alarmu
	żółty	miga – awaria lub pamięć awarii

Tabela 4. Opis diod LED klaviatur strefowych.



Informacja o czuwaniu może być wygaszana po czasie zdefiniowanym przez instalatora.

Jeżeli instalator włączył opcję globalną GRADE 3:

- dioda nie informuje o alarmach,
- miganie diody oznacza, że w systemie jest awaria, są zablokowane wejścia lub miał miejsce alarm.

Miganie na przemian diod i sygnalizuje oczekiwanie na drugie hasło podczas załączania lub wyłączania czuwania na dwa hasła.

Miganie kolejno wszystkich diod sygnalizuje brak komunikacji z centralą.

6.1.2 Klawisze

Klawisze umożliwiają autoryzację użytkownika przy pomocy hasła i uruchamianie funkcji dostępnych z klawiatury strefowej.

W klawiaturze INT-SCR dostępny jest dodatkowo przycisk . Steruje on wyjściem typu OC klawiatury (wyjście jest włączone, gdy naciśnięty jest przycisk).

6.1.3 Wbudowany czytnik kart zbliżeniowych

Klawiatura INT-SCR posiada wbudowany czytnik, który umożliwia obsługę przy pomocy kart zbliżeniowych (breloków lub innych transponderów pasywnych 125 kHz). Instalator określa, czy czytnik będzie obsługiwany.

Zbliżenie karty jest traktowane identycznie jak wprowadzenie hasła i zatwierdzenie klawiszem *****. Przytrzymanie karty (około 3 sekundy) jest traktowane identycznie jak wpisanie hasła i zatwierdzenie klawiszem **#**.

6.1.4 Sygnalizacja dźwiękowa

Dźwięki generowane w trakcie obsługi



Instalator może wyłączyć sygnalizację dźwiękową lub zastąpić ją miganiem podświetlenia klawiatury.

- 1 krótki dźwięk** – naciśnięcie dowolnego klawisza z cyfrą, potwierdzenie wpisania hasła lub odczytania karty.
- 2 krótkie dźwięki** – akceptacja pierwszego hasła podczas załączania lub wyłączania czuwania na dwa hasła.
- 3 krótkie dźwięki** – sygnalizacja:
 - rozpoczęcia procedury załączania czuwania (w strefie jest czas na wyjście) lub załączania czuwania (w strefie nie ma czasu na wyjście),
 - wyłączenia czuwania i/lub skasowania alarmu.
- 4 krótkie i 1 długi dźwięk** – potwierdzenie wykonania funkcji.
- 3 pary krótkich dźwięków** – użytkownik powinien zmienić hasło.
- 1 długi dźwięk** – odmowa załączania czuwania (są naruszone wejścia w strefie lub ma miejsce awaria).
- 2 długie dźwięki** – nieznane hasło/karta.
- 3 długie dźwięki** – funkcja niedostępna.

Zdarzenia sygnalizowane dźwiękiem



Sygnalizowane są tylko te zdarzenia, które wybrał instalator.

Alarmy są sygnalizowane przez czas zaprogramowany przez instalatora.

- 5 krótkich dźwięków** – naruszenie wejścia (sygnalizacja GONG).
- Długi dźwięk co 3 sekundy, a następnie seria krótkich dźwięków przez 10 sekund i 1 długi dźwięk** – odliczanie czasu na wyjście (jeżeli czas jest krótszy niż 10 sekund, wygenerowana zostanie jedynie końcowa sekwencja krótkich dźwięków).
- Sekwencja 7 coraz krótszych dźwięków powtarzana co kilka sekund** – odliczanie czasu opóźnienia autouzbrojenia.
- 2 krótkie dźwięki co sekundę** – odliczanie czasu na wejście.
- Dźwięk ciągły** – alarm.
- Długi dźwięk co 2 sekundy** – pamięć alarmu.

Długi dźwięk co sekundę – alarm pożarowy.

Krótki dźwięk co 2 sekundy – pamięć alarmu pożarowego.

Bardzo krótkie dźwięki – zbyt długo otwarte drzwi.

6.2 Funkcje dostępne z klawiatury strefowej

6.2.1 [Hasło]*

W zależności od typu użytkownika i jego uprawnień, ustawień klawiatury i stanu systemu alarmowego, wprowadzenie hasła i zatwierdzenie klawiszem * spowoduje wykonanie jednej lub kilku z poniższych funkcji:

- otwarcie przejścia (włączenie przekaźnika),
- wyłączenie czuwania w strefie,
- skasowanie alarmu,
- przełączenie stanu wyjść typu 25. PRZEŁĄCZNIK BI,
- włączenie wyjść typu 24. PRZEŁĄCZNIK MONO,
- potwierdzenie obchodu wartownika,
- włączenie czasowej blokady strefy.



Większość z wymienionych wyżej funkcji dostępna jest po włączeniu dla klawiatury strefowej opcji ZAMEK [OBSŁUGA ZAMKA]. Wpływ na dostępność funkcji mogą mieć również inne opcje klawiatury (np. jeżeli zamek realizuje funkcję ZAMKNIĘTY PODCZAS CZUWANIA [ZAŁ. W CZUWANIU], większość funkcji będzie niedostępna).

6.2.2 [Hasło]#

W zależności od typu użytkownika i jego uprawnień, ustawień klawiatury i stanu systemu alarmowego, wprowadzenie hasła i zatwierdzenie klawiszem # spowoduje wykonanie jednej lub kilku z poniższych funkcji:

- rozpoczęcie procedury załączenia czuwania w strefie / załączenie czuwania,
- wyłączenie czuwania w strefie,
- skasowanie alarmu,
- przełączenie stanu wyjść typu 25. PRZEŁĄCZNIK BI,
- włączenie wyjść typu 24. PRZEŁĄCZNIK MONO,
- potwierdzenie obchodu wartownika,
- włączenie czasowej blokady strefy,
- odblokowanie dostępu do bankomatu.

6.2.3 Szybkie załączenie czuwania

Instalator może zezwolić na załączanie czuwania bez autoryzacji użytkownika.

1. Wybrać typ czuwania, który ma zostać załączony (naciśnąć jeden z klawiszy: 0 – pełne czuwanie; 1 – pełne czuwanie + blokady; 2 – czuwanie bez wewnętrznych; 3 – czuwanie bez wewnętrznych i bez czasu na wejście).
2. Naciśnąć klawisz #. Rozpocznie się procedura załączania czuwania.

6.2.4 Wywołanie alarmu z klawiatury

Instalator może zezwolić na wywoływanie alarmów z klawiatury. W celu wywołania alarmu należy:

alarm pożarowy – nacisnąć na około 3 sekundy klawisz  (INT-S) /  (INT-SK) /  (INT-SCR),

alarm medyczny (pomocniczy) – nacisnąć na około 3 sekundy klawisz 0,

alarm napadowy – nacisnąć na około 3 sekundy klawisz   (INT-S) /  (INT-SK) /  (INT-SCR). Instalator określa, czy wywołany zostanie alarm napadowy głośny (uruchamiający głośną sygnalizację alarmu) czy cichy (bez głośnej sygnalizacji).

6.2.5 Wyciszenie sygnalizacji alarmu w klawiaturze

Jeżeli klawiatura sygnalizuje alarm, naciśnięcie dowolnego klawisza oznaczonego cyfrą wycisza sygnalizację na około 40 sekund.

6.2.6 Zmiana hasła

Instalator może zezwolić na zmianę własnego hasła przy pomocy klawiatury strefowej.

1. Nacisnąć i przytrzymać przez około 3 sekundy klawisz 1.
2. Gdy zaczną migać na przemian diody LED  i , wpisać dotychczasowe hasło i zatwierdzić klawiszem .
3. Gdy zaczną migać na przemian diody  i , wpisać nowe hasło i zatwierdzić klawiszem .

7. Obsługa klawiatury wejściowej

Klawiatura wielofunkcyjna INT-SCR może pracować w trybie klawiatury wejściowej (INT-ENT). Głównym zadaniem klawiatury wejściowej jest odblokowanie opóźnienia dla wejść o typie reakcji 3. OPÓŹNIONA WEWNĘTRZNA. Czas, przez który wejścia te będą działały jak opóźnione jest programowany dla klawiatury. Jeżeli do strefy przypisane jest kilka klawiatur wejściowych, dla każdej można zaprogramować inny czas odblokowania opóźnienia. Po upływie zaprogramowanego czasu, wejścia opóźnione wewnętrzne ponownie działać będą jak natychmiastowe.

7.1 Diody LED

Wykorzystywana jest tylko dioda . Jej miganie informuje o odliczaniu czasu odblokowania opóźnienia (wyłączenie czuwania nie ma wpływu na miganie diody).

7.2 Sygnalizacja dźwiękowa



Instalator może wyłączyć sygnalizację dźwiękową lub zastąpić ją miganiem podświetlenia klawiatury.

W trakcie obsługi klawiatura może generować następujące dźwięki:

- 1 krótki dźwięk** – naciśnięcie dowolnego klawisza z cyfrą, potwierdzenie wpisania hasła lub odczytania karty.
- 3 krótkie dźwięki** – potwierdzenie odblokowania opóźnienia.
- 4 krótkie i 1 długi dźwięk** – potwierdzenie obchodu wartownika lub wykonania funkcji sterowania wyjściami typu 24. PRZEŁĄCZNIK MONO lub 25. PRZEŁĄCZNIK BI.
- 3 pary krótkich dźwięków** – użytkownik powinien zmienić hasło.

2 długie dźwięki – nieznane hasło/karta.

3 długie dźwięki – odblokowanie opóźnienia jest niemożliwe (strefa nie czuwa lub opóźnienie już zostało uruchomione) albo funkcja niedostępna.

Klawiatura może dodatkowo sygnalizować dźwiękami CZAS ODBLOKOWANIA OPÓŹNIENIA.

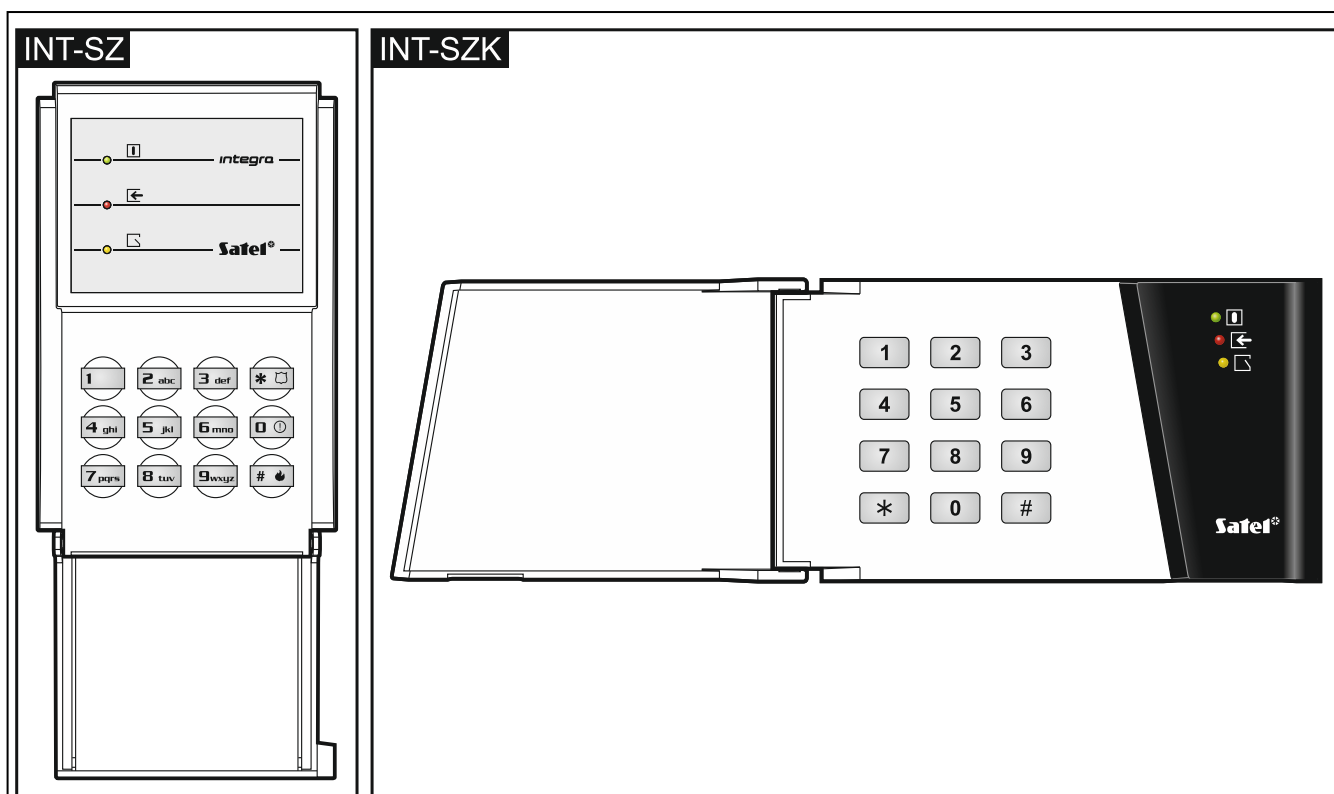
7.3 Funkcje dostępne z klawiatury wejściowej

W zależności od typu użytkownika i jego uprawnień, ustawień klawiatury i stanu systemu alarmowego, wprowadzenie hasła i zatwierdzenie klawiszem * lub # (zbliżenie karty zbliżeniowej) spowoduje:

- odblokowanie w strefie opóźnienia dla wejść o typie reakcji 3. OPÓŹNIONA WEWNĘTRZNA,
- przełączenie stanu wyjść typu 25. PRZEŁĄCZNIK BI,
- włączenie wyjść typu 24. PRZEŁĄCZNIK MONO,
- potwierdzenie obchodu wartownika.

8. Obsługa zamka szyfrowego

Podstawowym zadaniem zamka szyfrowego jest realizacja funkcji kontroli dostępu (nadzorowanie pojedynczego przejścia).



Rys. 5. Zamki szyfrowe.

Firma SATEL oferuje następujące zamki szyfrowe:

INT-SZ,

INT-SZK.

Zamki szyfrowe mogą być dostępne z różnymi wariantami kolorystycznymi podświetlenia klawiszy. O wariantie kolorystycznym informuje dodatkowe oznaczenie umieszczane w nazwie zamka (np. INT-SZ-GR – zielone podświetlenie; INT-SZ-BL – niebieskie podświetlenie).

8.1 Opis zamków szyfrowych

8.1.1 Diody LED

Dioda	Kolor	Opis działania
	zielony	świeci – zamek jest obsługiwany przez centralę
	czerwony	świeci – przejście otwarte
	żółty	miga – drzwi otwarte

Tabela 5. Opis diod LED zamków szyfrowych.

 *Miganie kolejno wszystkich diod sygnalizuje brak komunikacji z centralą.*

8.1.2 Klawisze

Klawisze umożliwiają autoryzację użytkownika przy pomocy hasła i uruchamianie funkcji dostępnych z zamka szyfrowego.

8.1.3 Sygnalizacja dźwiękowa

Dźwięki generowane w trakcie obsługi

 *Instalator może wyłączyć sygnalizację dźwiękową lub zastąpić ją miganiem podświetlenia klawiatury.*

1 krótki dźwięk – naciśnięcie dowolnego klawisza z cyfrą lub potwierdzenie wpisania hasła.

4 krótkie i 1 długi dźwięk – potwierdzenie otwarcia przejścia lub wykonania innej funkcji.

3 pary krótkich dźwięków – użytkownik powinien zmienić hasło.

2 długie dźwięki – nieznane hasło/karta.

3 długie dźwięki – funkcja niedostępna.

Zdarzenia sygnalizowane dźwiękiem

 *Sygnalizowane są tylko te zdarzenia, które wybrał instalator.*

5 krótkich dźwięków – naruszenie wejścia (sygnalizacja GONG).

Bardzo krótkie dźwięki – zbyt długo otwarte drzwi.

8.2 Funkcje dostępne z zamka szyfrowego

W zależności od typu użytkownika i jego uprawnień oraz ustawień zamka szyfrowego, wprowadzenie hasła i zatwierdzenie klawiszem ***** lub **#** spowoduje:

- otwarcie przejścia (włączenie przekaźnika),
- przełączenie stanu wyjść typu 25. PRZELĄCZNIK BI,
- włączenie wyjść typu 24. PRZELĄCZNIK MONO,
- potwierdzenie obchodu wartownika,
- włączenie czasowej blokady strefy.

Instalator może zezwolić na wywoływanie alarmów z klawiatury. W celu wywołania alarmu należy:

alarm pożarowy – nacisnąć na około 3 sekundy klawisz  (INT-SZ) /  (INT-SZK),

alarm medyczny (pomocniczy) – nacisnąć na około 3 sekundy klawisz 0,

alarm napadowy – nacisnąć na około 3 sekundy klawisz  (INT-SZ) /  (INT-SZK).

Instalator określa, czy wywołany zostanie alarm napadowy głośny (uruchamiający głośną sygnalizację alarmu) czy cichy (bez głośnej sygnalizacji).

Instalator może zezwolić na zmianę własnego hasła przy pomocy zamka szyfrowego. Należy postępować analogicznie, jak w przypadku zmiany hasła przy pomocy klawiatury strefowej (patrz: s. 40).

9. Potwierdzanie powiadamiania głosowego

Instalator może tak skonfigurować centralę, że wymagane jest potwierdzenie odsłuchania komunikatu głosowego. W przypadku braku potwierdzenia, centrala może łączyć się wielokrotnie, żeby odtworzyć komunikat. Odsłuchanie komunikatu może zostać potwierdzone z klawiatury telefonu z wybieraniem tonowym DTMF. Instalator określa, czy do potwierdzenia odebrania powiadamiania głosowego wystarczy dowolny ciąg 4 cyfr, czy też musi to być konkretne hasło. Po wprowadzeniu hasła centrala informuje przy pomocy sygnałów dźwiękowych:

1 krótki dźwięk powtarzany co 3 sekundy – komunikat został potwierdzony, należy poczekać na odtworzenie kolejnego komunikatu głosowego,

4 krótkie i 1 długi dźwięk – komunikat został potwierdzony, nie ma więcej komunikatów głosowych,

2 długie dźwięki – wprowadzone zostało błędne hasło (komunikat nie został potwierdzony).



W przypadku, gdy centrala powiadamia o kilku zdarzeniach i wymagane jest potwierdzenie powiadamiania głosowego, każdy komunikat należy potwierdzić. Dopiero po potwierdzeniu pierwszego komunikatu zostanie odtworzony drugi itd.

Instalator może tak skonfigurować centralę, że potwierdzenie odebrania komunikatu przez użytkownika:

- skasuje powiadamianie innych użytkowników,*
- pozwoli uzyskać dostęp do interaktywnego menu głosowego modułu INT-VG.*

10. Odpowiadanie na telefon i sterowanie telefoniczne



Poniższe informacje nie dotyczą central, do których podłączony jest moduł INT-VG.

Z funkcji odpowiadania na telefon i sterowania telefonicznego mogą korzystać użytkownicy posiadający **hasło telefoniczne**. Funkcje te wymagają posługiwania się telefonem z wybieraniem tonowym DTMF. Funkcja odpowiadania na telefon pozwala uzyskać informacje o stanie stref (czuwanie, alarmy). Dzięki funkcji sterowania telefonicznego można przy pomocy telefonu sterować wyjściami typu PRZEKAŹNIK TELEFONICZNY.

10.1 Odpowiadanie na telefon

1. Nawiązać połączenie z centralą w jeden z poniższych sposobów (należy ustalić z instalatorem, który sposób obsługuje centrala):

pojedyncze wywołanie – zadzwonić na numer telefonu centrali alarmowej. Po zaprogramowanej przez instalatora liczbie dzwonek centrala odbierze.

podwójne wywołanie – zadzwonić na numer telefonu centrali alarmowej. Po zaprogramowanej przez instalatora liczbie dzwonek odłożyć słuchawkę. W ciągu trzech minut ponownie zadzwonić. Centrala odbierze natychmiast.

Nawiązanie połączenia zostanie zasygnalizowane trzema krótkimi dźwiękami.

2. Na klawiaturze telefonu wpisać hasło telefoniczne. 4 krótkie i 1 długi dźwięk potwierdzą uzyskanie dostępu do funkcji odpowiadania na telefon. Jeśli podane hasło jest nieprawidłowe, centrala zasygnalizuje to dwoma długimi dźwiękami.



Jeżeli podczas wprowadzania hasła popełniony zostanie błąd, należy mimo tego wprowadzić 4 cyfry, a kiedy centrala zasygnalizuje, że hasło jest błędne, wprowadzić poprawne hasło.

Po podaniu trzech błędnych haseł, centrala rozłączy się.

W przypadku pojedynczego wywołania, jeżeli:

- hasło nie zostanie podane i nastąpi koniec połączenia,
 - podane zostanie błędne hasło i nastąpi koniec połączenia,
- centrala przez kilka następnych minut nie będzie odbierać połączeń. Pozwala to podłączyć za centralą np. faks.*

3. W ciągu maksymalnie 15 sekund podać dwucyfrowy numer strefy (np. 01, 07 lub 15). Centrala poinformuje o stanie strefy przy pomocy dźwięków:
3 krótkie dźwięki – strefa nie czuwa,
4 krótkie i 1 długi dźwięk – strefa czuwa.
Jeżeli przez 15 sekund nie zostanie naciśnięty żaden klawisz w telefonie, centrala rozłączy się.
4. Po naciśnięciu na klawiaturze telefonu kolejno klawiszy 0 i # centrala rozłączy się.

10.2 Sterowanie telefoniczne

1. Uzyskać dostęp do funkcji odpowiadania na telefon (punkty 1-2 w rozdziale „Odpowiadanie na telefon”).
2. W ciągu maksymalnie 15 sekund na klawiaturze telefonu nacisnąć kolejno klawisze 2 i #. 4 krótkie i 1 długi dźwięk potwierdzą uzyskanie dostępu do funkcji sterowania telefonicznego.
3. W ciągu maksymalnie 15 sekund podać dwucyfrowy numer przekaźnika telefonicznego (np. 01, 07 lub 15). Centrala poinformuje o zmianie stanu przekaźnika przy pomocy dźwięków:
3 krótkie dźwięki – przekaźnik został wyłączony,
4 krótkie i 1 długi dźwięk – przekaźnik został włączony.



Sposób działania wyjścia typu PRZekaźnik TELEFONICZNY zależy od tego, jak skonfigurował je instalator.

4. Po naciśnięciu na klawiaturze telefonu kolejno klawiszy 0 i # centrala rozłączy się. Można też nacisnąć klawisze 1 i #, aby wrócić do funkcji odpowiadania na telefon.

10.3 Dźwiękowa weryfikacja alarmu



Zdalna dźwiękowa weryfikacja alarmu jest możliwa, gdy do centrali podłączony jest moduł INT-AV.

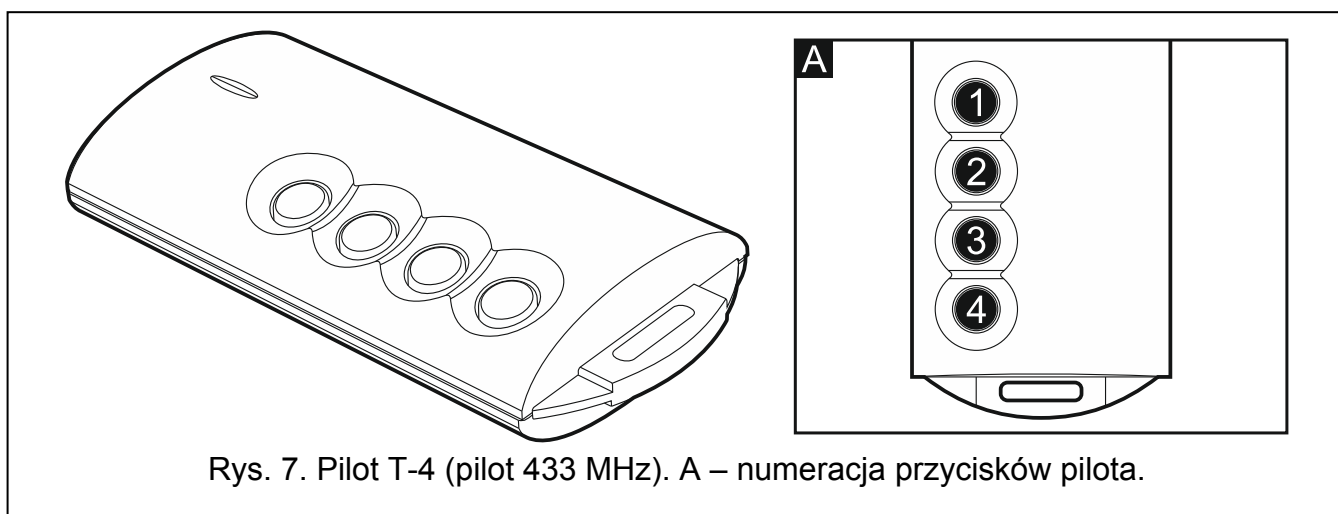
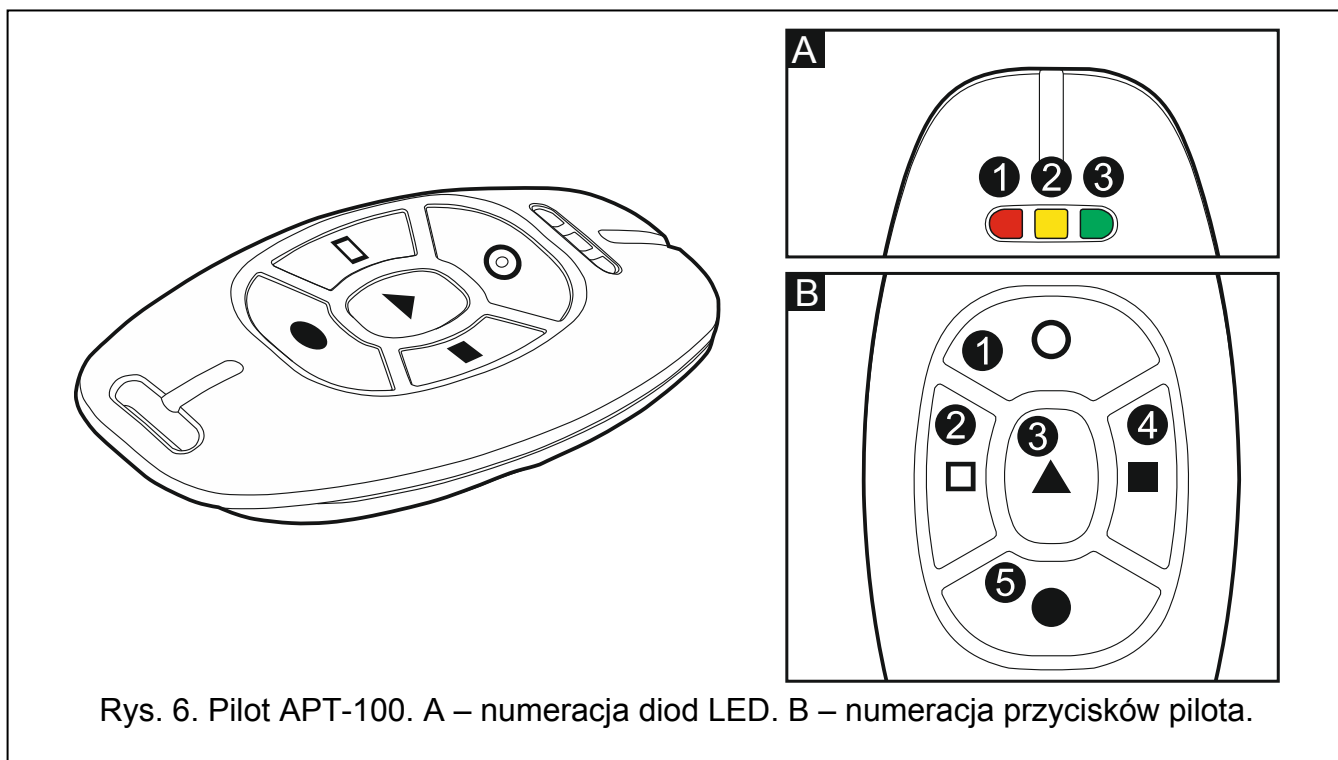
1. Uzyskać dostęp do funkcji odpowiadania na telefon (punkty 1-2 w rozdziale „Odpowiadanie na telefon”).
2. W ciągu maksymalnie 15 sekund na klawiaturze telefonu nacisnąć kolejno klawisze 3 i #. 4 krótkie i 1 długi dźwięk potwierdzą uzyskanie dostępu do funkcji dźwiękowej weryfikacji alarmu. Komendy DTMF, z których można korzystać po rozpoczęciu sesji podsłuchu / rozmowy, opisane są w instrukcji do modułu INT-AV.

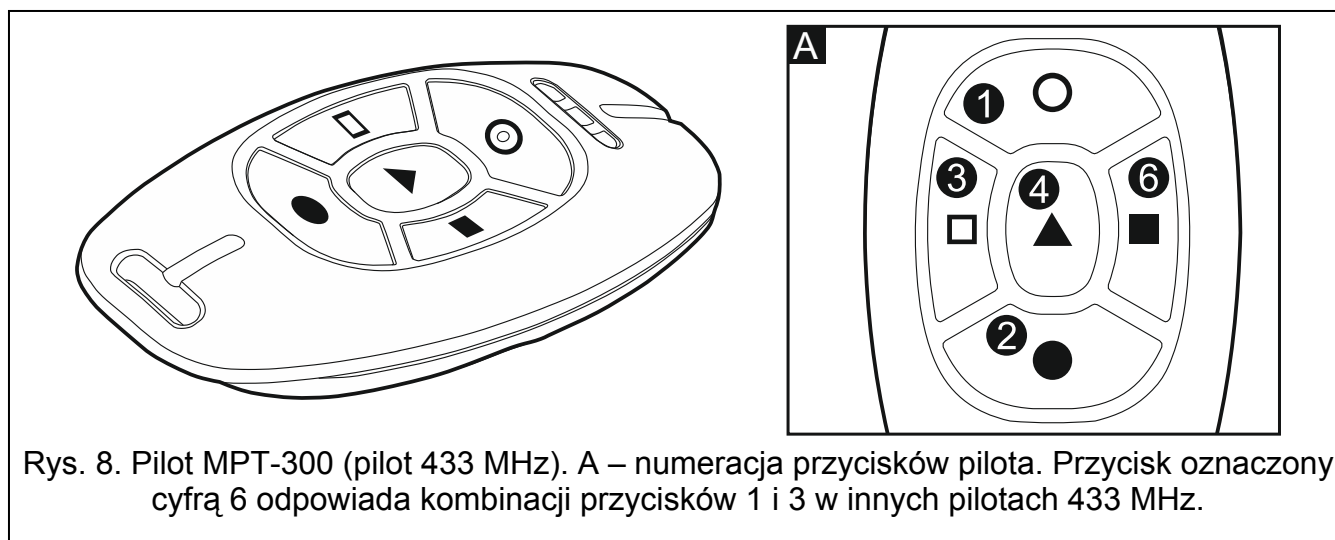
11. Obsługa systemu alarmowego przy pomocy pilota

W przypadku centrali, do której podłączony jest moduł ACU-120, ACU-270, ACU-100, ACU-250, INT-RX lub INT-RX-S, możliwe jest sterowanie systemem przy pomocy pilota. Użytkownik może posiadać maksymalnie 2 piloty:

- dwukierunkowy pilot APT-100 – obsługiwany przez system ABAX (kontroler ACU-120, ACU-270, ACU-100 (wersja oprogramowania 2.00 lub nowsza) lub ACU-250),
- pilot 433 MHz – obsługiwany przez moduł INT-RX lub INT-RX-S.

Pojedynczy pilot pozwala na realizację do 6 funkcji. Dla każdego pilota indywidualnie określa się funkcje realizowane po naciśnięciu przycisku lub kombinacji przycisków, a w przypadku dwukierunkowych pilotów APT-100 także informacje wyświetlane na diodach LED pilota (patrz: „Dodanie pilota” s. 29).





12. Historia zmian w treści instrukcji

Data	Wersja oprogramowania	Wprowadzone zmiany
2013-08	1.12	• Dodane zostały informacje o centrali INTEGRA 256 Plus. • Dodana została informacja o manipulatorze INT-TSG (s. 5). • Dodana została uwaga dotycząca użytkownika posiadającego uprawnienie UŻYTKOWNIK PROSTY (s. 9). • Uzupełniona została lista funkcji użytkownika (s. 10). • Dodany został opis funkcji użytkownika ZMIANA HASŁA TELEFONICZNEGO (s. 18). • Dodany został opis uprawnienia UŻYTKOWNIK PROSTY (s. 26). • Dodany został opis uprawnienia ADMINISTRATOR (s. 26). • Zmodyfikowana została informacja dotycząca pilotów, które można przypisać użytkownikowi (s. 26). • Dodana została uwaga dotycząca przycisków pilota i wejścia 256 (s. 26). • Zmodyfikowana została informacja dotycząca maksymalnego czasu trwania testu wejść (s. 34). • Dodany został rozdział „Dźwiękowa weryfikacja alarmu” (s. 44). • Treść rozdziału „Obsługa systemu alarmowego przy pomocy pilota” została zmodyfikowana i uzupełniona (s. 45).
2013-12	1.12	• Dodane zostały informacje o manipulatorach INT-KLFR (s. 4, 5 i 8) i INT-TSI (s. 5). • Zmodyfikowany został opis funkcji IP/MAC ETHM-1 (s. 21).
2014-10	1.13	• Dodane zostały informacje o module ETHM-1 Plus. • Dodana została uwaga o możliwości wyłączenia skrótów w menu użytkownika przez instalatora (s. 14). • Dodana została informacja o nowej funkcjonalności klawisza 0 podczas edycji listy wielokrotnego wyboru w trybie tekstowym (s. 15, 23, 31 i 31).
2015-10	1.14	• Dodane zostały uwagi dotyczące przekazania przez instalatora informacji na temat obsługi systemu alarmowego (s. 3). • Zmodyfikowany został rozdział dotyczący sprawności technicznej systemu alarmowego (s. 3). • Dodana została informacja o manipulatorze INT-TSH (s. 5). • Dodane zostały informacje o możliwości programowania histerezy dla wyjść typu 120. TERMOSTAT (s. 13 i 19).

		• Dodane zostały informacje dotyczące możliwości testowania pojedynczego wejścia (s. 13 i 34). • Zmodyfikowany został opis funkcji GONG W MANIPULATORZE (s. 19). • Zaktualizowany został opis funkcji IP/MAC ETHM-1 (s. 21). • Dodana została informacja o automatycznej synchronizacji zegara centrali z serwerem czasu po restarcie centrali (s. 21). • Uzupełnione zostały informacje dotyczące skracania czasu na wyjście z manipulatora (s. 24). • Zmodyfikowany został rozdział dotyczący blokowania wejść (s. 30).
--	--	---

13. Skrócony opis obsługi systemu z manipulatora



miga – awaria lub pamięć awarii / Grade 3: awaria lub pamięć awarii, zablokowane wejścia lub alarm



świeci – czuwają wszystkie obsługiwane przez manipulator strefy

miga – czuwają niektóre strefy



świeci lub **miga** – alarm lub pamięć alarmu

[HASŁO]# – załączenie czuwania / wyłączenie czuwania / skasowanie alarmu

Szybkie załączenie czuwania:

0# - czuwanie pełne

1# - czuwanie pełne + blokady

2# - czuwanie bez wewnętrznych

3# - czuwanie bez wewnętrznych i bez czasu na wyjście

9# – koniec odliczania czasu na wyjście

8# – szybkie sterowanie wyjściami

[HASŁO]* – wejście w menu użytkownika

Skróty w menu użytkownika:

1 Zmiana hasła

2 Użytkownicy [Administratorzy]

21 Nowy użytkownik [Nowy administrator]

22 Edycja użytkownika [Edycja administratora]

23 Usunięcie użytkownika [Usunięcie administratora]

4 Blokowanie wejść

41 Blokady czasowe

42 Blokady trwałe

5 Przegląd zdarzeń

51 Przegląd wybranych zdarzeń

52 Przegląd wszystkich zdarzeń

6 Programowanie zegara

7 Stan systemu

8 Sterowanie

9 Tryb serwisowy

0 Downloading

01 Start DWNL-RS

02 Koniec DWNL-RS

03 Start DWNL-MOD.

04 Start DWNL-TEL

07 ETHM-1 – DloadX

08 ETHM-1 – GuardX



○ ○ – 1. grupa (numery: 1-32 / adresy 00-1F)

○ ● – 2. grupa (numery: 33-64 / adresy 20-3F)

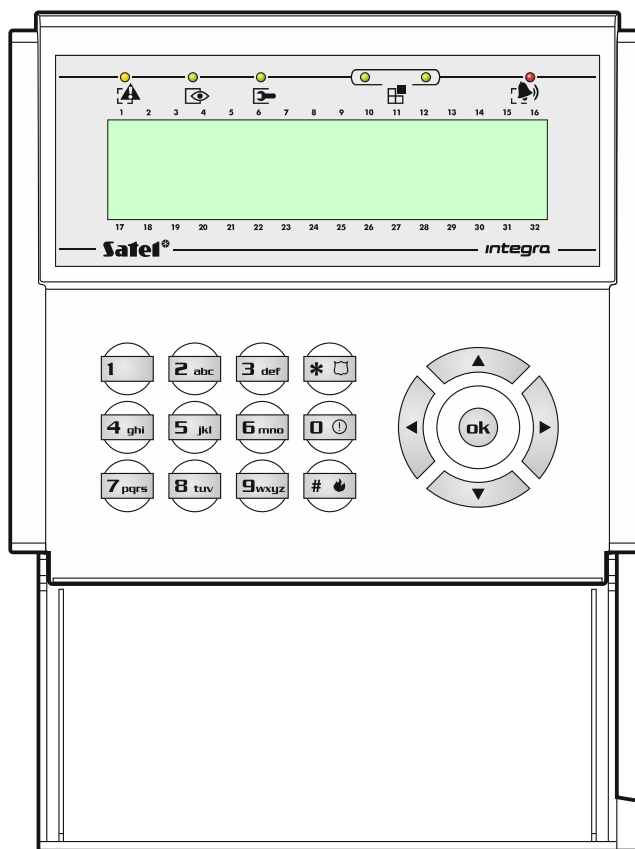
● ○ – 3. grupa (numery: 65-96)

● ● – 4. grupa (numery: 97-128)

(○ – dioda nie świeci; ● – dioda świeci)



miga – uruchomiony jest tryb serwisowy



Klawisze skrótów (naciśnięcie na około 3 sekundy):

1 – sprawdzenie stanu wejść

4 – sprawdzenie stanu stref

5 – przegląd pamięci alarmów

6 – przegląd pamięci awarii

7 – przegląd bieżących awarii

8 – włączenie/wyłączenie sygnalizacji GONG

9 – przełączenie wyświetlacza z trybu gotowości w tryb wyświetlania stanu stref i odwrotnie



! – wywołanie alarmu medycznego



🔥 – wywołanie alarmu pożarowego



🛡️ – wywołanie alarmu napadowego



INT-GSM

Moduł komunikacyjny GPRS



Wersja oprogramowania 1.00

int-gsm_pl 07/18

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLSKA
tel. 58 320 94 00 • serwis 58 320 94 30 • dz. techn. 58 320 94 20; 604 166 075
www.satel.pl

OSTRZEŻENIA

Moduł powinien być instalowany przez wykwalifikowanych specjalistów.

Przed przystąpieniem do instalacji zapoznaj się z niniejszą instrukcją w celu uniknięcia błędów, które mogą skutkować wadliwym działaniem lub nawet uszkodzeniem sprzętu.

Wszystkie połączenia elektryczne należy wykonywać przy wyłączonym zasilaniu.

Wprowadzanie w urządzeniu jakichkolwiek modyfikacji, które nie są autoryzowane przez producenta, lub dokonywanie samodzielnych napraw skutkuje utratą uprawnień wynikających z gwarancji.

Tabliczka znamionowa urządzenia umieszczona jest na podstawie obudowy.

W urządzeniu wykorzystano FreeRTOS (www.freertos.org).

Firma SATEL stawia sobie za cel nieustanne podnoszenie jakości swoich produktów, co może skutkować zmianami w ich specyfikacji technicznej i oprogramowaniu. Aktualna informacja o wprowadzanych zmianach znajduje się na naszej stronie internetowej.

Proszę nas odwiedzić:

<http://www.satel.pl>

Niniejszym SATEL sp. z o.o. deklaruje, że urządzenie jest zgodne z zasadniczymi wymaganiami i innymi właściwymi postanowieniami Dyrektywy 2014/53/EU. Deklaracja zgodności jest dostępna pod adresem www.satel.eu/ce

W instrukcji mogą wystąpić następujące symbole:



- uwaga;



- uwaga krytyczna.

SPIS TREŚCI

1. Wprowadzenie.....	2
2. Właściwości.....	2
3. Opis modułu	5
3.1 Płytkę elektroniki	5
4. Instalacja	6
4.1 Montaż w obudowie	6
4.2 Ustawienie adresu.....	6
4.3 Instalacja anteny	7
4.4 Podłączenie	7
4.4.1 Podłączenie do centrali alarmowej	7
4.4.2 Podłączenie do modułu ETHM-1 Plus	8
4.5 Uruchomienie modułu	9
4.6 Montaż kart SIM	9
5. Konfigurowanie ustawień modułu	9
5.1 INT-GSM.....	10
5.2 Funkcje INT-GSM	12
5.2.1 Telefon GSM	12
5.2.2 Obsługa PRE-PAID	15
5.2.3 Powiadamianie SMS / Sterowanie CLIP	16
5.2.4 Sterowanie SMS	18
5.2.5 Monitorowanie	19
5.2.6 Zdalna aktualizacja	21
5.3 Funkcje użytkownika	22
5.4 Wirtualny manipulator	23
5.5 Makropolecenia.....	24
5.5.1 Grupy.....	24
5.5.2 Definicje.....	25
5.5.3 Definiowanie makropoleceń	28
6. Zdalne programowanie i obsługa centrali za pośrednictwem modułu	33
6.1 Program GUARDX	33
6.1.1 Konfigurowanie ustawień programu GUARDX	33
6.1.2 Zainicjowanie połączenia przy pomocy wiadomości SMS	35
6.1.3 Zainicjowanie połączenia z manipulatora (przez centralę alarmową)	36
6.1.4 Nawiązanie połączenia za pośrednictwem serwera SATEL	36
6.2 Aplikacja mobilna INTEGRA CONTROL	36
6.2.1 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (Android)	37
6.2.2 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (iOS)	39
6.2.3 Nawiązanie komunikacji.....	41
7. Dane techniczne.....	42

1. Wprowadzenie

Niniejsza instrukcja opisuje moduł INT-GSM oraz sposób jego instalacji i konfiguracji. Moduł jest obsługiwany przez centrale alarmowe INTEGRA / INTEGRA Plus z wersją oprogramowania 1.18 lub nowszą. Moduł może zostać podłączony bezpośrednio do centrali alarmowej albo do modułu ETHM-1 Plus (wymagana wersja oprogramowania 2.05 lub nowsza), który jest podłączony do centrali INTEGRA / INTEGRA Plus.

2. Właściwości

Komunikacja

- Wbudowany telefon GSM pracujący w sieciach telefonii komórkowej 850 / 900 / 1800 / 1900 MHz.
- Obsługa dwóch kart SIM.
- Możliwość jednoczesnego odbierania wiadomości i połączeń przychodzących przez obie karty SIM.
- Możliwość zdalnego sprawdzenia stanu dostępnych środków oraz ważności konta karty SIM zainstalowanej w module.
- Możliwość zdefiniowania kodu MCC / MNC operatora sieci, do której ma się logować moduł.
- Transmisje GPRS szyfrowane przy wykorzystaniu zaawansowanego algorytmu opartego o 192-bitowy klucz.

Monitorowanie

- Monitorowanie zdarzeń do dwóch stacji monitorujących za pośrednictwem sieci GSM.
- Dwa tory transmisji:
 - GPRS,
 - wiadomości SMS.
- Określanie priorytetu torów transmisji.

Powiadamianie

- Powiadamianie o zdarzeniach w formie wiadomości SMS tworzonych automatycznie na podstawie opisów z pamięci zdarzeń centrali alarmowej.
- 16 numerów telefonów do powiadamiania.
- Powiadamianie o zdarzeniach w formie wiadomości e-mail tworzonych automatycznie na podstawie opisów z pamięci zdarzeń centrali alarmowej w przypadku współpracy z centralą INTEGRA Plus.
- 16 adresów e-mail do powiadamiania.
- Informowanie użytkowników aplikacji INTEGRA CONTROL o zdarzeniach przy pomocy powiadomień push.

Sterowanie

- Sterowanie systemem alarmowym przy pomocy:
 - wiadomości SMS,
 - CLIP (bez ponoszenia kosztów),
 - programu GUARDX (GPRS),
 - aplikacji INTEGRA CONTROL (GPRS).

- Możliwość określenia telefonów autoryzowanych do sterowania SMS lub CLIP.
- Możliwość wskazania funkcji sterujących dostępnych z dowolnych telefonów.

Aplikacja mobilna INTEGRA CONTROL

- Obsługa systemu alarmowego z urządzeń mobilnych:
 - sterowanie systemem alarmowym,
 - sprawdzanie stanu systemu alarmowego.
- Konfigurowanie systemu alarmowego z urządzeń mobilnych.
- Proste i wygodne nawiązywanie komunikacji między aplikacją INTEGRA CONTROL a modułem dzięki usłudze zestawiania połączeń SATEL.

Konfigurowanie systemu alarmowego

- Zdalne konfigurowanie systemu alarmowego przy pomocy komputera z zainstalowanym programem DLOADX przez GPRS.

Administrowanie systemem alarmowym

- Zdalne administrowanie systemem alarmowym przy pomocy komputera z zainstalowanym programem GUARDX przez GPRS.

Aktualizacja oprogramowania modułu

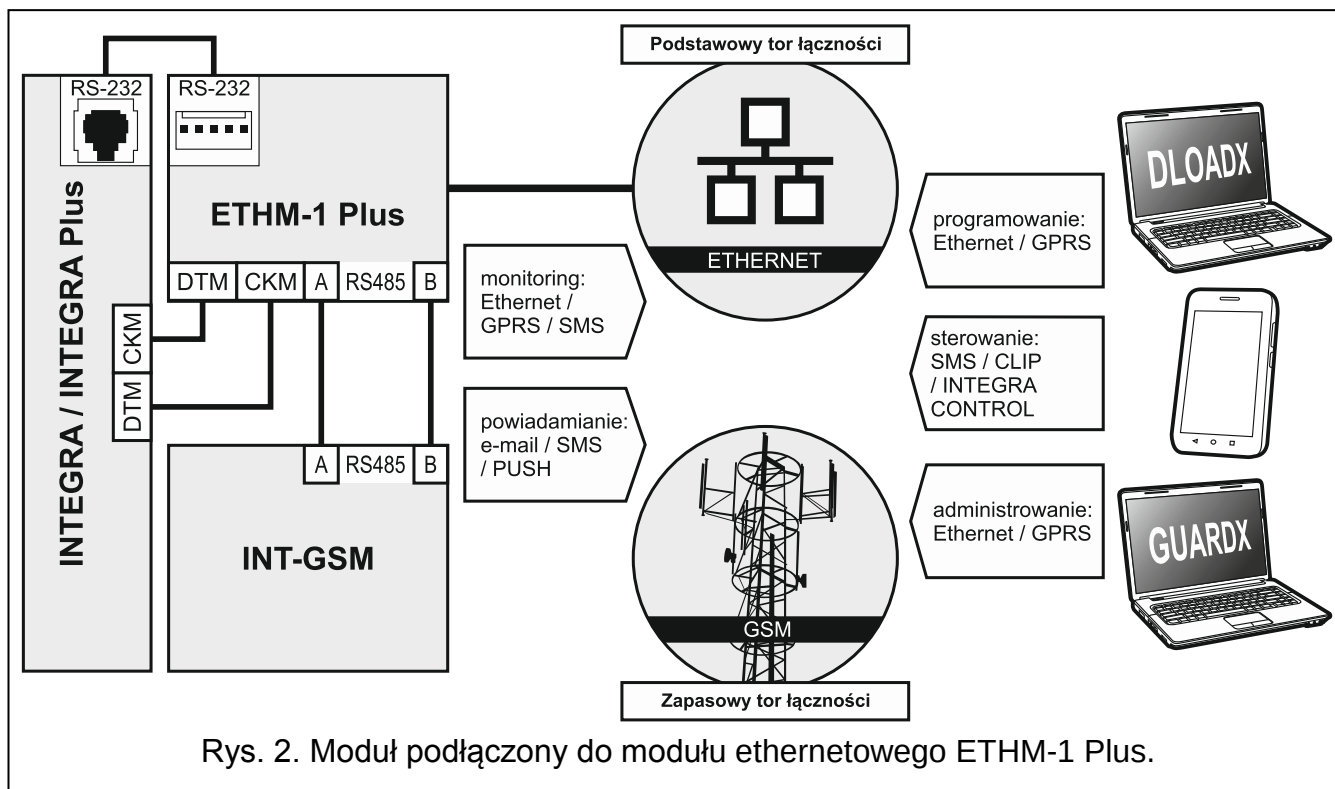
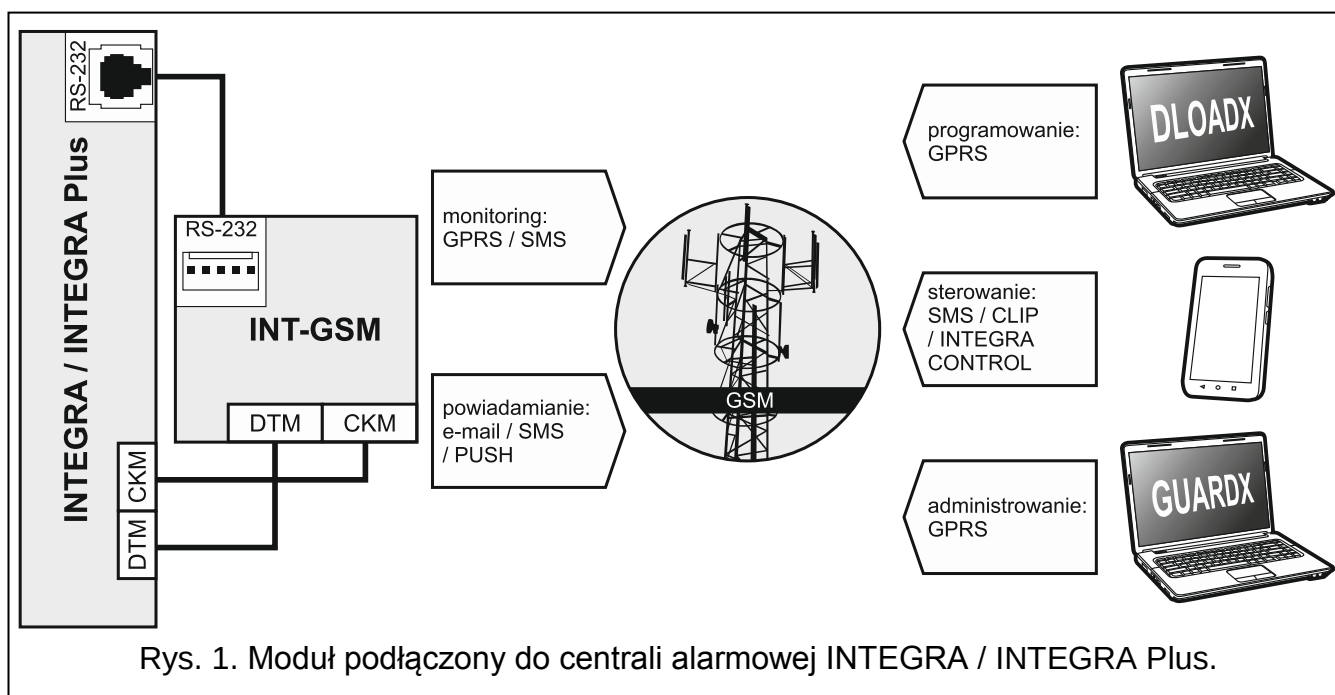
- Aktualizacja oprogramowania przy pomocy komputera podłączonego do portu RS-232 centrali.
- Aktualizacja oprogramowania z wykorzystaniem komunikacji GPRS i serwera aktualizacji UPSERV (zdalna aktualizacja).

Współpraca z modułem ethernetowym ETHM-1 Plus

- GPRS jako zapasowy tor łączności dla sieci Ethernet.
- Określanie priorytetu torów monitorowania zdarzeń (Ethernet, GPRS i SMS).
- Monitoring dwutorowy (Dual Path Reporting) zgodny z normą EN 50136.

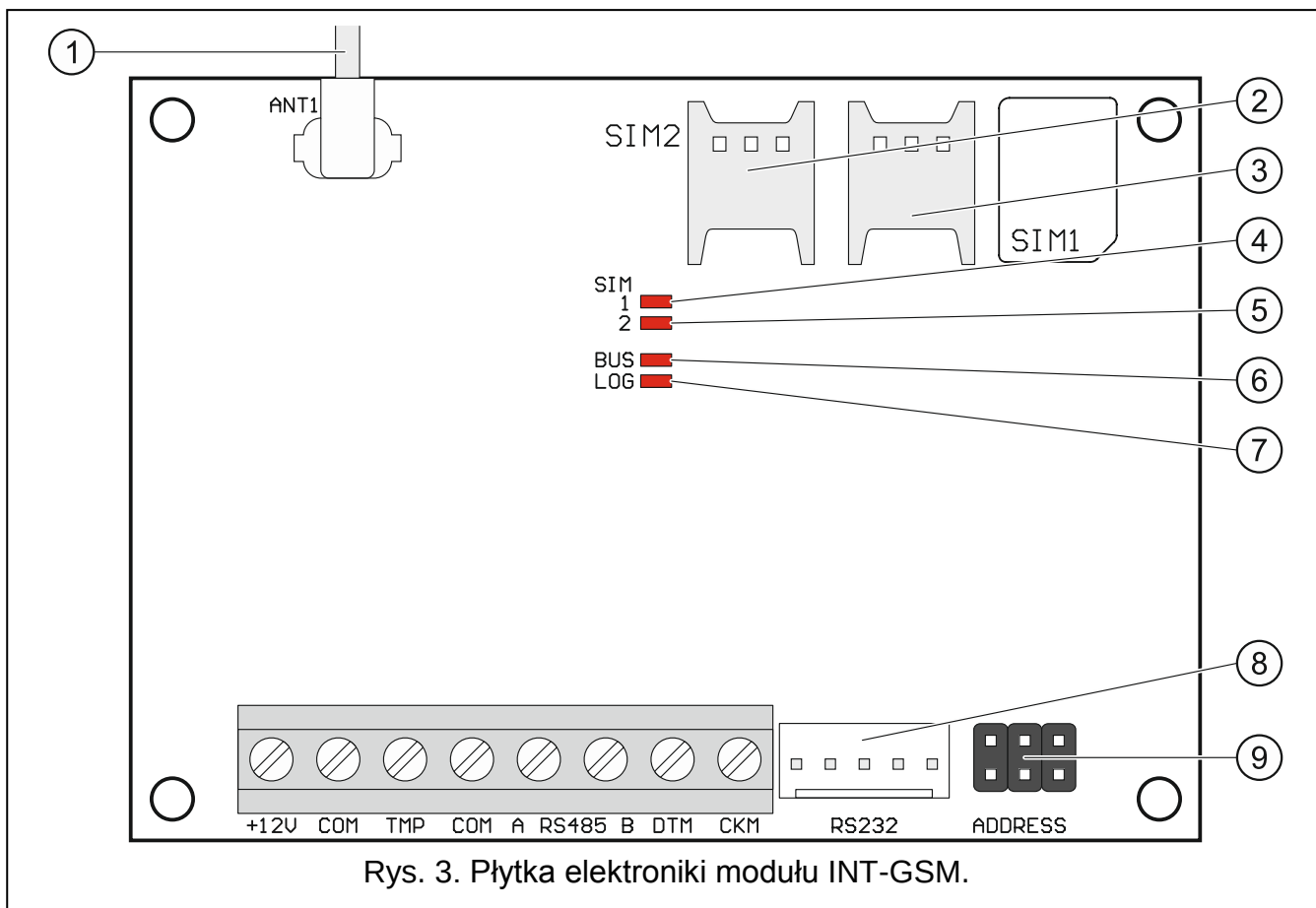
Płyta elektroniki

- Port RS-485 umożliwiający podłączenie modułu INT-GSM do modułu ETHM-1 Plus.
- Magistrala komunikacyjna umożliwiająca podłączenie modułu INT-GSM do magistrali manipulatorów centrali alarmowej.
- Port RS-232 umożliwiający:
 - połączenie z portem RS-232 centrali alarmowej (wymagane na potrzeby zdalnego konfigurowania przy pomocy programu DLOADX i zalecane na potrzeby zdalnego administrowania przy pomocy programu GUARDX),
 - podłączenie komputera na potrzeby aktualizacji oprogramowania modułu.
- Diody LED informujące o statusie modułu.
- Zasilanie napięciem stałym 12 V ($\pm 15\%$).



3. Opis modułu

3.1 Płytki elektroniki



Rys. 3. Płytki elektroniki modułu INT-GSM.

- ① kabel anteny (antena dodawana jest do modułu).
- ② gniazdo przeznaczone do zamontowania drugiej karty SIM.
- ③ gniazdo przeznaczone do zamontowania pierwszej karty SIM.
- i** *Nie zaleca się wkładania karty SIM do gniazda przed zaprogramowaniem w module jej kodu PIN (jeśli karta wymaga podania kodu PIN).*
- ④ dioda LED SIM1. Świeci, gdy aktywna jest karta zamontowana w gnieździe SIM 1.
- ⑤ dioda LED SIM2. Świeci, gdy aktywna jest karta zamontowana w gnieździe SIM 2.
- ⑥ dioda LED BUS. Miga, gdy trwa wymiana danych z centralą.
- ⑦ dioda LED LOG:
 - świeci – obecne zasilanie,
 - miga – trwa komunikacja za pośrednictwem modułu.
- ⑧ port RS-232.
- ⑨ kołki do ustawienia adresu modułu (patrz: „Ustawienie adresu” s. 6).

Opis zacisków

- +12V** – wejście zasilania (12 V DC $\pm 15\%$).
- COM** – masa.

TMP	– wejście sabotażowe (NC) – jeżeli nie jest wykorzystywane, powinno być zwarte do masy.
A RS485 B	– port RS-485 umożliwiający połączenie z modułem ETHM-1 Plus.
DTM	– dane (magistrala komunikacyjna).
CKM	– zegar (magistrala komunikacyjna).

4. Instalacja



Wszystkie połączenia elektryczne należy wykonywać przy wyłączonym zasilaniu.

Nie zaleca się włączania zasilania urządzenia, gdy nie jest podłączona antena.

Instalacja, do której moduł ma zostać podłączony, powinna być wyposażona w:

- dwubiegunowy rozłącznik z separacją zestyków równą co najmniej 3 mm.
- zabezpieczenie przeciwzwarciowe bezpiecznikiem typu zwłocznego o wartości 16 A.

Moduł INT-GSM powinien być instalowany w pomieszczeniach zamkniętych o normalnej wilgotności powietrza. Wybierając miejsce montażu pamiętaj, że grube mury, metalowe ścianki itp. zmniejszają zasięg sygnału radiowego. Nie zaleca się montażu w pobliżu instalacji elektrycznych, ponieważ może to spowodować wadliwe funkcjonowanie urządzenia.

4.1 Montaż w obudowie



Obudowa, w której montowany jest moduł, powinna spełniać warunki dla obudów przeciwpożarowych.

Jeżeli moduł ma być podłączony bezpośrednio do centrali alarmowej, powinien być montowany w tej samej obudowie, co centrala alarmowa. Ułatwi to połączenie portów RS-232 centrali i modułu.

1. Zamocuj płytkę elektroniki modułu w obudowie.
2. Jeżeli moduł ma nadzorować styk sabotażowy obudowy, podłącz przewody styku sabotażowego do zacisków TMP i COM. Jeżeli moduł nie ma nadzorować styku sabotażowego obudowy, zacisk TMP połącz z zaciskiem COM modułu.

4.2 Ustawienie adresu



Ustawienie adresu jest wymagane, jeżeli moduł będzie podłączony do magistrali manipulatorów centrali alarmowej. Jeżeli moduł INT-GSM będzie podłączony do modułu ETHM-1 Plus, adresu nie trzeba ustawiać.

Adres ustawia się przy pomocy zworek zakładanych na kołki ADDRESS. W tabeli 1 przedstawiono sposób zakładania zworek w celu ustawienia określonego adresu (■ - zworka założona; □ - zworka zdjęta).

Adres	0	1	2	3	4	5	6	7
Stan kołków	□□□	■□□	□■□	■■□	□□■	■□■	□■■	■■■

Tabela 1.

Ustaw w module adres z zakresu:

- od 0 do 3, jeżeli podłączony jest do centrali INTEGRA 24 lub INTEGRA 32,
- od 0 do 7, jeżeli podłączony jest do innej centrali INTEGRA lub do centrali INTEGRA Plus.

Adres musi być inny, niż w pozostałych urządzeniach podłączonych do magistrali manipulatorów centrali alarmowej (centrala nie obsługuje urządzeń o identycznych adresach).

4.3 Instalacja anteny

Moduł INT-GSM sprzedawany jest razem z anteną. Antenę tę można zastąpić anteną montowaną na obudowie lub anteną przeznaczoną do montażu w pewnej odległości od obudowy. Wymagane jest wówczas użycie przejściówki IPX-SMA.

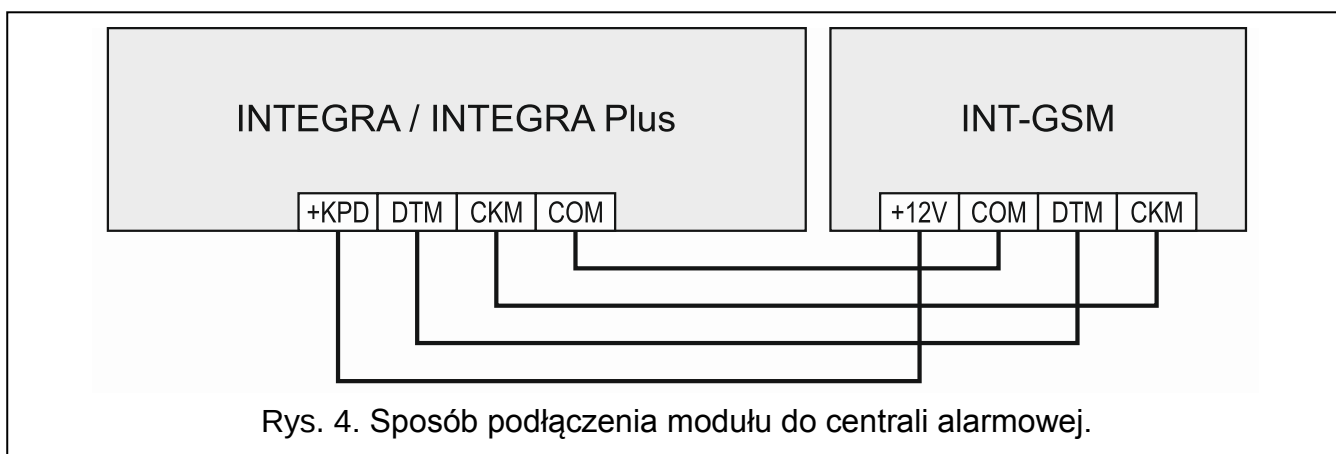
Zastosowanie anteny montowanej w pewnej odległości od obudowy jest wskazane, jeżeli w miejscu montażu modułu grube mury, metalowe ścianki itp. zmniejszają zasięg sygnału radiowego.

Antena nie powinna być umieszczana równolegle do przewodów instalacji elektrycznej niskonapięciowej, gdyż może to obniżyć skuteczność anteny.

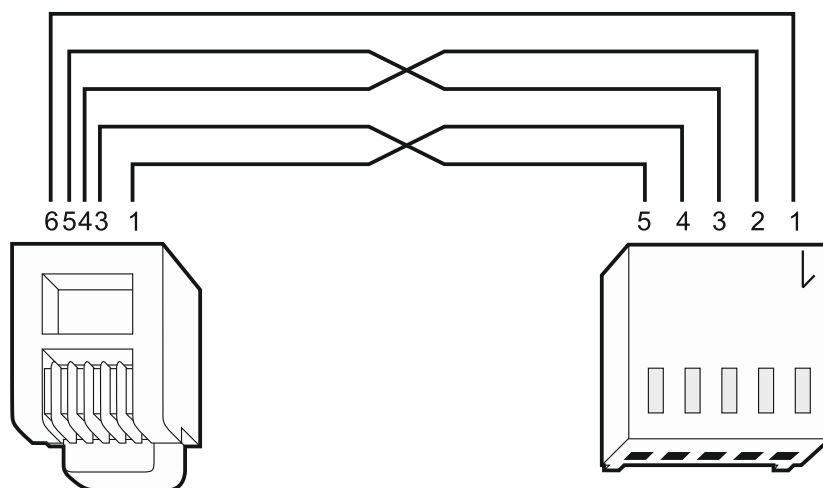
4.4 Podłączenie

Moduł może zostać podłączony bezpośrednio do centrali alarmowej albo do modułu ETHM-1 Plus. Zaleca się stosowanie kabla prostego nieekranowanego.

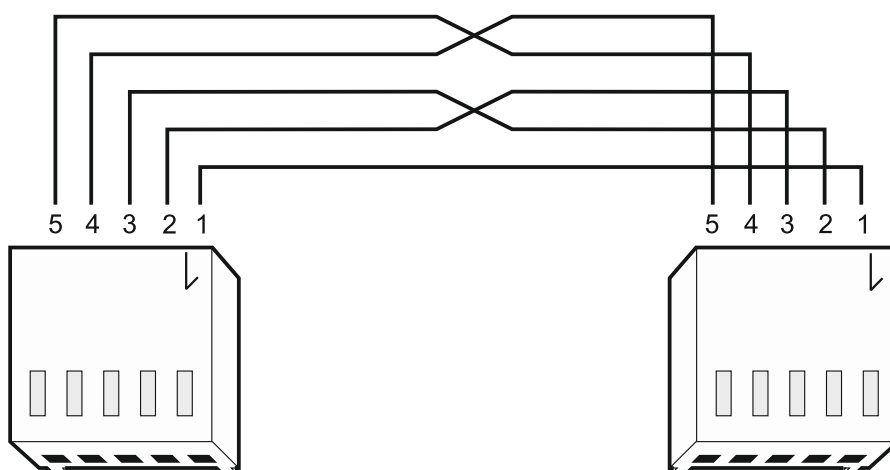
4.4.1 Podłączenie do centrali alarmowej



1. Zaciski +12V, COM, DTM i CKM modułu połącz z zaciskami centrali alarmowej (rys. 4). Do połączenia zacisków +12V i COM użyj przewodów giętkich o przekroju 0,5-0,75 mm² albo przewodów sztywnych o przekroju 1-2,5 mm². Jeśli do połączenia zacisków DTM i CKM użyjesz kabla typu „skrętka”, pamiętaj, że jedną parą skręconych przewodów nie wolno przysyłać sygnałów CKM (zegar) i DTM (dane). Przewody muszą być prowadzone w jednym kablu.
2. Jeżeli centrala alarmowa ma być programowana za pośrednictwem modułu przy pomocy programu DLOADX, połącz port RS-232 modułu z portem RS-232 centrali. W zależności od centrali alarmowej, połączenie należy wykonać przy pomocy kabla:
INTEGRA z gniazdem typu RJ / INTEGRA Plus: **RJ/PIN5** (rys. 5),
INTEGRA z gniazdem typu PIN5: **PIN5/PIN5** (rys. 6),
Wymienione kable dostępne są w ofercie firmy SATEL.

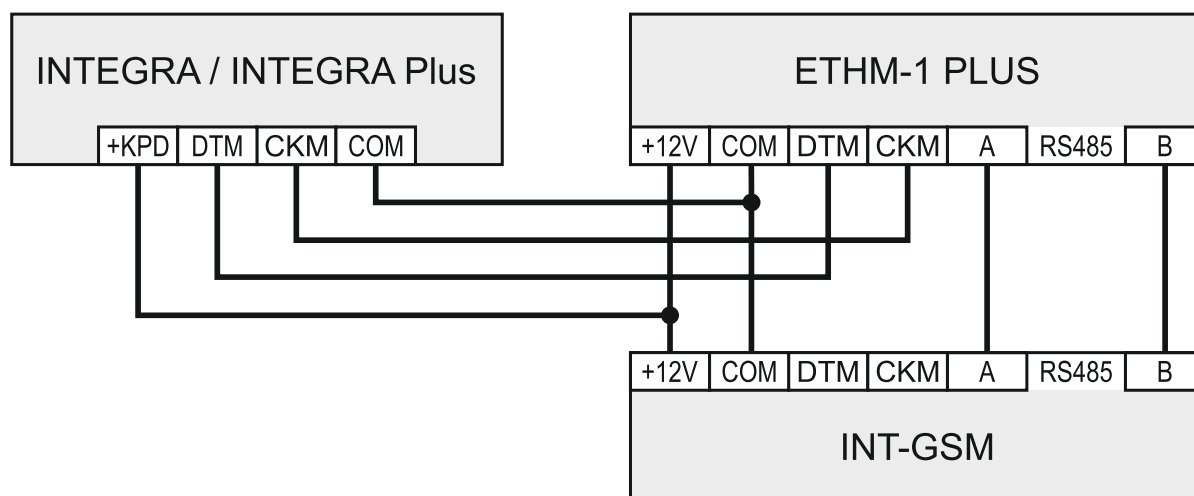


Rys. 5. Schemat kabla służącego do połączenia portów RS-232 modułu INT-GSM i centrali INTEGRA / INTEGRA Plus z gniazdem typu RJ.



Rys. 6. Schemat kabla służącego do połączenia portów RS-232 modułu INT-GSM i centrali INTEGRA z gniazdem PIN5.

4.4.2 Podłączenie do modułu ETHM-1 Plus



Rys. 7. Sposób podłączenia modułu INT-GSM do modułu ETHM-1 Plus.

Jeżeli moduł ma współpracować z modułem ETHM-1 Plus (wymagana wersja oprogramowania: 2.05 lub nowsza), połączenia między modułami i centralą alarmową wykonaj zgodnie z rysunkiem 7.

4.5 Uruchomienie modułu

1. Włącz zasilanie systemu alarmowego.
2. Uruchom w centrali alarmowej funkcję identyfikacji (patrz: instrukcja instalatora centrali alarmowej). Jeżeli moduł jest podłączony do centrali alarmowej, zostanie zidentyfikowany jako „INT-GSM”. Jeżeli moduł jest podłączony do modułu ETHM-1 Plus, na liście urządzeń pojawi się „ETHM+GSM” (zamiast „ETHM-1”).
3. Skonfiguruj moduł (patrz: „Konfigurowanie ustawień modułu”). Jeżeli wymaga tego karta / karty SIM, przy pomocy programu DLOADX zaprogramuj kod / kody PIN (patrz: s. 12).

4.6 Montaż kart SIM

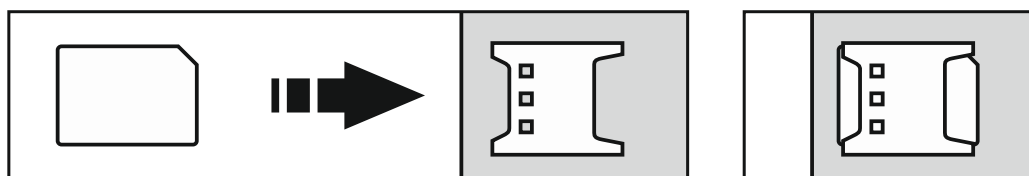
W module można zamontować dwie karty nano-SIM.

1. Wyłącz zasilanie systemu alarmowego.
2. Zainstaluj w module kartę / karty SIM (rys. 8).
3. Włącz zasilanie systemu alarmowego. Logowanie telefonu do sieci GSM może potrwać kilka minut.



Do przesyłania danych w technologii GPRS zaleca się używanie kart SIM z planem taryfowym dedykowanych do komunikacji M2M (machine-to-machine).

Jeżeli zaprogramowany zostanie błędny kod PIN, moduł zgłosi awarię. Kolejna próba użycia kodu PIN nastąpi po 4 minutach. Po trzeciej próbie użycia błędnego kodu PIN, karta SIM zostanie zablokowana. W celu odblokowania karty SIM należy przełożyć ją do telefonu komórkowego i wprowadzić kod PUK.



Rys. 8. Sposób montażu karty nano-SIM.

5. Konfigurowanie ustawień modułu

Ustawienia modułu możesz skonfigurować przy pomocy:

- programu DLOADX: okno „Struktura” → zakładka „Sprzęt” → gałąź „Manipulatory” → [nazwa modułu] (rys. 9),
- manipulatora: ► TRYB SERWISOWY ► STRUKTURA ► SPRZĘT ► MANIPULATORY ► USTAWIENIA ► [nazwa modułu].

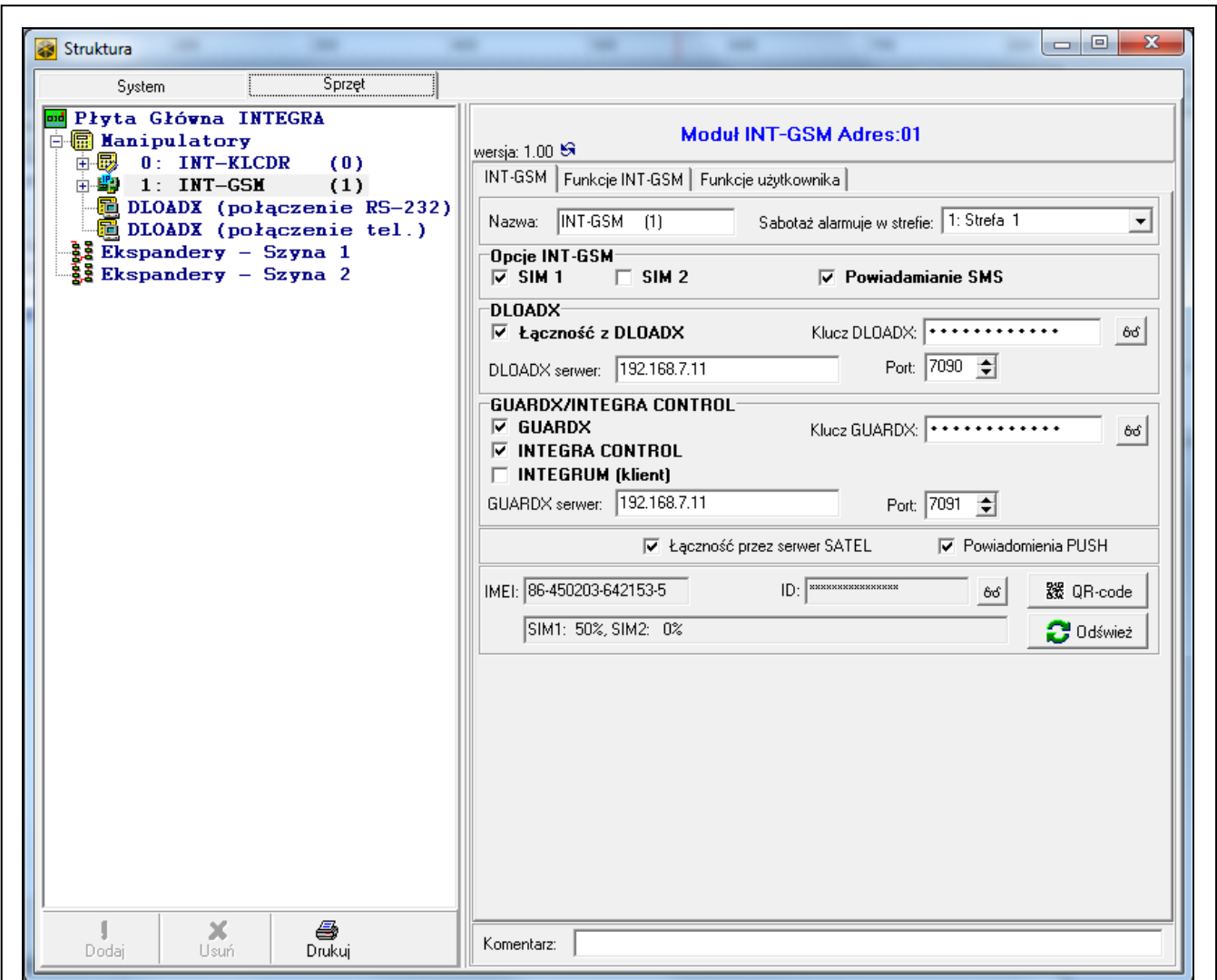


Wszystkie ustawienia możesz skonfigurować tylko przy pomocy programu DLOADX.

W instrukcji używane są nazwy parametrów i opcji z programu DLOADX. Gdy opisywany jest parametr lub opcja, w nawiasie kwadratowym znajdziesz nazwę prezentowaną na wyświetlaczu manipulatora.

5.1 INT-GSM

W rozdziale opisane zostały ustawienia modułu INT-GSM podłączonego bezpośrednio do centrali alarmowej. Opis ustawień dla modułu INT-GSM podłączonego do modułu ETHM-1 Plus znajdziesz w instrukcji modułu ETHM-1 Plus.



Rys. 9. Program DLOADX: ustawienia modułu INT-GSM podłączonego bezpośrednio do centrali INTEGRA / INTEGRA Plus.

Nazwa – indywidualna nazwa urządzenia (do 16 znaków).

Sabotaż alarmuje w strefie [Sabotaż w str.] – strefa, w której wywołany zostanie alarm w przypadku sabotażu modułu.

Opcje INT-GSM

SIM 1 / SIM 2 [SIM1 / SIM2] – jeżeli opcja jest włączona, moduł obsługuje daną kartę SIM. Opcję należy wyłączyć, jeżeli dana karta nie ma być używana. Wyłączenie opcji zapobiegnie niepotrzebnemu zgłaszaniu awarii związanych z tą kartą.

Powiadamianie SMS [Powiadam. SMS] – jeżeli opcja jest włączona, moduł może powiadamiać o zdarzeniach dotyczących systemu alarmowego przy pomocy wiadomości SMS.

DLOADX

Łączność z DLOADX [Z DLOADX] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między programem DLOADX a centralą alarmową za pośrednictwem modułu.

Klucz DLOADX [Klucz DLOADX] – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do kodowania danych podczas komunikacji z programem DLOADX za pośrednictwem modułu.

DLOADX serwer [Adres DLOADX] – adres komputera z programem DLOADX. Jeżeli komputer ten nie znajduje się w tej samej sieci lokalnej, musi to być adres publiczny. Można wpisać adres IP lub nazwę domeny.



W manipulatorze funkcja służąca do zaprogramowania adresu komputera z programem DLOADX znajduje się w menu użytkownika w podmenu ZMIANA OPCJI (dostępna jest dla serwisu i administratorów).

Port [Port DLOADX] – numer portu TCP używanego do komunikacji z programem DLOADX. Możesz wprowadzić wartość z zakresu od 1 do 65535. Musi ona być różna od wprowadzonej dla pozostałych portów. Domyślnie: 7090.

GUARDX / INTEGRA CONTROL

GUARDX [Z GUARDX] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między programem GUARDX a centralą alarmową za pośrednictwem modułu. Opcja jest niedostępna, gdy włączona jest opcja „INTEGRUM (klient)”.

INTEGRA CONTROL [Z GSM] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między aplikacją INTEGRA CONTROL a centralą alarmową za pośrednictwem modułu. Połączenie zestawiane jest przez serwer SATEL. Opcja jest niedostępna, gdy włączona jest opcja „INTEGRUM (klient)”.

INTEGRUM (klient) [INTEGRUM] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między systemem INTEGRUM (wersja 2.0 lub nowsza) a centralą alarmową za pośrednictwem modułu. Gdy opcja jest włączona, opcje „GUARDX” i „INTEGRA CONTROL” są niedostępne.

GUARDX serwer [Adres GUARDX] – adres komputera z programem GUARDX lub serwera INTEGRUM. Jeżeli komputer ten nie znajduje się w tej samej sieci lokalnej, musi to być adres publiczny. W przypadku komputera z programem GUARDX można wpisać adres IP lub nazwę domeny. Dla serwera systemu INTEGRUM należy wpisać nazwę domeny (np. integrum.ip.com).



W manipulatorze funkcja służąca do zaprogramowania adresu komputera z programem GUARDX / serwera systemu INTEGRUM znajduje się w menu użytkownika w podmenu ZMIANA OPCJI (dostępna jest dla serwisu i administratorów).

Klucz GUARDX [Klucz pozostałe] – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do kodowania danych podczas komunikacji z:

- programem GUARDX,
- aplikacją INTEGRA CONTROL,
- systemem INTEGRUM.

Port [Port pozostałe] – numer portu TCP używanego do komunikacji z:

- programem GUARDX,
- aplikacją INTEGRA CONTROL,
- systemem INTEGRUM.

Możesz wprowadzić wartość z zakresu od 1 do 65535. Musi ona być różna od wprowadzonej dla pozostałych portów. Domyślnie: 7091.

Serwer SATEL

Łączność przez serwer SATEL [Serwer SATEL] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia za pośrednictwem serwera SATEL (Usługa Zestawiania Połączeń).

Powiadomienia PUSH [Powiadom. PUSH] – jeżeli opcja jest włączona, aplikacja INTEGRA CONTROL może informować o zdarzeniach przy pomocy powiadomień push. Opcja jest dostępna, gdy w module włączona jest komunikacja z serwerem SATEL.

Informacje

IMEI – indywidualny numer identyfikacyjny telefonu GSM.

ID – indywidualny numer identyfikacyjny przydzielony modułowi INT-GSM przez serwer SATEL.



Jeżeli moduł ma zostać użyty w innym systemie alarmowym, skasuj dotychczasowy numer ID. Należy to zrobić po podłączeniu modułu do nowej centrali i nawiązaniu połączenia z serwerem SATEL, przy pomocy funkcji ZMIEN ID dostępnej w manipulatorze (►TRYB SERWISOWY ►STRUKTURA ►SPRZĘT ►MANIPULATORY ►USTAWIENIA ►[nazwa modułu] ►ZMIEN ID). Po skasowaniu dotychczasowego numeru ID moduł otrzyma nowy. Aplikacje INTEGRA CONTROL używające starego numeru ID nie będą mogły połączyć się z centralą.

[Sygnał GSM] – informacja o poziomie sygnału GSM.



– kliknij, aby otworzyć okno, w którym prezentowany jest kod QR. Kod QR zawiera informacje wymagane podczas konfigurowania ustawień dotyczących komunikacji przez serwer SATEL. Kod QR można odczytać przy pomocy urządzenia mobilnego lub wyeksportować do pliku w formacie JPEG i przekazać użytkownikom. Kod QR upraszcza konfigurowanie ustawień aplikacji INTEGRA CONTROL.

Odśwież – kliknij, aby odświeżyć wszystkie informacje.

5.2 Funkcje INT-GSM



Ustawienia konfigurowane w zakładce „Funkcje INT-GSM” przechowywane są w pamięci modułu. Przed rozpoczęciem konfigurowania kliknij na przycisk „Odczyt”, a po zakończeniu konfigurowania – na przycisk „Zapis”. Ustawienia te nie są

odczytywane / zapisywane po kliknięciu na przycisk  w menu głównym programu DLOADX.

Przyciski

Odczyt – kliknij, żeby odczytać ustawienia z modułu.

Zapis – kliknij, żeby zapisać ustawienia do modułu.

Przerwij – kliknij, żeby przerwać odczyt lub zapis ustawień.

Reset – kliknij, żeby skasować ustawienia (przywrócić ustawienia fabryczne).

5.2.1 Telefon GSM

SIM 1 / SIM 2

PIN – kod PIN karty SIM.

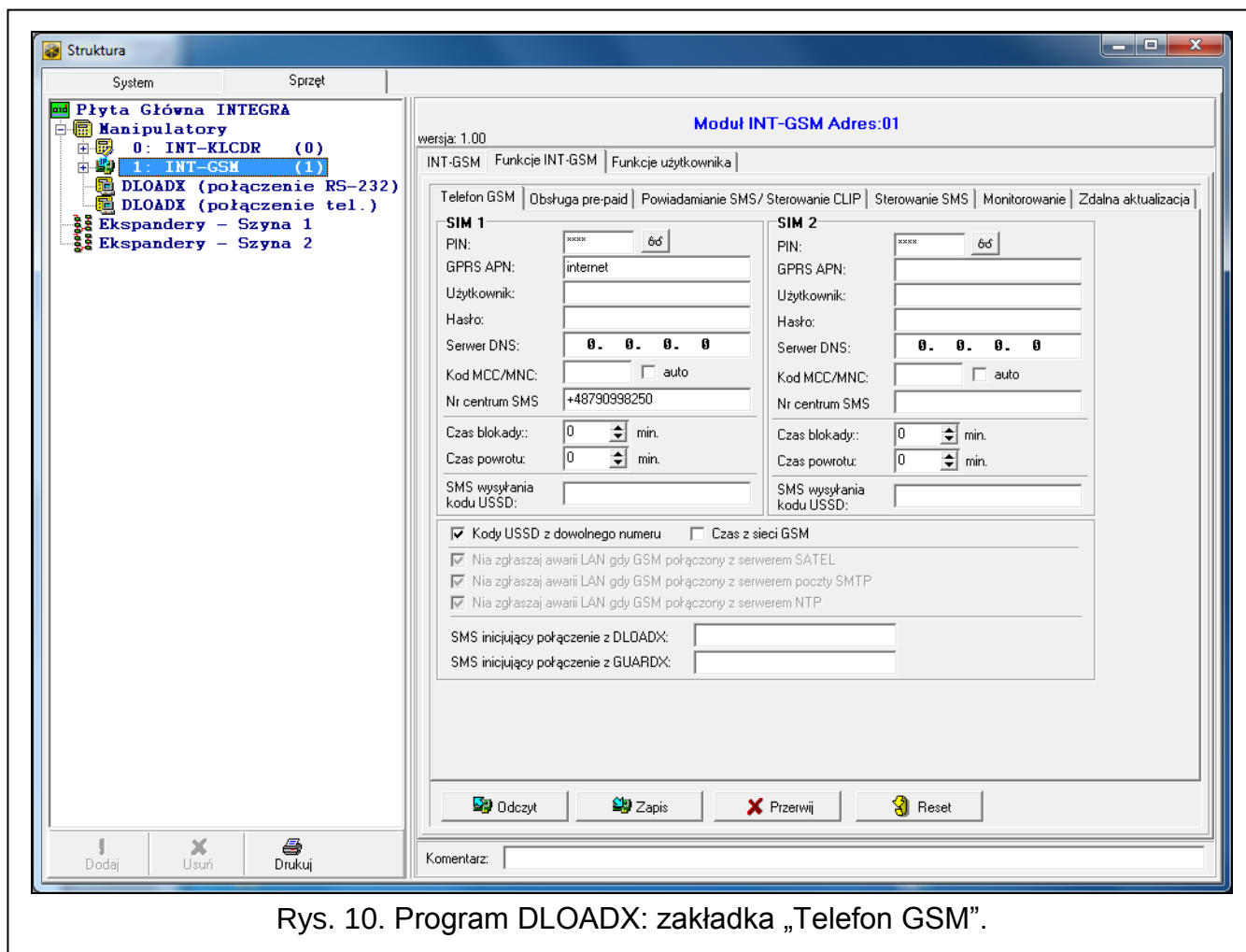


Jeżeli zaprogramowany zostanie błędny kod PIN, moduł zgłosi awarię. Po trzeciej próbie użycia błędnego kodu PIN, karta SIM zostanie zablokowana. W celu odblokowania karty SIM należy przełożyć ją do telefonu komórkowego i wprowadzić kod PUK.

GPRS APN – nazwa punktu dostępu dla połączenia Internet GPRS.

Użytkownik – nazwa użytkownika dla połączenia Internet GPRS.

Hasło – hasło dla połączenia Internet GPRS.



Rys. 10. Program DLOADX: zakładka „Telefon GSM”.

Serwer DNS – adres IP serwera DNS, którego ma używać moduł. Jeżeli adres został zapisany przez operatora w pamięci karty SIM, nie trzeba go programować. W innym przypadku zaleca się zaprogramowanie adresu IP serwera DNS. Jest on niezbędny, w przypadku przesyłania danych w technologii GPRS, gdy adres urządzenia, z którym moduł ma się połączyć (stacja monitorująca, komputer z programem DLOADX lub GUARDX, serwer INTEGRUM), podany został w formie nazwy.



Parametry GPRS można uzyskać od operatora sieci GSM.

Kod MCC/MNC – kody operatora sieci GSM, do której ma się logować karta SIM. Wprowadź kolejno:

- MCC (Mobile Country Code) – kod kraju (np. 260 – Polska),
- MNC (Mobile Network Code) – kod operatora (np. dla Polski: 01 – Plus; 02 – T-Mobile; 03 – Orange; 06 i 98 – Play; 07 – Netia).

Pamiętaj, że wpisanie niewłaściwych danych może uniemożliwić logowanie do sieci GSM. Jeśli nie wprowadzisz kodu, moduł będzie się logował do dostępnej sieci GSM.

auto – jeżeli opcja jest włączona, gdy moduł nie będzie mógł się zalogować do sieci GSM operatora określonego przy pomocy kodu MCC/MNC, zaloguje się do dostępnej sieci GSM.

Nr centrum SMS – numer telefoniczny centrum zarządzającego wiadomościami SMS. Pośredniczy ono przy przesyłaniu wiadomości SMS. Jeżeli numer został zapisany przez operatora w pamięci karty SIM, nie trzeba go programować. W innym przypadku, jeżeli moduł ma wysyłać wiadomości SMS, należy go wprowadzić. Numer musi być odpowiedni dla operatora sieci, w jakiej zarejestrowana jest karta SIM.

Czas blokady – czas, przez który niemożliwe jest przełączenie na drugą kartę SIM. Odliczany jest od momentu przełączenia na daną kartę. W przypadku monitorowania, tory transmisji zaprogramowane jako następne w kolejności, jeżeli będą wymagały przełączenia na drugą kartę, będą w trakcie odliczania czasu blokady pomijane. Wprowadzenie wartości 0 oznacza, że możliwe jest natychmiastowe przełączenie na drugą kartę SIM.

Czas powrotu – czas, po którym ma być używana druga karta SIM. Wprowadzenie wartości 0 oznacza, że nie nastąpi automatyczne przełączenie na drugą kartę SIM.



Jeżeli mają być używane dwie karty SIM, jedna z nich powinna być traktowana jako priorytetowa. Zaleca się zaprogramowanie dla niej czasu powrotu równego 0.

SMS wysyłania kodu USSD – polecenie sterujące, które będzie wysyłane w wiadomości SMS razem z kodem USSD. Moduł wykona kod USSD, a uzyskaną od operatora odpowiedź odeśle na numer telefonu, z którego wysłana została wiadomość SMS z poleceniem sterującym. Możesz wprowadzić do 16 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Treść polecenia musi być różna od treści innych poleceń SMS sterujących centralą.

Wiadomość SMS z kodem USSD powinna mieć postać: „xxxxxx=yyyy=”, gdzie: „xxxxxx” - polecenie sterujące, „yyyy” – kod USSD obsługiwany przez operatora sieci.

Nie zaleca się korzystania z zaawansowanych funkcji dostępnych dzięki usłudze USSD, gdy w odpowiedzi na wprowadzony kod prezentowane jest menu.

Polecenie sterujące wysyłaniem kodów USSD może być używane do wysyłania wiadomości SMS za pośrednictwem modułu.

Kod USSD z dowolnego numeru – jeżeli opcja jest włączona, polecenie sterujące służące do przesyłania kodów USSD lub sprawdzenia stanu konta karty SIM (patrz: „SMS sterujący sprawdz. środków” s. 15) może być wysłane z dowolnego telefonu. Jeżeli opcja jest wyłączona, polecenie może być wysłane tylko z telefonu, którego numer jest zapisany w module (patrz: „Powiadamianie SMS / Sterowanie CLIP” s. 16).

Czas z sieci GSM – jeżeli opcja jest włączona, zegar centrali może być synchronizowany z czasem operatora sieci GSM.

Nie zgłaszaj awarii LAN gdy GSM połączony z serwerem SATEL – opcja dostępna, jeżeli moduł INT-GSM podłączony jest do modułu ETHM-1 Plus. Jeżeli opcja jest włączona, brak sieci Ethernet nie wywoła awarii, gdy uda się połączyć z serwerem SATEL za pośrednictwem modułu INT-GSM (GPRS).

Nie zgłaszaj awarii LAN gdy GSM połączony z serwerem poczty SMTP – opcja dostępna, jeżeli moduł INT-GSM podłączony jest do modułu ETHM-1 Plus. Jeżeli opcja jest włączona, brak sieci Ethernet nie wywoła awarii, gdy uda się połączyć z serwerem SMTP za pośrednictwem modułu INT-GSM (GPRS).

Nie zgłaszaj awarii LAN gdy GSM połączony z serwerem NTP – opcja dostępna, jeżeli moduł INT-GSM podłączony jest do modułu ETHM-1 Plus. Jeżeli opcja jest włączona, brak sieci Ethernet nie wywoła awarii, gdy uda się połączyć z serwerem NTP za pośrednictwem modułu INT-GSM (GPRS).

SMS

SMS inicjujący połączenie z DLOADX – polecenie sterujące, którego wysyłanie w wiadomości SMS zainicjuje łączność między centralą alarmową a programem DLOADX za pośrednictwem:

- modułu INT-GSM podłączonego do centrali (GPRS),

- modułu ETHM-1 Plus, do którego podłączony jest moduł INT-GSM (Ethernet). Jeżeli nie uda się nawiązać połączenia przez Ethernet, podjęta zostanie próba nawiązania komunikacji przez GPRS.

Możesz wprowadzić do 16 znaków alfanumerycznych (cyfry, litery i znaki specjalne).

SMS inicjujący połączenie z GUARDX – polecenie sterujące, którego wysyłanie w wiadomości SMS zainicjuje łączność między centralą alarmową a programem GUARDX za pośrednictwem:

- modułu INT-GSM podłączonego do centrali (GPRS),
- modułu ETHM-1 Plus, do którego podłączony jest moduł INT-GSM (Ethernet). Jeżeli nie uda się nawiązać połączenia przez Ethernet, podjęta zostanie próba nawiązania komunikacji przez GPRS.

Możesz wprowadzić do 16 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Treść poleceń sterujących musi być różna.

Treść jednego polecenia sterującego nie powinna znaleźć się w treści innego polecenia.

*W wiadomości SMS można umieścić adres komputera, z którym moduł ma się połączyć, i numer portu TCP, który ma zostać użyty do komunikacji. Wiadomość taka powinna mieć postać: **xxxx=aaaa:pp=** („xxxx” – polecenie sterujące; „aaaa” – adres komputera (adres IP lub nazwa domeny); „pp” – numer portu).*

5.2.2 Obsługa PRE-PAID

SIM 1 / SIM 2

Kod USSD spr. konta – kod USSD, który służy do sprawdzenia stanu konta karty SIM. Jeżeli zostanie zaprogramowany, moduł będzie mógł kontrolować ilość środków na koncie karty SIM.

Min. ilość środków – minimalna ilość środków na koncie karty SIM. Jeżeli ilość środków spadnie poniżej minimum:

- wywołana zostanie awaria,
- gdy moduł sprawdza stan konta karty SIM automatycznie, informacja o stanie konta zostanie przesłana jako wiadomość SMS na telefony do powiadamiania SMS / sterowania CLIP, dla których włączona jest opcja „SMS>>” (patrz: „Powiadamianie SMS / Sterowanie CLIP” s. 16).

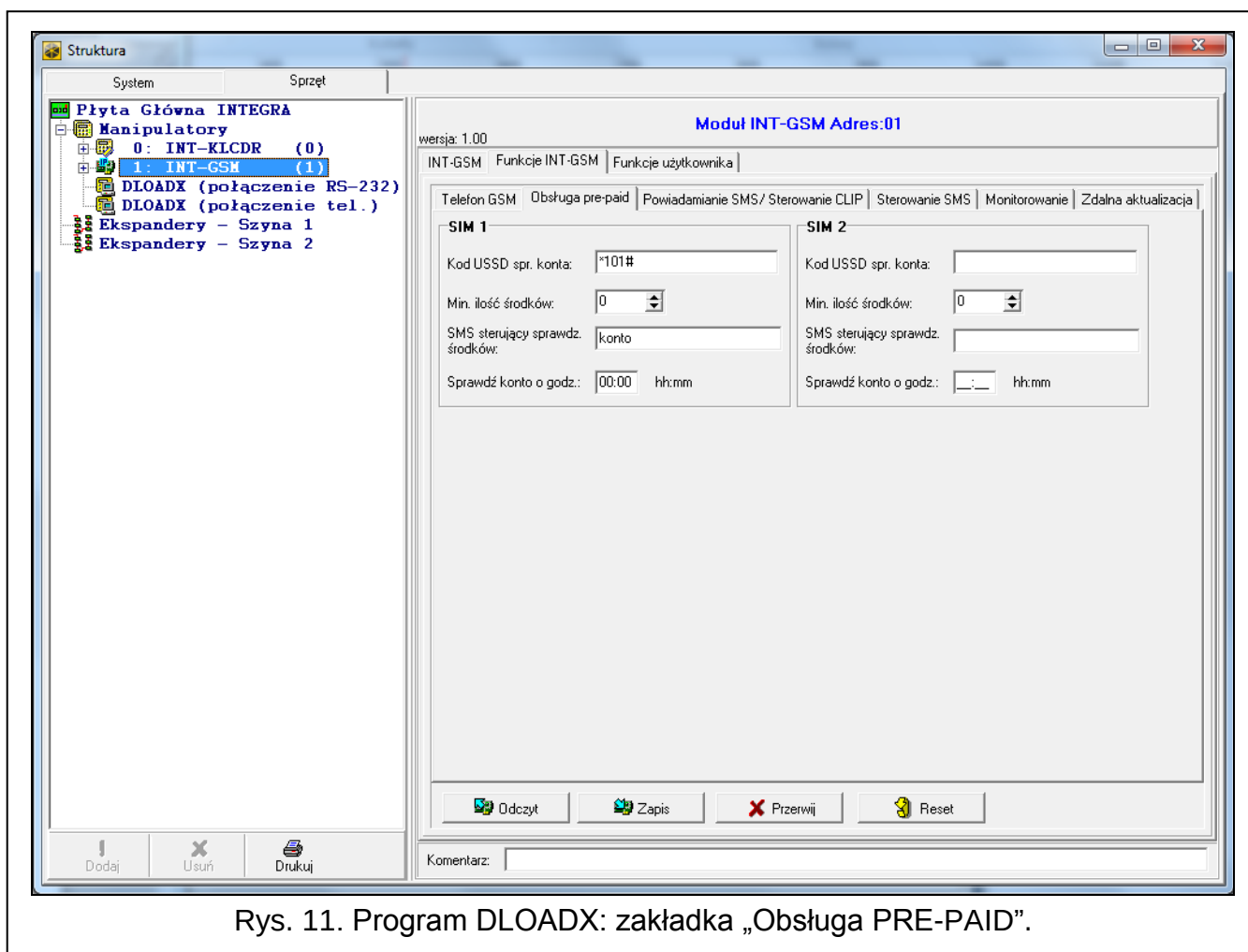
Jeżeli wprowadzisz 0, wyłączysz sprawdzanie.

SMS sterujący sprawdz. środków – polecenie sterujące, którego wysyłanie w wiadomości SMS uruchomi funkcję sprawdzenia stanu konta karty SIM. Moduł wykona kod USSD zaprogramowany w polu „Kod USSD spr. konta”, a uzyskaną od operatora odpowiedź odeśle na numer telefonu, z którego wysłane zostało polecenie sterujące. Możesz wprowadzić do 16 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Jeżeli w module włączona jest opcja „Powiadomienia PUSH”, to powiadomienie o stanie konta karty SIM na którym nie ma środków na wysłanie wiadomości SMS, ale są środki na usługę Internetu, zostanie zrealizowane w formie wiadomości push (w telefonie musi być zainstalowana aplikacja INTEGRA CONTROL).

Sprawdź konto o godz. – godzina, o której moduł będzie sprawdzał stan konta karty SIM. Jeżeli nie wprowadzisz wartości, wyłączysz sprawdzanie.



Rys. 11. Program DLOADX: zakładka „Obsługa PRE-PAID”.

5.2.3 Powiadamianie SMS / Sterowanie CLIP

Możesz zaprogramować 16 numerów telefonów, na które moduł może realizować powiadomienia SMS o zdarzeniach w systemie alarmowym. Treść wiadomości SMS generowana jest automatycznie na podstawie opisów z pamięci zdarzeń centrali alarmowej.

Jeżeli do numeru telefonu przypisany zostanie użytkownik centrali alarmowej, z telefonu tego będzie można sterować centralą przy pomocy CLIP i wiadomości SMS.

Dodatkowo możesz wskazać użytkownika centrali, który będzie mógł sterować centralą z dowolnego numeru telefonu. Zaleca się utworzenie w centrali użytkownika, który będzie miał uprawnienia dostosowane do wymagań sterowania SMS/CLIP, a nie do codziennej obsługi systemu alarmowego.

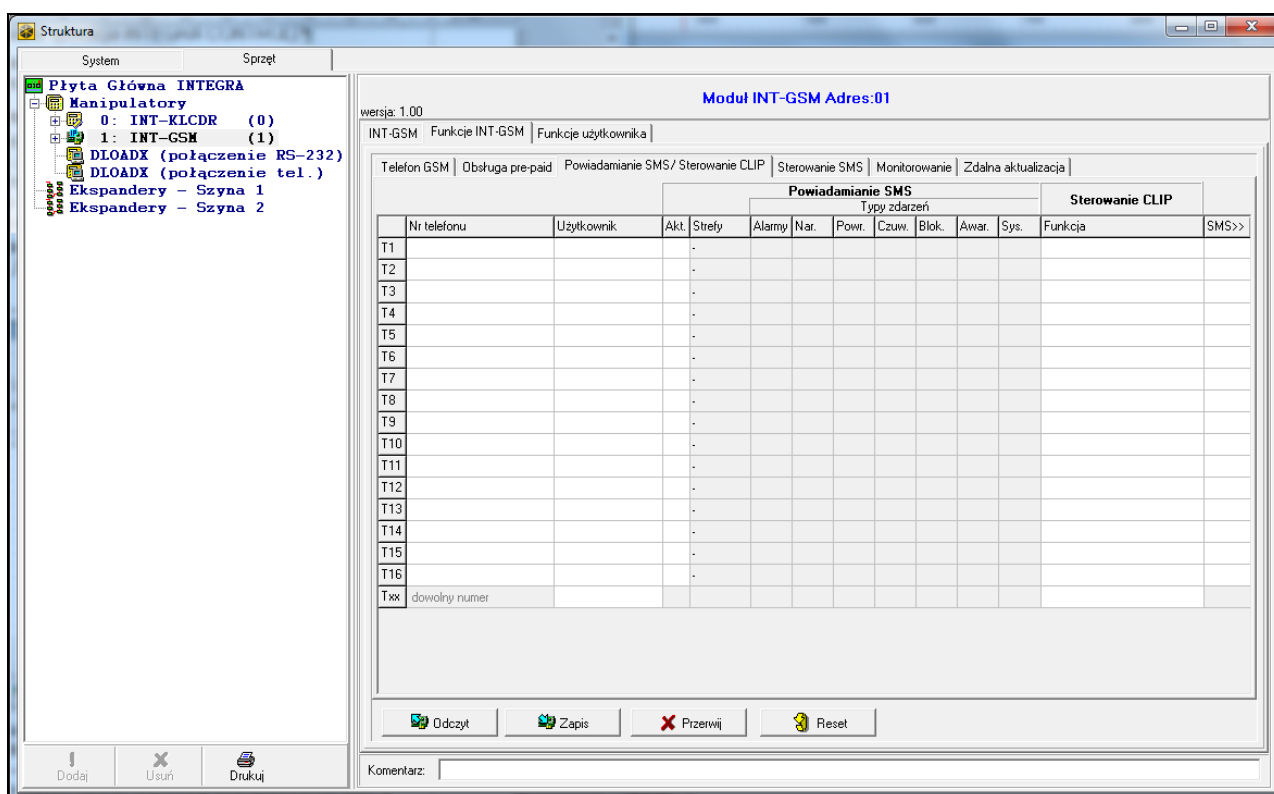
Moduł może powiadamiać o zdarzeniach przy pomocy wiadomości SMS, gdy w ustawieniach modułu włączona jest opcja „Powiadamianie SMS”.

Nr telefonu – numer telefonu, na który moduł będzie realizował powiadomienia SMS.

Użytkownik – użytkownik centrali alarmowej. Jeżeli dla danego numeru (w tym dowolnego numeru telefonu – wiersz Txx) określisz użytkownika, to z numeru tego będzie można sterować centralą alarmową przy pomocy CLIP (patrz: „Sterowanie CLIP” s. 17) i wiadomości SMS (patrz: „Sterowanie SMS” s. 18). Wprowadź numer użytkownika lub kliknij na przycisk , aby wybrać użytkownika z listy.



Z numeru telefonu, dla którego został określony użytkownik można również przy pomocy wiadomości SMS zainicjować pobieranie nowego oprogramowania oraz aktualizację oprogramowania modułu (patrz: „Zdalna aktualizacja” s. 21).



Rys. 12. Program DLOADX: zakładka „Powiadamianie SMS / Sterowanie CLIP”.

Powiadamianie SMS

Akt. – jeżeli opcja jest włączona, moduł może powiadamiać o zdarzeniach dany telefon.

Strefy – określ, o zdarzeniach w jakich strefach będzie powiadamiany dany numer telefonu. Kliknij na przycisk, aby otworzyć listę stref. Gdy lista się wyświetli, kliknij dwukrotnie w numer strefy, aby ją wybrać. Jeżeli nie określisz strefy, numer nie będzie powiadamiany o zdarzeniach.

Typy zdarzeń – określ, o jakiego typu zdarzeniach będzie powiadamiany dany numer telefonu. Kliknij dwukrotnie na pole, aby wybrać typ zdarzenia.

Sterowanie CLIP

CLIP oznacza dzwonenie bez nawiązania połączenia (po usłyszeniu sygnału dzwonka należy odłożyć słuchawkę), czyli bez ponoszenia kosztów. Moduł zidentyfikuje numer telefonu dzwoniącego i odpowiednio zareaguje.

W wierszach od T1 do T16 możesz zaprogramować funkcję uruchamianą przy pomocy CLIP z danego numeru telefonu. Dodatkowo w wierszu Txx możesz zaprogramować jedną funkcję, którą będzie można uruchomić w centrali przy pomocy CLIP z dowolnego numeru telefonu. W obydwu przypadkach numer telefonu musi być przypisany do użytkownika centrali.



Numery telefonów zaprogramowane w wierszach do T1 do T16 nie są traktowane przez moduł jako numery dowolne.

Funkcja – funkcja, którą uruchomi CLIP. Wprowadź numer funkcji lub kliknij na przycisk , aby wybrać funkcję z listy. Lista dostępnych funkcji definiowana jest w zakładce „Sterowanie SMS” (patrz: „Funkcja” s. 18).

Przełącz SMS

SMS>> – jeżeli opcja jest włączona, na dany numer telefonu przesyłane są odebrane przez moduł nieznanne wiadomości SMS (np. informacje otrzymywane od operatora sieci GSM).

5.2.4 Sterowanie SMS

Moduł umożliwia sterowanie systemem alarmowym przy pomocy wiadomości SMS zawierających odpowiednie polecenia sterujące. Wiadomości SMS należy wysyłać na numer karty SIM. W module możesz zaprogramować 32 polecenia sterujące.

SMS sterujący – polecenie sterujące, którego wysłanie w wiadomości SMS uruchomi w centrali funkcję wybraną w polu „Funkcja”. Możesz wprowadzić do 16 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Treść poleceń sterujących powinna być różna.

Treść jednego polecenia sterującego nie powinna znaleźć się w treści innego polecenia.

W jednej wiadomości SMS możesz umieścić kilka poleceń sterujących rozdzielając je spacjami.

Polecenie sterujące może stanowić tylko fragment wiadomości SMS. Dzięki temu w pamięci telefonu możesz zapisać polecenie sterujące wraz z komentarzem i całość wysłać do modułu.

Funkcja – funkcja uruchamiana po odebraniu polecenia sterującego w wiadomości SMS lub przy pomocy CLIP (patrz: „Sterowanie CLIP” s. 17). Jeżeli zaprogramujesz funkcję bez definiowania polecenia sterującego (pole „SMS sterujący”), to będzie można ją uruchomić tylko przy pomocy CLIP. Wprowadź numer funkcji lub kliknij na przycisk , aby wybrać funkcję z listy:

1: Status (tekst)

2: Status (symb.)

3: Załącz czuwanie (0) – pełne czuwanie.

4: Załącz czuwanie (1) – pełne czuwanie + blokady.

5: Załącz czuwanie (2) – czuwanie bez wewnętrznych.

6: Załącz czuwanie (3) – czuwanie bez wewnętrznych i bez czasu na wejście.

7: Wyłącz czuwanie

8: Kasuj alarm

9: Włącz wyjścia

10: Wyłącz wyjścia

11: Przełącz wyjścia

12: Blokuj wejścia

13: Blokuj trwale we.

14: Odblokuj we.

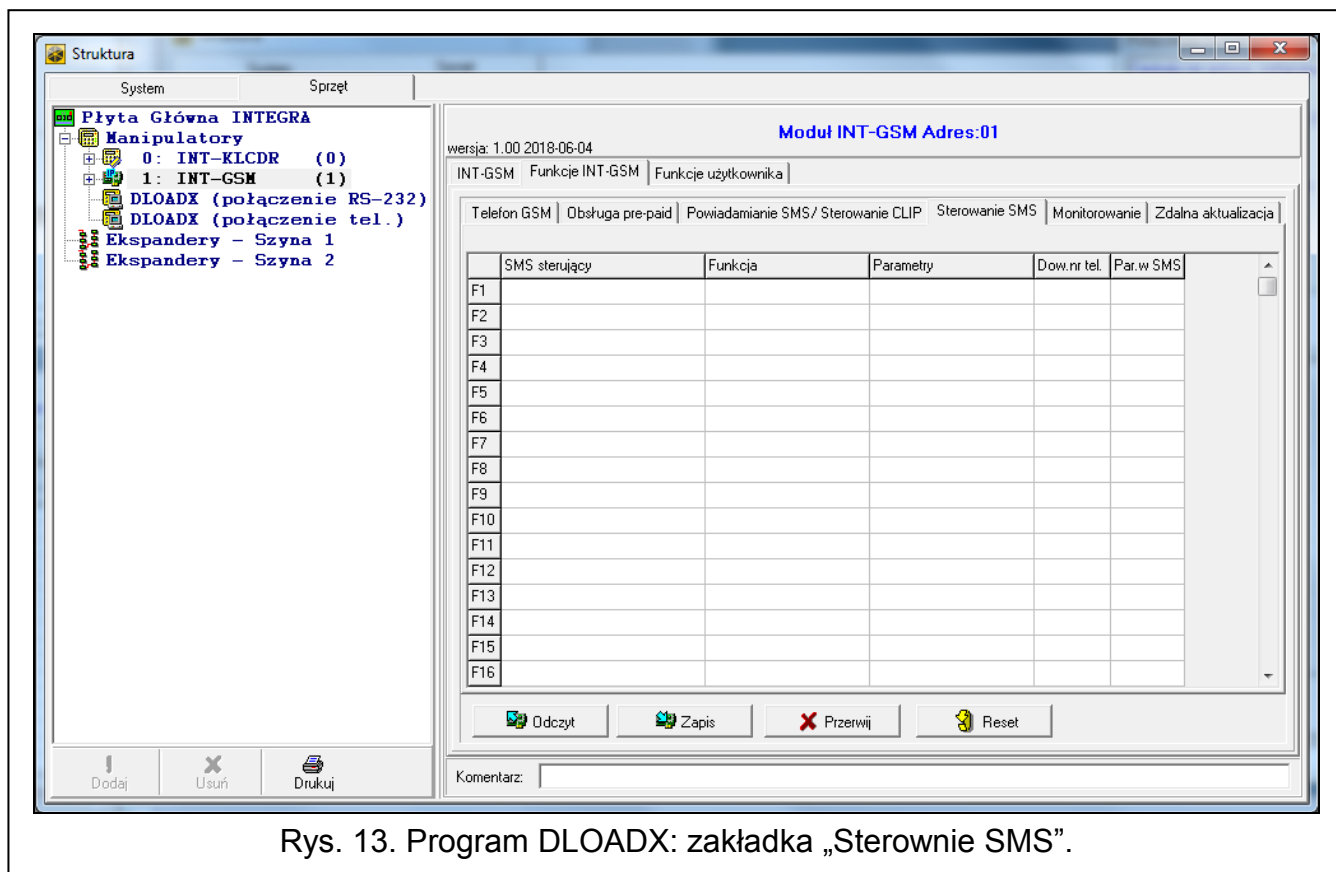
15: Narusz wejście



Strefy muszą być sterowane hasłem użytkownika.

Wejścia, które mają być blokowane, nie mogą mieć włączonej opcji “Użytkownik nie blokuje”.

Wyjścia muszą być typu 24. PRZEŁĄCZNIK MONO, 25. PRZEŁĄCZNIK BI, 105. ROLETA W GÓRĘ, 106. ROLETA W DÓŁ lub PRZEKAŹNIK TELEFONICZNY.



Rys. 13. Program DLOADX: zakładka „Sterownie SMS”.

Parametry – określ, z jakimi parametrami uruchomi się dana funkcja. Kliknij na przycisk , aby otworzyć listę parametrów. Gdy lista się wyświetli, kliknij dwukrotnie w numer, aby wybrać strefę / wyjście / wejście (w przypadku funkcji „15: Naruszyć wejście” możesz wybrać tylko jedno wejście).

Dow.nr tel. – jeżeli opcja jest włączona, dana funkcja może być uruchomiona z dowolnego numeru telefonu. Sterowanie centralą z dowolnego numeru telefonu jest możliwe, gdy w zakładce „Powiadomianie SMS / Sterowanie CLIP” dla dowolnego numeru telefonu został wybrany użytkownik centrali alarmowej (patrz: „Użytkownik” s. 16).

Par.w SMS – jeżeli opcja jest włączona, dana funkcja może być uruchomiona z parametrami wysłanymi razem z poleceniem sterującym w wiadomości SMS. Pozwala to na uruchomienie funkcji z innymi parametrami niż te, które zostały zaprogramowane dla niej w polu „Parametry”. Wiadomość SMS musi mieć wówczas postać: „xxxxxx=a,b,c,d=”, gdzie: „xxxxxx” - polecenie sterujące, „a,b,c,d” - parametry, np. 1,2,3, 4 (numery stref / wyjść / wejść oddzielone przecinkami). W przypadku funkcji „15: Naruszyć wejście” polecenie sterujące musi mieć postać: „xxxxxx=a=”, gdzie: „xxxxxx” - polecenie sterujące, „a” – numer wejścia, np. 1 (można wskazać tylko jedno wejście).

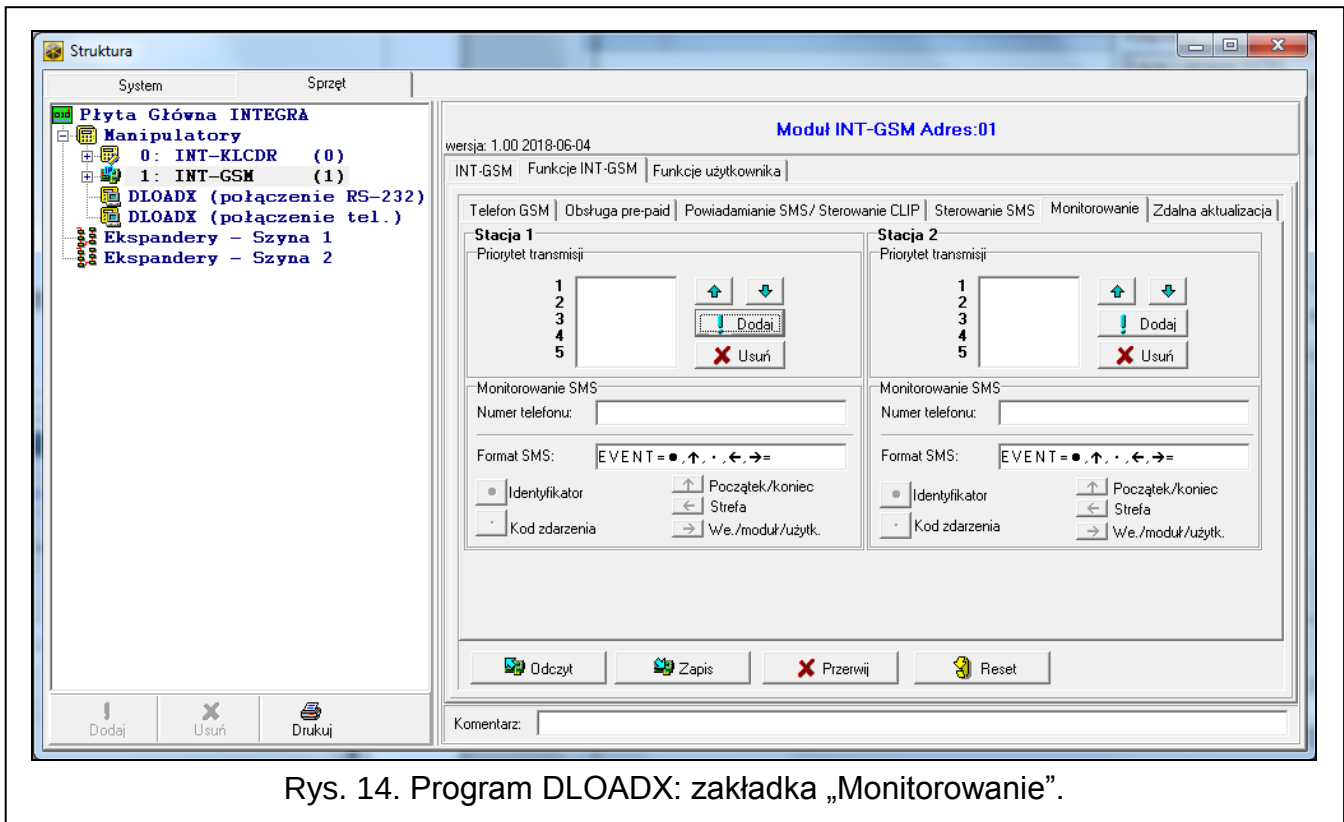
5.2.5 Monitorowanie

Moduł umożliwia centrali alarmowej wysyłanie kodów zdarzeń do stacji monitorującej poniższymi torami transmisji:

- GPRS,
- wiadomości SMS (brak potwierdzenia odebrania kodów zdarzeń).



Współpraca modułu INT-GSM z modułem ETHM-1 Plus umożliwia realizowanie monitoringu dwutorowego (Dual Path Reporting) zgodnego z normą EN 50136. Informacje na temat konfigurowania monitoringu dwutorowego znajdują się w instrukcjach programowania central alarmowych.



Rys. 14. Program DLOADX: zakładka „Monitorowanie”.

Stacja 1 / Stacja 2

Priorytet transmisji

W przypadku niepowodzenia przesłania kodu zdarzenia do stacji monitorującej jednym torem transmisji, moduł może skorzystać z innego toru transmisji. Należy określić kolejność, według której moduł będzie używał różnych torów transmisji. Pomyślne przesłanie zdarzenia do stacji monitorującej przerwie procedurę (wyjątkiem są transmisje testowe).



Moduł używa tylko tych torów transmisji, dla których określony został priorytet (umieszczone są na liście określającej kolejność używania torów transmisji).

Jeżeli moduł INT-GSM jest podłączony do modułu ETHM-1 Plus, należy określić priorytet także dla transmisji przez Ethernet (ETHM).

W przypadku monitoringu SMS, moduł nie otrzymuje potwierdzenia odebrania kodów zdarzeń przez stację monitorującą, dlatego ten tor transmisji powinien być używany jako ostatni w kolejności.

Przełączenie się z jednej karty SIM na drugą wymaga czasu (m.in. ze względu na czas logowania do sieci), dlatego lepiej najpierw wykorzystać wszystkie tory transmisji dostępne dla jednej karty SIM.

Wpływ na przełączanie się z jednej karty SIM na drugą mają parametry „Czas blokady” i „Czas powrotu” (patrz: „Telefon GSM” s. 12).

Monitorowanie SMS

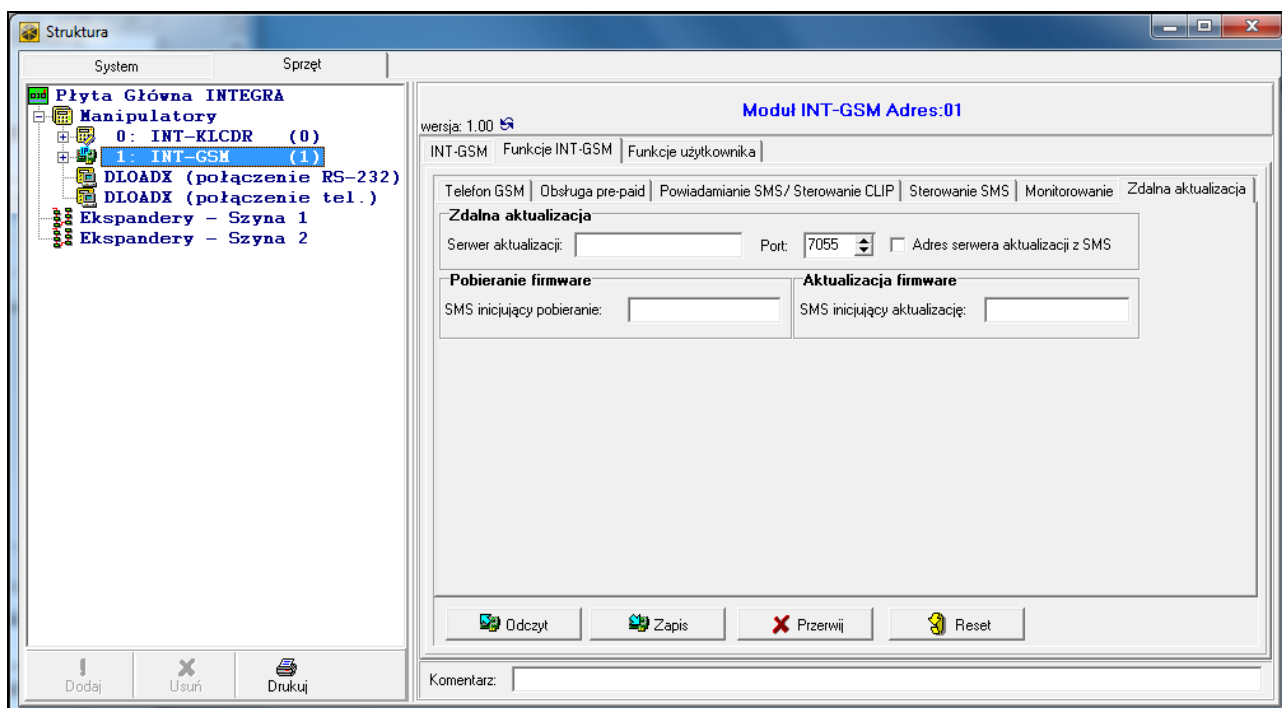
Numer telefonu – numer telefonu stacji monitorującej dla monitoringu SMS.

Format SMS – format wiadomości SMS dla monitoringu SMS. Musi zostać zdefiniowany zgodnie z wymaganiami stacji monitorującej. Zaprogramowany domyślnie w module

format wiadomości SMS odpowiada domyślnym ustawieniom stacji monitorującej STAM-2 (wersja programu 1.2.0 lub nowsza) dla formatu Contact ID.

5.2.6 Zdalna aktualizacja

Zdalną aktualizację oprogramowania modułu umożliwia serwer aktualizacji „UpServ”, który znajduje się w ofercie firmy SATEL.



Rys. 15. Program DLOADX: zakładka „Zdalna aktualizacja”.

Serwer aktualizacji – adres serwera aktualizacji „UpServ”. Możesz wpisać adres IP lub nazwę domeny.

Port – numer portu TCP używanego do komunikacji z serwerem aktualizacji „UpServ”. Możesz wprowadzić wartości od 0 do 65535 (0=wyłączony).

Adres serwera aktualizacji z SMS – jeżeli opcja jest włączona, w wiadomości SMS inicjującej pobieranie oprogramowania z serwera aktualizacji można podać adres serwera i numer portu. Jeżeli opcja jest włączona, a w wiadomości SMS inicjującej pobieranie nie będzie adresu lub numeru portu, to moduł użyje zaprogramowanych ustawień.



Wiadomości SMS, które inicjują pobieranie nowego oprogramowania i aktualizację oprogramowania modułu, mogą być wysyłane tylko z telefonu, którego numer jest zapisany w module (patrz: „Powiadamianie SMS / Sterowanie CLIP” s. 16).

Pobieranie firmware



Podczas pobierania nowego oprogramowania moduł realizuje swoje normalne funkcje.

SMS inicjujący pobieranie – polecenie sterujące, którego wysłanie w wiadomości SMS uruchomi pobieranie oprogramowania z serwera. Możesz wprowadzić do 8 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Treść polecenia musi różnić się od treści pozostałych poleceń sterujących zaprogramowanych w module.

Jeżeli w module włączona jest opcja „Adres serwera aktualizacji z SMS” i chcesz, żeby moduł połączył się z innym serwerem aktualizacji, niż przewidują to ustawienia

modułu, wiadomość powinna mieć postać: **xxxx=aaaa:pp=** („xxxx” – polecenie sterujące; „aaaa” – adres serwera (adres IP lub nazwa domeny); „pp” – numer portu).

Moduł powiadamia przy pomocy wiadomości SMS, jak przebiegło pobieranie nowego oprogramowania. Powiadamiany jest telefon, z którego wysłana została wiadomość SMS inicjująca pobieranie oprogramowania.

Jeżeli w czasie pobierania nowego oprogramowania ponownie wyślesz wiadomość SMS zawierającą polecenie inicjujące pobieranie oprogramowania, moduł w odpowiedzi poinformuje o postępie pobierania (wartość procentowa).

Aktualizacja firmware



Podczas aktualizacji oprogramowania moduł nie realizuje swoich normalnych funkcji.

Przed aktualizacją oprogramowania modułu, w centrali alarmowej należy włączyć „Tryb serwisowy”. W innym przypadku uruchomienie aktualizacji spowoduje, że centrala zgłosi brak obecności modułu INT-GSM.

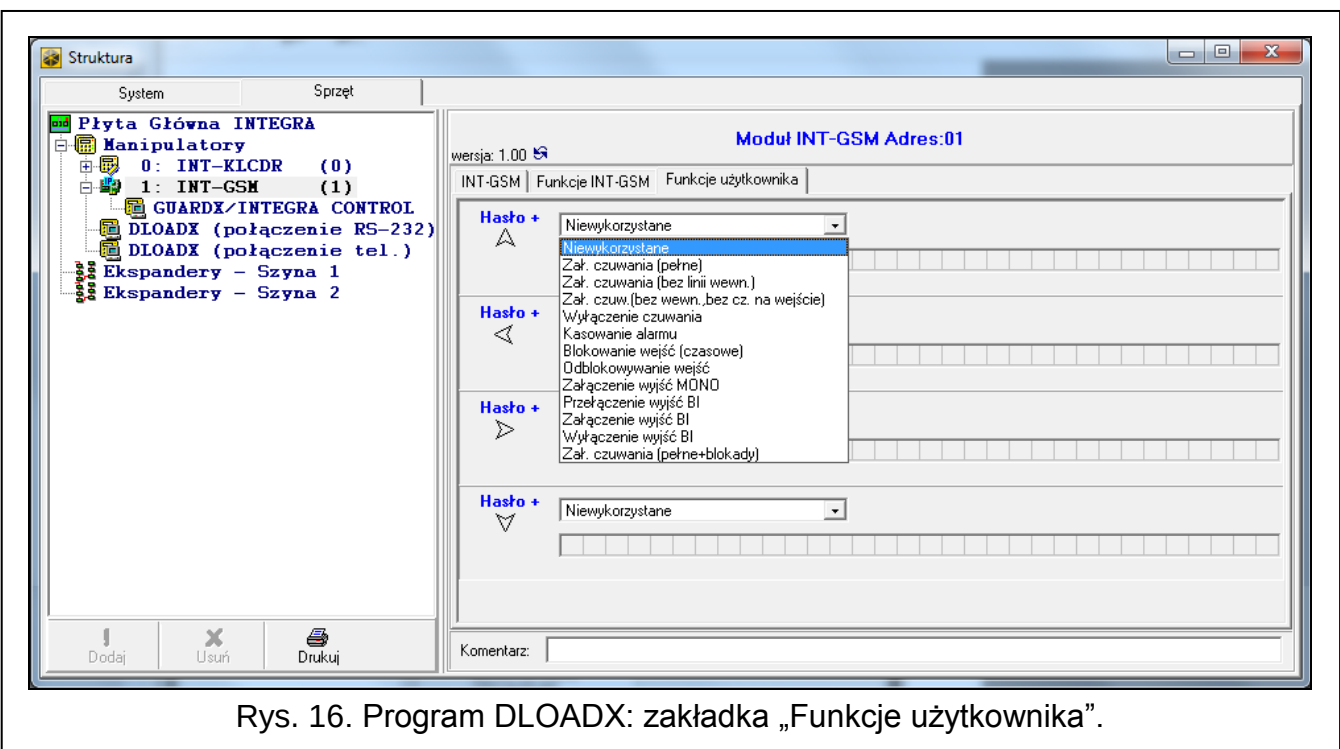
SMS inicjujący aktualizację – polecenie sterujące, którego wysłanie w wiadomości SMS uruchomi aktualizację oprogramowania. Możesz wprowadzić do 8 znaków alfanumerycznych (cyfry, litery i znaki specjalne).



Treść polecenia musi różnić się od treści pozostałych poleceń sterujących zaprogramowanych w module.

Moduł powiadamia przy pomocy wiadomości SMS, jak przebiegła aktualizacja oprogramowania. Powiadamiany jest telefon, z którego wysłana została wiadomość SMS inicjująca aktualizację oprogramowania.

5.3 Funkcje użytkownika

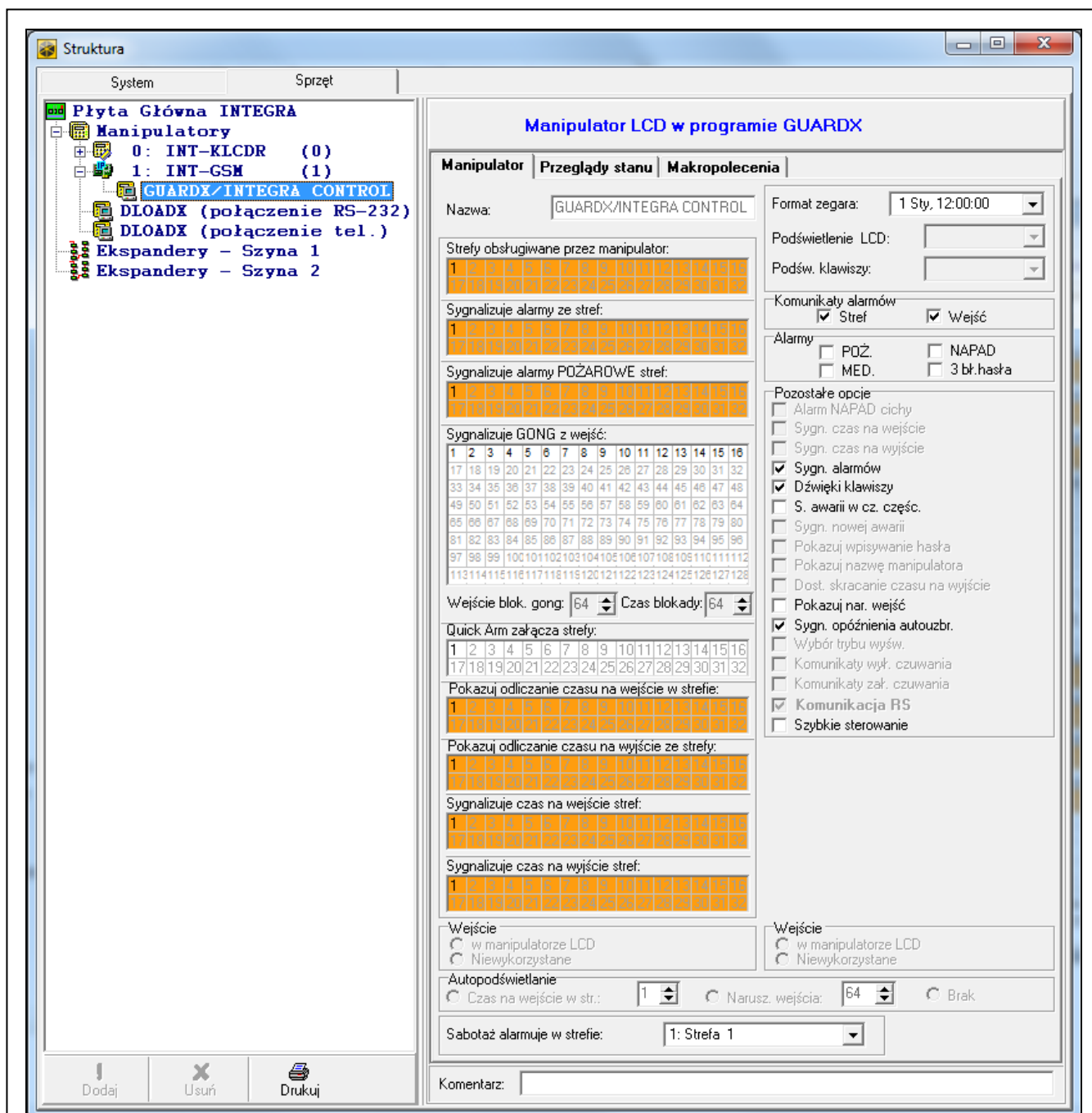


Rys. 16. Program DLOADX: zakładka „Funkcje użytkownika”.

W przypadku korzystania w urządzeniu mobilnym z aplikacji INTEGRRA CONTROL, wirtualny manipulator umożliwia szybkie uruchamianie funkcji użytkownika po wprowadzeniu hasła i naciśnięciu klawisza ze strzałką.

5.4 Wirtualny manipulator

Wirtualny manipulator pozwala obsługiwać i programować system alarmowy analogicznie, jak manipulator fizyczny. Z wirtualnego manipulatora można korzystać w programach DLOADX i GUARDX i w urządzeniu mobilnym (po zainstalowaniu aplikacji INTEGRRA CONTROL).



Rys. 17. Program DLOADX: parametry i opcje wirtualnego manipulatora dostępnego w programie GUARDX lub urządzeniu mobilnym.

Parametry i opcje wirtualnego manipulatora dostępnego w programie DLOADX można zaprogramować przy pomocy:

- programu DLOADX: okno „Struktura” → zakładka „Sprzęt” → gałąź „Manipulatory” → gałąź „DLOADX (połączenie RS-232)”,
- manipulatora: ►TRYB SERWISOWY ►STRUKTURA ►SPRZĘT ►MANIPULATORY ►USTAWIENIA ►DLOADX RS.

Ustawienia wirtualnego manipulatora dostępnego w programie GUARDX lub urządzeniu mobilnym można zaprogramować przy pomocy:

- programu DLOADX: okno „Struktura” → zakładka „Sprzęt” → gałąź „Manipulatory” → [nazwa modułu] → gałąź „GUARDX/INTEGRA CONTROL” (rys. 17),
- manipulatora: ►TRYB SERWISOWY ►STRUKTURA ►SPRZĘT ►MANIPULATORY ►USTAWIENIA ►GUARDX ADRES n [n = adres modułu].

Opis parametrów i opcji manipulatorów znajduje się w instrukcji programowania centrali alarmowej INTEGRA / INTEGRA Plus (tylko część z tych parametrów i opcji jest dostępna dla manipulatora wirtualnego).

5.5 Makropolecenia

Aplikacja INTEGRA CONTROL pozwala na sterowanie systemem alarmowym przy pomocy makropoleceń, co umożliwia szybkie i łatwe uruchamianie szeregu różnych funkcji po dotknięciu zaledwie kilku klawiszy. Makropolecenia można zdefiniować w programie DLOADX (okno „Struktura” → zakładka „Sprzęt” → gałąź „Manipulatory” → gałąź [nazwa modułu] → gałąź „GUARDX/INTEGRA CONTROL” → zakładka „Makropolecenia”).

Zdefiniowane makropolecenia mogą zostać automatycznie pobrane przez aplikację INTEGRA CONTROL po nawiązaniu połączenia z modułem INT-GSM.

Makropolecenia można wczytać do aplikacji bez nawiązywania połączenia z modułem. Plik z makropoleceniami można wyeksportować, a następnie zapisać w pamięci urządzenia mobilnego (do przeniesienia pliku można użyć karty pamięci lub skorzystać z innych rozwiązań przewidzianych dla danego urządzenia). Metoda ta pozwala aplikacji INTEGRA CONTROL na używanie makropoleceń zdefiniowanych np. dla manipulatora INT-TSG. Zamiast pliku z makropoleceniami zdefiniowanymi dla modułu INT-GSM, można wczytać plik z makropoleceniami zdefiniowanymi dla manipulatora.



Dane dotyczące makropoleceń przechowywane są w pamięci modułu. Przed przystąpieniem do definiowania makropoleceń kliknij na przycisk „Odczyt” w zakładce „Makropolecenia”, żeby odczytać dane z modułu. Po zdefiniowaniu makropoleceń, kliknij na przycisk „Zapis” w zakładce „Makropolecenia”, żeby zapisać dane do modułu. Dane dotyczące makropoleceń nie są odczytywane / zapisywane po kliknięciu



na przycisk w menu głównym programu DLOADX.

Przyciski

Odczyt – kliknij, żeby odczytać dane dotyczące makropoleceń z modułu.

Zapis – kliknij, żeby zapisać dane dotyczące makropoleceń do modułu.

Przerwij – kliknij, żeby przerwać odczyt lub zapis danych dotyczących makropoleceń.

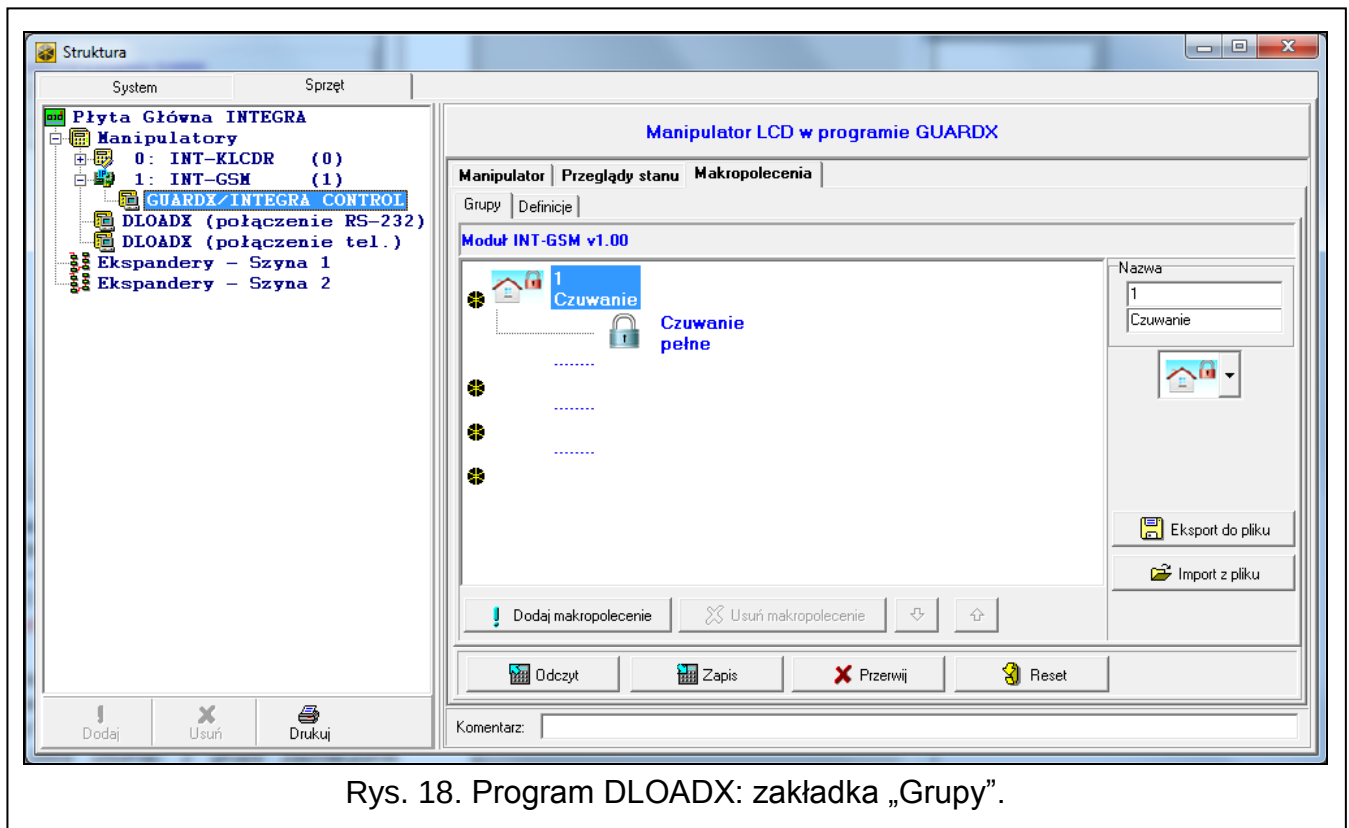
Reset – kliknij, żeby skasować wszystkie zdefiniowane makropolecenia (przywrócić ustawienia fabryczne).

5.5.1 Grupy

Makropolecenia, które mają być dostępne dla użytkowników aplikacji INTEGRA CONTROL, muszą być przypisane do jednej z czterech grup. Do grupy można przypisać do 16

makropoleceń. Program DLOADX prezentuje grupy makropoleceń i przypisane do nich makropolecenia w formie drzewa.

Nazwa – nazwa grupy makropoleceń (do 16 znaków w dwóch liniach, do 8 znaków w linii). Nazwy nie należy wprowadzać, jeśli nie ma być wyświetlana.



Rys. 18. Program DLOADX: zakładka „Grupy”.

Ikona – ikona grupy makropoleceń. Lista dostępnych ikon zostanie wyświetlona po kliknięciu na przycisk .

Dodaj makropolecenie – przycisk dostępny po kliknięciu na grupę makropoleceń. Umożliwia wyświetlenie listy zawierającej nazwy zdefiniowanych makropoleceń. Po kliknięciu na nazwę, makropolecenie zostanie dodane do grupy.

Usuń makropolecenie – przycisk dostępny po kliknięciu na dowolne makropolecenie. Umożliwia usunięcie tego makropolecenia z grupy.



– kliknij, żeby przesunąć zaznaczone makropolecenie w ramach grupy w dół.



– kliknij, żeby przesunąć zaznaczone makropolecenie w ramach grupy w górę.

Eksport do pliku – kliknij, żeby wyeksportować zdefiniowane makropolecenia do pliku. Plik z makropoleczeniami będzie można wczytać do aplikacji INTEGRA CONTROL lub zaimportować do innego urządzenia obsługującego makropolecenia.

Import z pliku – kliknij, żeby zaimportować makropolecenia z pliku.

5.5.2 Definicje

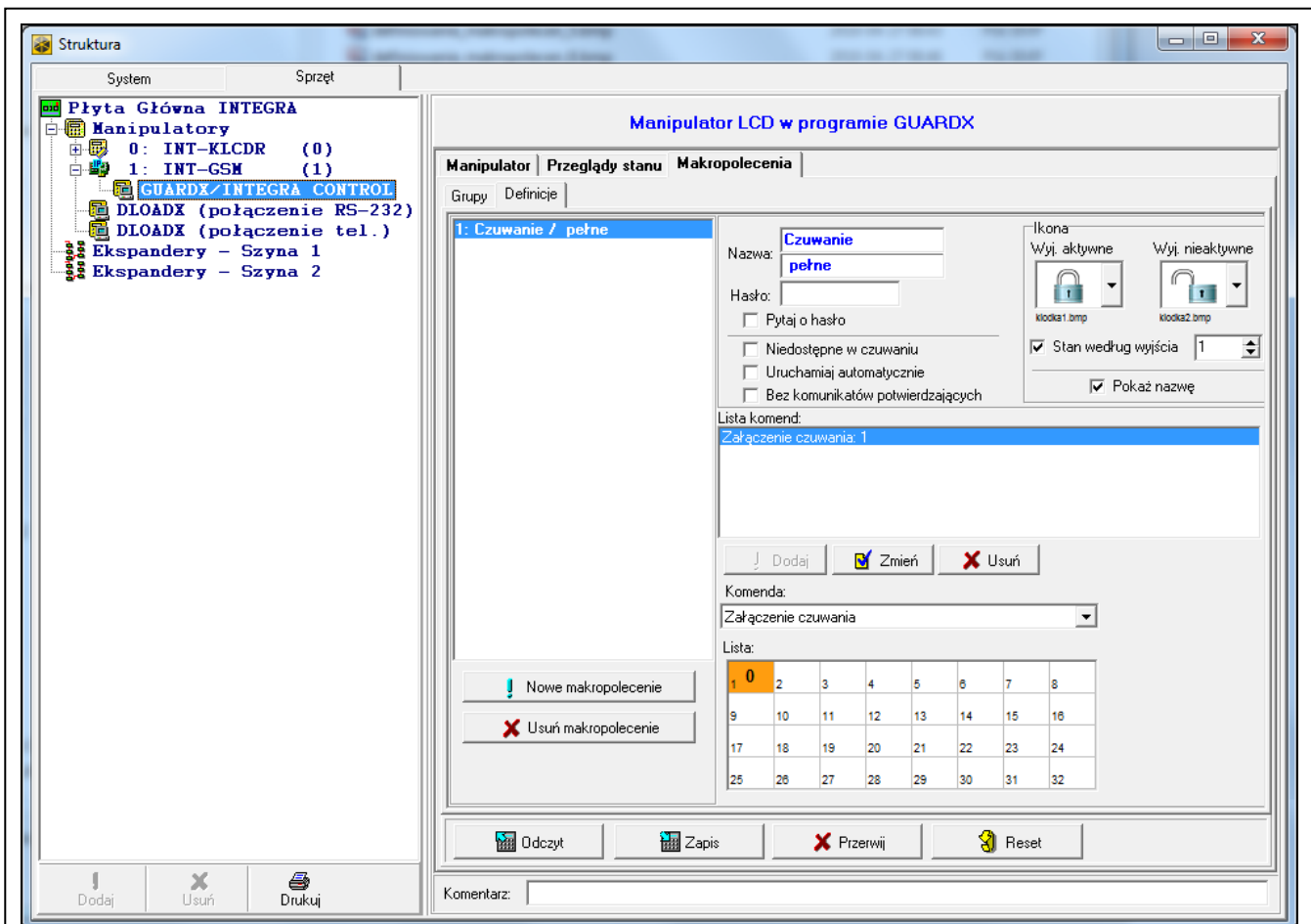
Makropolecenia można tworzyć i konfigurować w zakładce „Definicje”. Makropolecenie to złożona z pojedynczych komend sekwencja działań, które ma wykonać centrala po uruchomieniu makropolecenia.

Nowe makropolecenie – kliknij, żeby utworzyć nowe makropolecenie.

Usuń makropolecenie – kliknij, żeby usunąć zaznaczone makropolecenie.

Nazwa – indywidualna nazwa makropolecenia (do 16 znaków w dwóch liniach, do 8 znaków w linii).

Pytaj o hasło – jeżeli opcja jest włączona, makropolecenie zostanie uruchomione dopiero po dodatkowej autoryzacji użytkownika.



Rys. 19. Program DLOADX: zakładka „Definicje”.

Niedostępne w czuwaniu – jeżeli opcja jest włączona, makropolecenie będzie niedostępne, gdy czuwa dowolna ze stref obsługiwanych przez wirtualny manipulator.

Uruchamiaj automatycznie – jeżeli opcja jest włączona, makropolecenie można uruchamiać bez potrzeby wchodzenia do grupy.

Bez komunikatów potwierdzających – jeżeli opcja jest włączona, po uruchomieniu makropolecenia nie pojawiają się komunikaty informujące o wykonaniu polecenia lub o błędzie (wciąż wyświetlany będzie ekran, z którego uruchomiono makropolecenie).

Ikona

Ikona – ikona makropolecenia. Lista dostępnych ikon zostanie wyświetlona po kliknięciu na

przycisk . Jeżeli włączona jest opcja „Stan według wyjścia”, dla makropolecenia należy wybrać 2 ikony. Jedna ikona wyświetlana będzie, gdy wyjście będzie nieaktywne, a druga – gdy będzie aktywne.

Stan według wyjścia – jeżeli opcja jest włączona, ikona makropolecenia będzie zmieniać się w zależności od stanu wyjścia, którego numer należy wskazać w polu obok. Należy wybrać wyjście, którego stan zależy od działań podejmowanych przez centralę po uruchomieniu makropolecenia. Pozwoli to informować użytkownika przy pomocy ikon makropolecenia np. o stanie wyjść sterowanych przy pomocy makropolecenia lub stanie stref, w których makropolecenie załącza czuwanie.

Pokaż nazwę – jeżeli opcja jest włączona, nazwa makropolecenia jest wyświetlana.

Komendy

Lista komend – komendy przypisane do aktualnie zaznaczonego makropolecenia. Przyciski



umożliwiają zmianę kolejności komend (przesuwanie zaznaczonej komendy w dół i w górę).

Dodaj – kliknij, żeby do listy komend dodać nową, wybraną w polu „Komenda”.

Zmień – kliknij, żeby zapisać zmiany w parametrach komendy wprowadzone już po dodaniu komendy do listy (w innym przypadku wprowadzone zmiany nie zostaną zachowane).

Usuń – kliknij, żeby usunąć z listy zaznaczoną komendę.

Komenda – realizowana przez centralę funkcja, którą można przypisać do makropolecenia.

Lista wszystkich dostępnych funkcji zostanie wyświetlona po kliknięciu na przycisk . W zależności od tego, którą funkcję wybrałeś:

Załączenie czuwania – zaznacz strefy, w których ma zostać załączone czuwanie (dwukrotnie kliknij na pole oznaczone numerem strefy) i określ typ czuwania (kolejne kliknięcia na pole oznaczone numerem strefy; cyfra w środku pola oznacza: 0 - pełne czuwanie; 1 – pełne czuwanie + blokady; 2 – czuwanie bez wewnętrznych; 3 - czuwanie bez wewnętrznych i bez czasu na wejście).

Wyłączenie czuwania – zaznacz strefy, w których ma zostać wyłączone czuwanie (dwukrotnie kliknij na pole oznaczone numerem strefy).

Kasowanie alarmu – zaznacz strefy, w których ma zostać skasowany alarm (dwukrotnie kliknij na pole oznaczone numerem strefy).

Blokowanie wejść – zaznacz wejścia, które mają zostać czasowo zablokowane (dwukrotnie kliknij na pole oznaczone numerem wejścia).

Odblokowanie wejść – zaznacz wejścia, które mają zostać odblokowane (dwukrotnie kliknij na pole oznaczone numerem wejścia).

Załączenie wyjść – zaznacz wyjścia, które mają zostać włączone (dwukrotnie kliknij na pole oznaczone numerem wyjścia).

Wyłączenie wyjść – zaznacz wyjścia, które mają zostać wyłączone (dwukrotnie kliknij na pole oznaczone numerem wyjścia).

Zmień stan wyjść – zaznacz wyjścia, których stan ma się zmienić (dwukrotnie kliknij na pole oznaczone numerem wyjścia).

Telegram KNX – zaprogramuj następujące parametry telegramu KNX dla modułu INT-KNX:

Moduł INT-KNX – moduł INT-KNX, który ma wysłać telegram.

Adres grupowy – adres grupowy, który umieszczony zostanie w telegramie.

Typ – typ telegramu.

Wartość – wartość, która umieszczona będzie w telegramie (parametr dostępny dla niektórych typów telegramu).

Priorytet – priorytet telegramu (jeżeli dwa elementy magistrali zaczną nadawać równocześnie, telegram z wyższym priorytetem będzie miał pierwszeństwo).

Telegram KNX (v2) – zaprogramuj następujące parametry dotyczące ustawiania wartości obiektu komunikacyjnego KNX:

Moduł INT-KNX – moduł INT-KNX-2, w którym ma zostać ustawiona wartość.

Makropolecenie – nazwa obiektu typu „Wirtualny (makro)” zdefiniowana w module INT-KNX-2.

Typ danych – rozmiar i znaczenie danych obiektu komunikacyjnego zdefiniowane w module INT-KNX-2 dla wybranego obiektu.

Wartość – wartość, która ma zostać ustawiona (jeśli typ danych przewiduje wysłanie ciągu znaków, możesz wprowadzić do 13 znaków).

Skracanie cz. na wy. (brak dodatkowych parametrów do konfiguracji).

Szybkie załączenie czuwania – wybierz typ czuwania, który ma być załączony.



Strefy muszą być sterowane hasłem użytkownika.

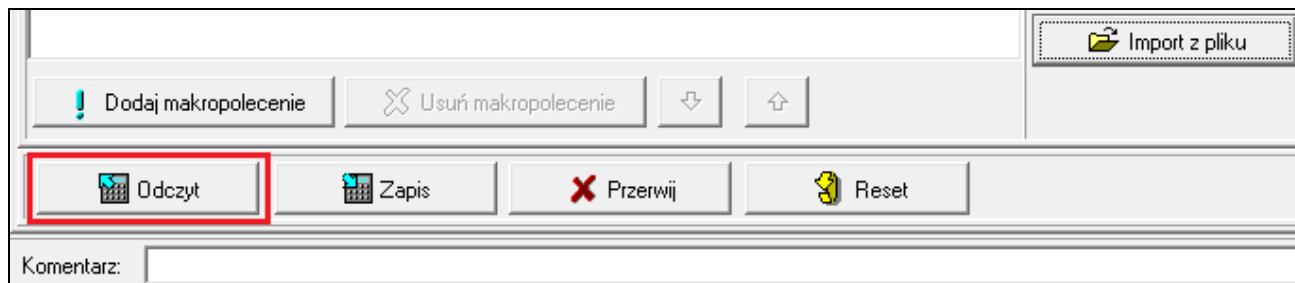
Wejścia nie mogą mieć włączonej opcji „Użytkownik nie blokuje”.

Wyjścia muszą być typu 24. PRZEŁĄCZNIK MONO, 25. PRZEŁĄCZNIK BI, 105. ROLETA W GÓRĘ, 106. ROLETA W DÓŁ lub PRZEKAŹNIK TELEFONICZNY.

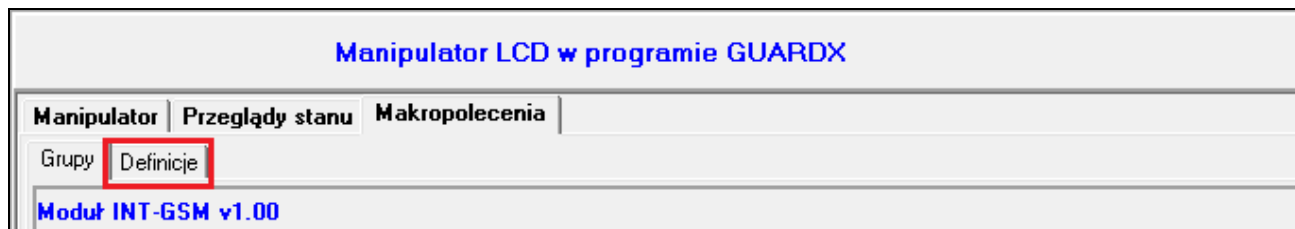
Aplikacja INTEGRA CONTROL może sterować systemem KNX, jeżeli do centrali podłączony jest moduł INT-KNX / INT-KNX-2.

5.5.3 Definiowanie makropoleceń

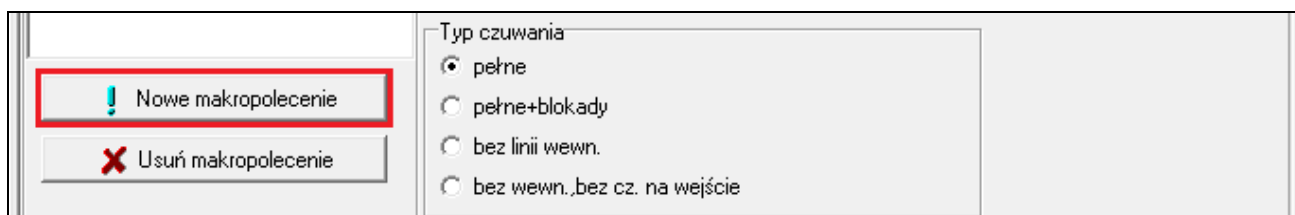
1. Kliknij na przycisk „Odczyt”, żeby odczytać z modułu dane dotyczące makropoleceń.



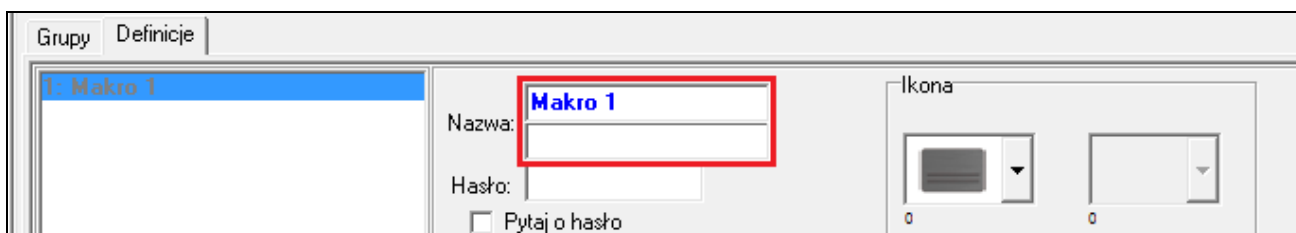
2. Kliknij na zakładkę „Definicje”.



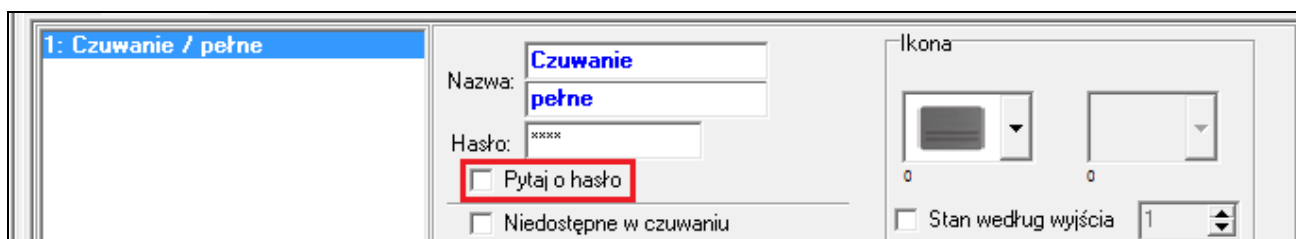
3. Kliknij na przycisk „Nowe makropolecenie”. Na liście pojawi się nowe makropolecenie.



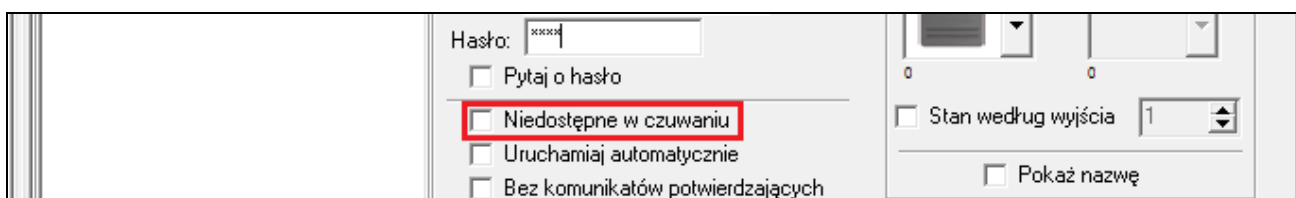
4. Wprowadź nazwę nowego makropolecenia.



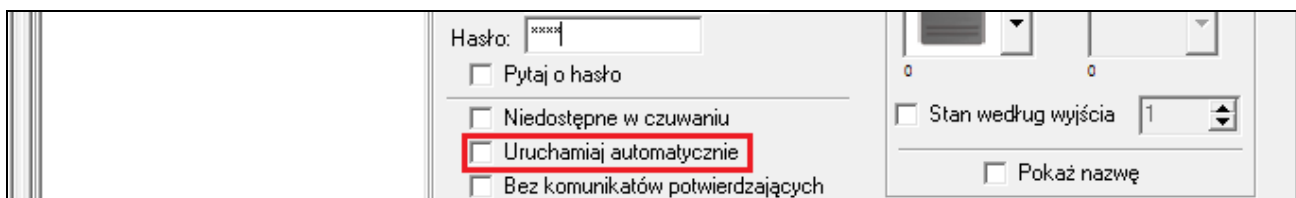
5. Jeżeli uruchomienie makropolecenia ma być każdorazowo poprzedzane autoryzacją użytkownika, włącz opcję „Pytaj o hasło”.



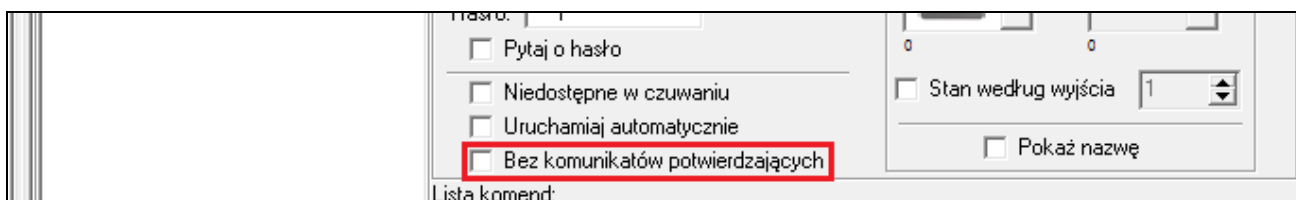
6. Jeżeli makropolecenie ma być niedostępne, gdy czuwa dowolna ze stref obsługiwanych przez aplikację, włącz opcję „Niedostępne w czuwaniu”.



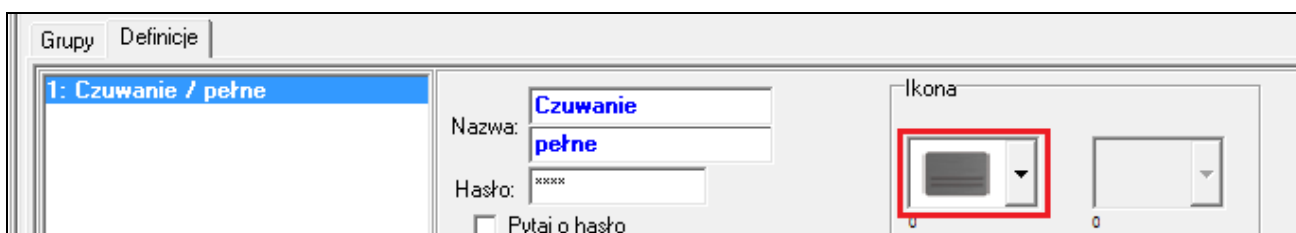
7. Jeżeli makropolecenie ma być dostępne bez wchodzenia do grupy, włącz opcję „Uruchamiaj automatycznie”.



8. Jeżeli po uruchomieniu makropolecenia nie mają być wyświetlane komunikaty potwierdzające, włącz opcję „Bez komunikatów potwierdzających”.

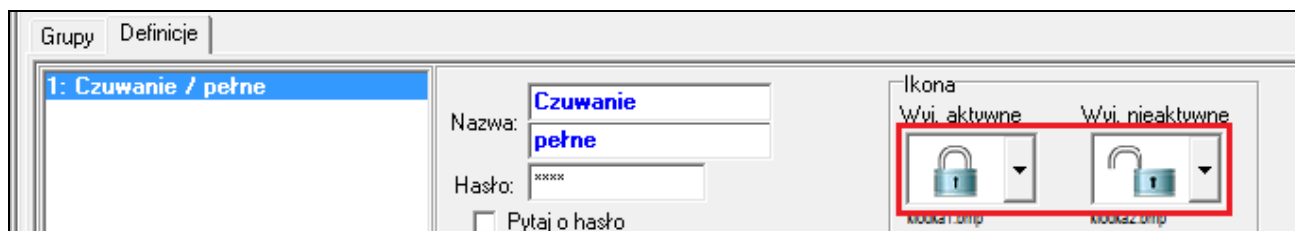
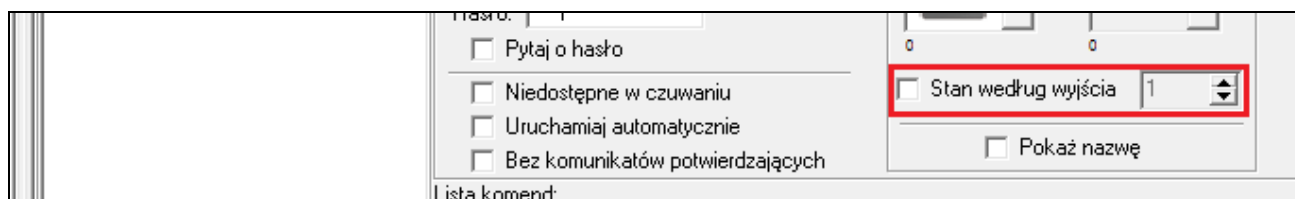


9. Kliknij na przycisk i wybierz ikonę dla makropolecenia.

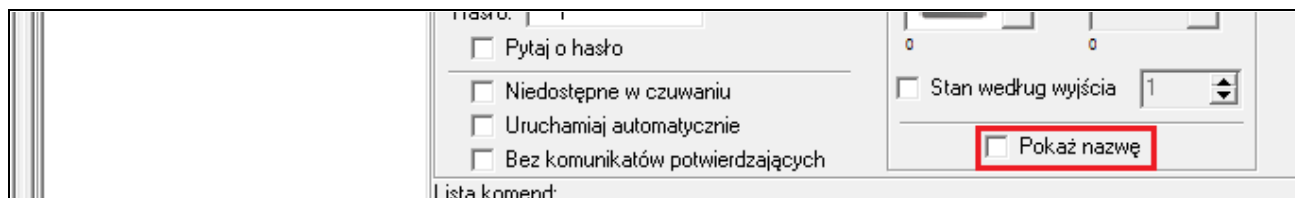


10. Jeżeli ikona ma się zmieniać w zależności od stanu wybranego wyjścia:

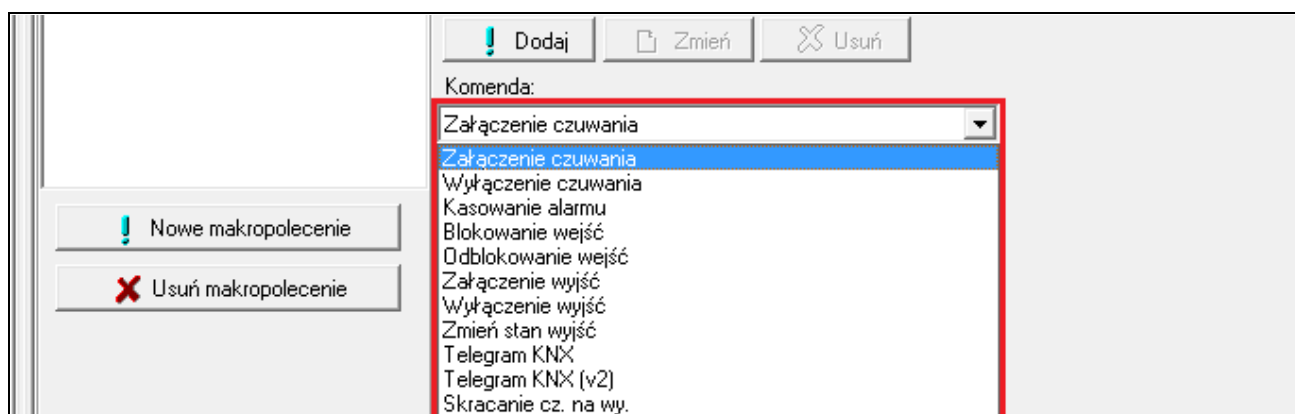
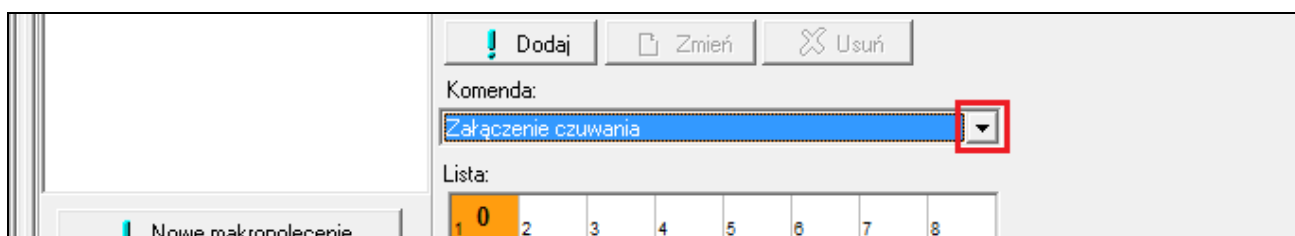
- włącz opcję „Stan według wyjścia”,
- wskaż numer wyjścia,
- wybierz ikony.



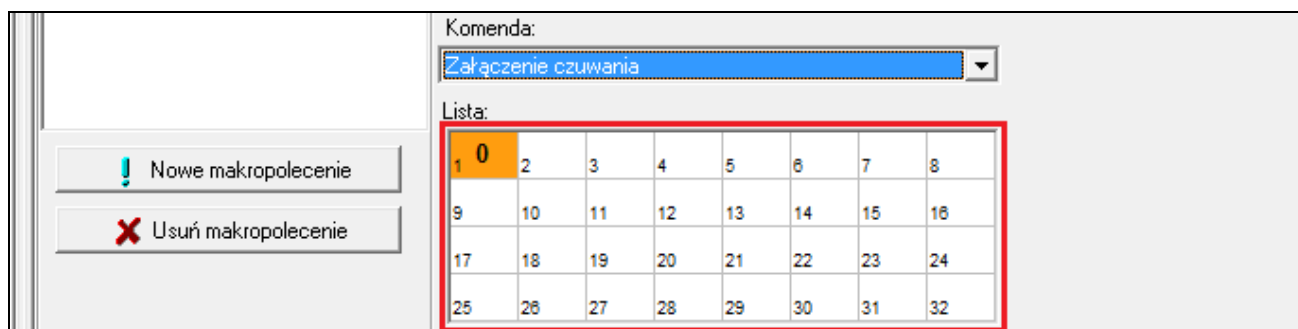
11. Jeżeli ma być wyświetlana nazwa makropolecenia, włącz opcję „Pokaż nazwę”.



12. Kliknij na przycisk  i wybierz z listy funkcję, którą ma uruchamiać nowe makropolecenie.



13. Skonfiguruj parametry komendy.



Komenda:

Załączenie czuwania

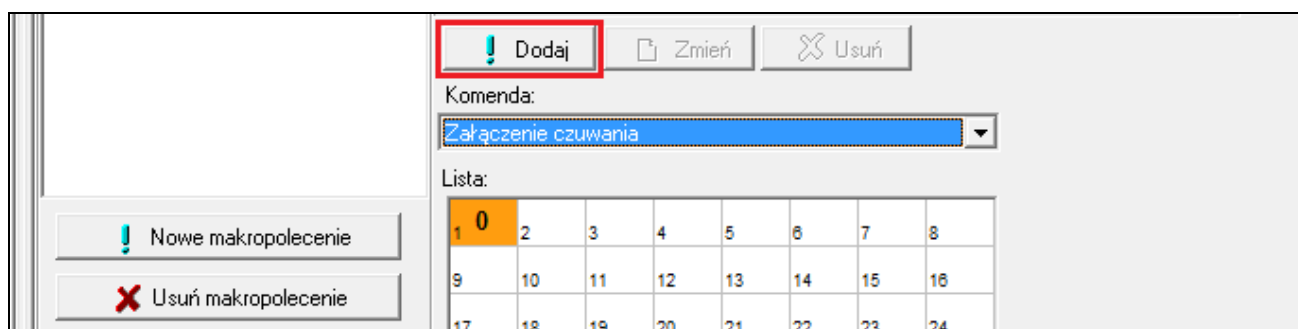
Lista:

1	0	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	
17	18	19	20	21	22	23	24	
25	26	27	28	29	30	31	32	

Nowe makropolecenie

Usuń makropolecenie

14. Kliknij na przycisk „Dodaj”. Na liście komend przypisanych do makropolecenia pojawi się nowa. Po kliknięciu na komendę możesz jeszcze zmodyfikować jej parametry (po dokonaniu zmian kliknij na przycisk „Zmień”).



Dodaj

Zmień

Usuń

Komenda:

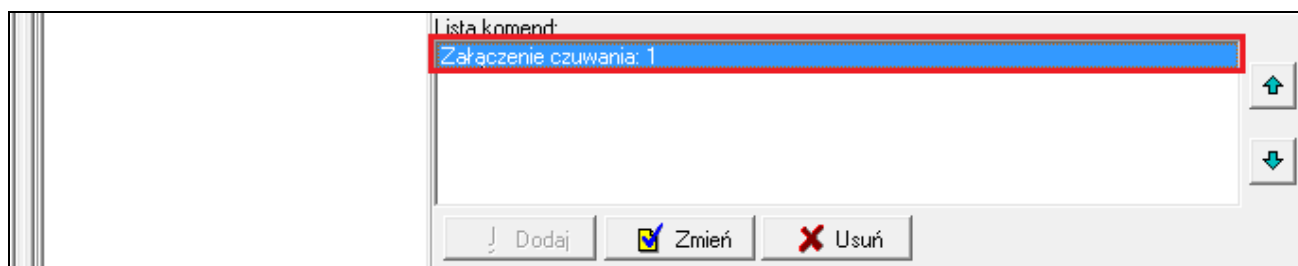
Załączenie czuwania

Lista:

1	0	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	
17	18	19	20	21	22	23	24	

Nowe makropolecenie

Usuń makropolecenie



Lista komend:

Załączenie czuwania: 1

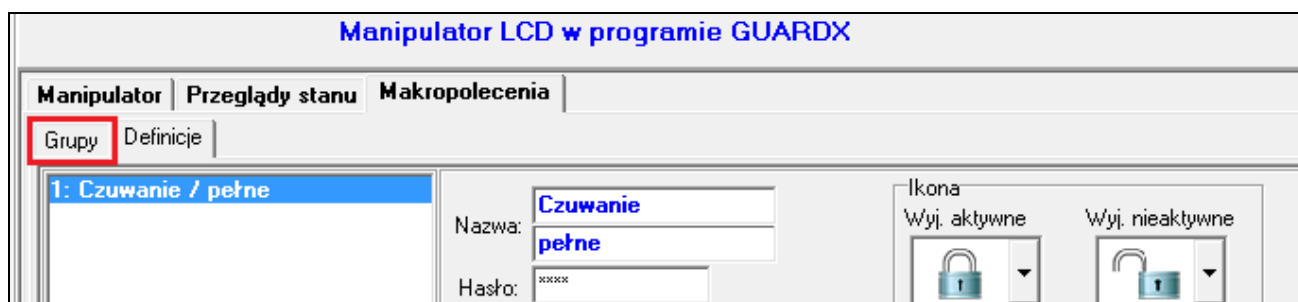
Dodaj

Zmień

Usuń

15. Powtórz czynności z punktów 12-14, jeśli chcesz dodać kolejne komendy.

16. Kliknij na zakładkę „Grupy”.



Manipulator LCD w programie GUARDX

Manipulator Przeglądy stanu Makropolecenia

Grupy Definicje

1: Czuwanie / pełne

Nazwa: Czuwanie
pełne

Hasło: XXXX

Ikona

Wyj. aktywne

Wyj. nieaktywne

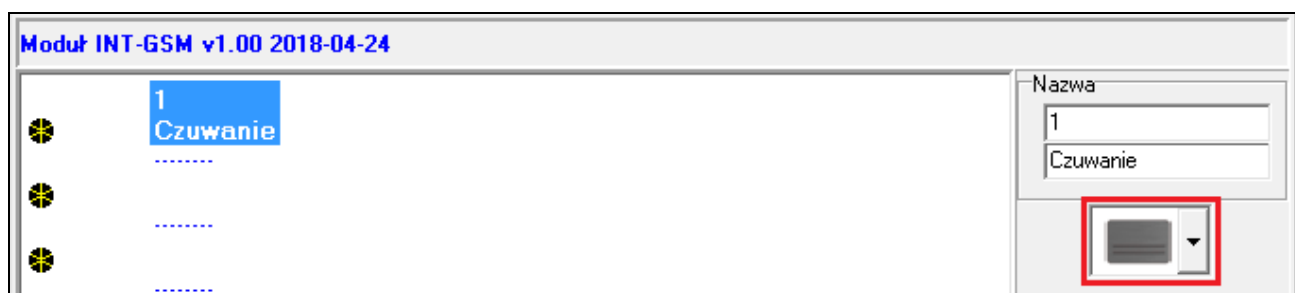
17. Kliknij na grupę, którą chcesz edytować.



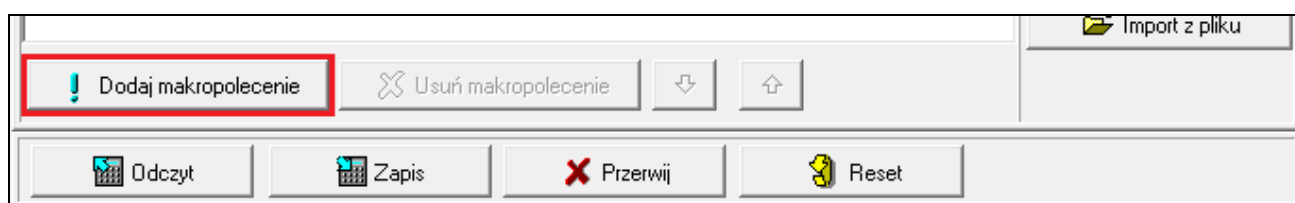
18. Wpisz nazwę grupy, jeżeli ma być wyświetlana.



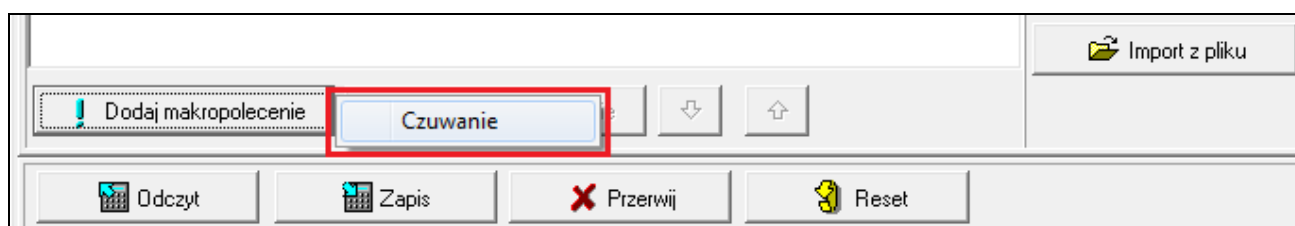
19. Kliknij na przycisk  i wybierz ikonę dla grupy makropoleceń.

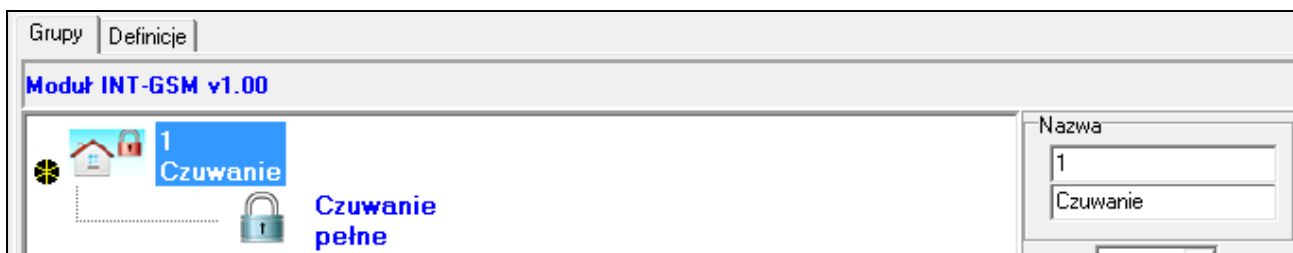


20. Kliknij na przycisk „Dodaj makropolecenie”. Wyświetlona zostanie lista wszystkich zdefiniowanych makropoleceń.

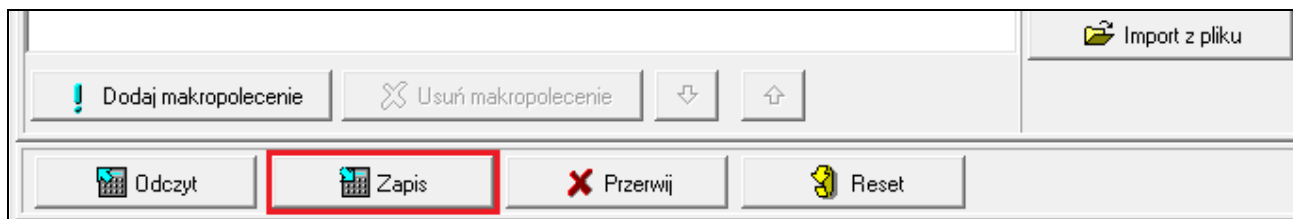


21. Kliknij na makropolecenie, żeby dodać je do grupy. Makropolecenie zostanie umieszczone na drzewie pod grupą.





22. Kliknij na przycisk „Zapis”, żeby zapisać do modułu dane dotyczące makropoleceń.



6. Zdalne programowanie i obsługa centrali za pośrednictwem modułu

Informacje na temat konfigurowania centrali alarmowej przy pomocy programu DLOADX znajdują się w instrukcjach programowania central alarmowych.

6.1 Program GUARDX



Jeżeli moduł INT-GSM jest podłączony do modułu ETHM-1 Plus, łączność za pośrednictwem modułu INT-GSM (przez GPRS) jest używana tylko, gdy nie uda się nawiązać połączenia przez Ethernet (patrz instrukcja modułu ETHM-1 Plus).

Połączenie między programem GUARDX a centralą alarmową za pośrednictwem modułu INT-GSM podłączonego do centrali można nawiązać w jeden z poniższych sposobów:

1. Zainicjowanie połączenia z manipulatora (przez centralę alarmową). Systemem alarmowym można zarządzać tylko z określonej lokalizacji. Sposób zalecany, gdy właściciel systemu alarmowego nie chce, by zarządzano systemem bez jego wiedzy. Komputer z programem GUARDX musi mieć publiczny adres IP.
2. Zainicjowanie połączenia przy pomocy wiadomości SMS. Komputer z programem GUARDX musi mieć publiczny adres IP.
3. Nawiązanie połączenia za pośrednictwem serwera SATEL. Systemem alarmowym można zarządzać z dowolnej lokalizacji. Komputer z programem GUARDX nie potrzebuje publicznego adresu IP.



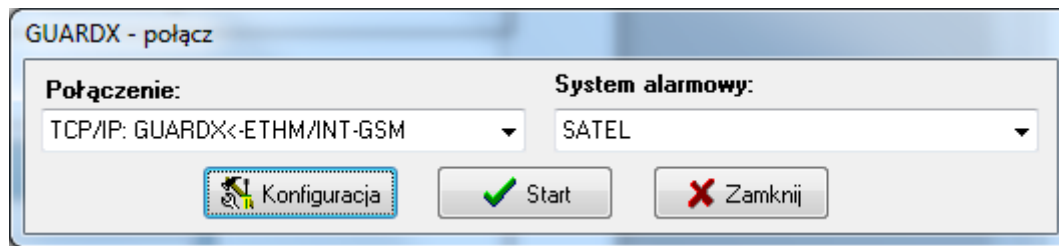
Nawiązanie połączenia jest możliwe, gdy w centrali i w programie GUARDX zaprogramowane są identyczne identyfikatory („Identyfikator centrali” i „Identyfikator GUARDX”).

Wymagane ustawienia modułu INT-GSM dla wszystkich sposobów nawiązania łączności:

- włączona opcja „GUARDX” (s. 11),
- zaprogramowany klucz kodowania danych („Klucz GUARDX” s. 11).

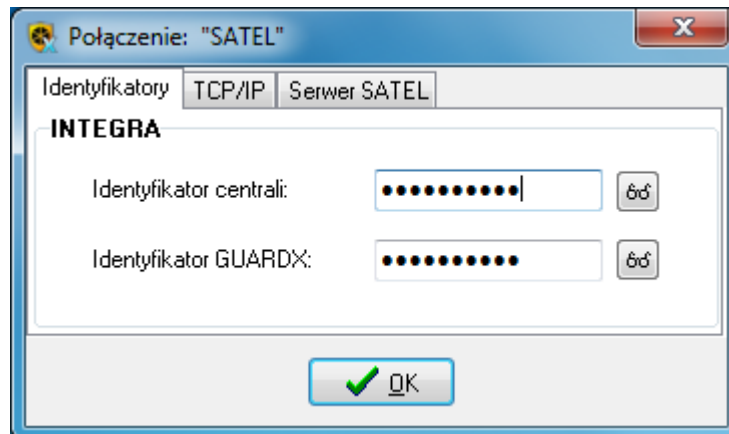
6.1.1 Konfigurowanie ustawień programu GUARDX

Ustawienia dotyczące komunikacji z systemem alarmowym możesz skonfigurować po kliknięciu w oknie startowym programu GUARDX (rys. 20) na przycisk „Konfiguracja”.



Rys. 20. Program GUARDX: okno startowe.

Zakładka „Identyfikatory”



Rys. 21. Program GUARDX: zakładka „Identyfikatory” w oknie „Połączenie”.

Identyfikator centrali – identyfikator centrali alarmowej. Musi mieć 10 znaków (cyfry lub litery od A do F).

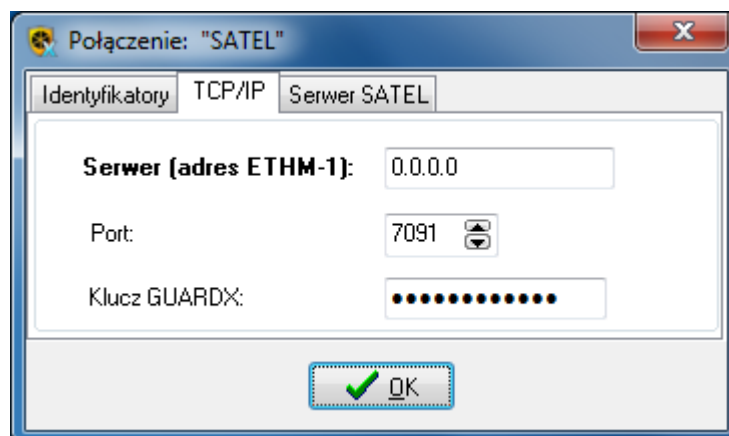
Identyfikator GUARDX – identyfikator komputera z programem GUARDX. Musi mieć 10 znaków (cyfry lub litery od A do F).

Wprowadzone numery są widoczne po kliknięciu na .



W programie GUARDX muszą zostać wprowadzone identyczne identyfikatory, jak w centrali.

Zakładka „TCP/IP”



Rys. 22. Program GUARDX: zakładka „TCP/IP” w oknie „Połączenie”.

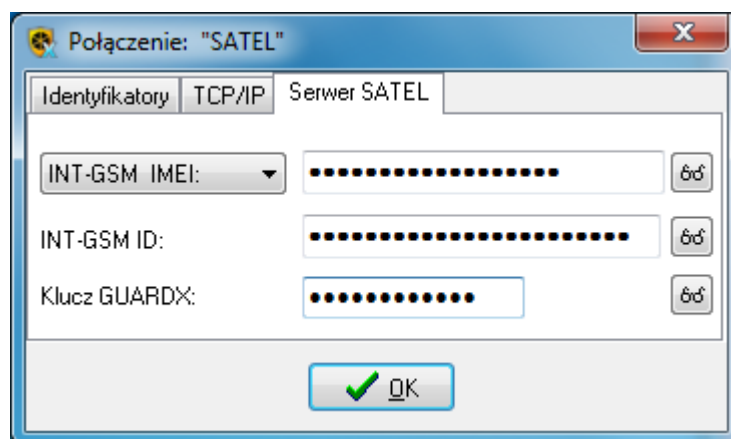
Poniższe ustawienia dotyczą komunikacji bezpośrednio z modułem.

Port – numer portu TCP używanego podczas komunikacji między centralą a komputerem z programem GUARDX.

Klucz GUARDX – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do kodowania danych podczas komunikacji między centralą a komputerem z programem GUARDX. Wprowadzony numer jest widoczny po kliknięciu na .

Zakładka „Serwer SATEL”

Poniższe ustawienia dotyczą komunikacji za pośrednictwem serwera SATEL.



Rys. 23. Program GUARDX: zakładka „Serwer SATEL” w oknie „Połączenie”.

Wybierz wariant „INT-GSM IMEI”.

INT-GSM IMEI – indywidualny numer identyfikacyjny telefonu GSM modułu.

INT-GSM ID – indywidualny numer identyfikacyjny przydzielony modułowi INT-GSM przez serwer SATEL.

Klucz GUARDX – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do kodowania danych podczas komunikacji między centralą a komputerem z programem GUARDX.

Wprowadzone numery są widoczne po kliknięciu na .

6.1.2 Zainicjowanie połączenia przy pomocy wiadomości SMS

Wymagane ustawienia modułu INT-GSM:

- zaprogramowane: adres komputera z programem GUARDX („GUARDX serwer” s. 11) i numer portu TCP, jeżeli ma być inny niż 7091 (s. 11),
- zaprogramowane polecenie sterujące, którego przesłanie w wiadomości SMS zainicjuje nawiązanie łączności z programem GUARDX (patrz: „SMS inicjujący połączenie z GUARDX” s. 15).

Wymagane ustawienia programu GUARDX dla komunikacji bezpośrednio z modulem:

- zaprogramowane: numer portu TCP używanego do komunikacji i klucz kodowania danych („Klucz GUARDX”).
1. W oknie startowym (rys. 20), w polu „Połączenie”, wybierz „TCP/IP: GUARDX<-ETHM/INT-GSM”, a następnie kliknij na przycisk „Start”. Zostanie wyświetlone okno z informacją, że program oczekuje na połączenie.
 2. Wyślij do modułu INT-GSM wiadomość SMS o treści:
xxxx („xxxx” – polecenie sterujące inicjujące nawiązanie łączności z programem GUARDX) – moduł ma się połączyć z komputerem, którego adres został zaprogramowany w module.

xxxx=aaaa:p= („xxxx” – polecenie sterujące inicjujące nawiązanie łączności z programem GUARDX; „aaaa” – adres komputera z programem GUARDX; „p” – port TCP) – moduł ma się połączyć z komputerem, którego adres podany został w wiadomości SMS i użyć do komunikacji portu TCP podanego w wiadomości SMS.

3. W oknie, które wyświetli się po nawiązaniu komunikacji, wprowadź hasło administratora / użytkownika centrali.

6.1.3 Zainicjowanie połączenia z manipulatora (przez centralę alarmową)

Wymagane ustawienia modułu INT-GSM:

- zaprogramowane: adres komputera z programem GUARDX („GUARDX server” s. 11) i numer portu TCP, jeżeli ma być inny niż 7091 (s. 11).

Wymagane ustawienia programu GUARDX dla komunikacji bezpośrednio z modułem:

- zaprogramowane: numer portu TCP używanego do komunikacji i klucz kodowania danych („Klucz GUARDX”).
1. W oknie startowym (rys. 20), w polu „Połączenie” wybierz „TCP/IP: GUARDX<-ETHM/INT-GSM”, a następnie kliknij na przycisk „Start”. Zostanie wyświetlone okno z informacją, że program oczekuje na połączenie.
 2. Poproś użytkownika o uruchomienie funkcji INT-GSM → GUARDX ([*hasło*]* ►DOWNLOADING ►INT-GSM →GUARDX). Funkcja jest dostępna dla serwisu, administratora i użytkownika posiadającego uprawnienie „Uruchamianie funkcji DOWNLOAD”.
 3. W oknie, które wyświetli się po nawiązaniu komunikacji, wprowadź hasło administratora / użytkownika centrali.

6.1.4 Nawiązanie połączenia za pośrednictwem serwera SATEL



Do komunikacji za pośrednictwem serwera SATEL jako porty wychodzące używane są porty z zakresu 1024-65535. Porty te nie mogą być zablokowane.

Wymagane ustawienia modułu INT-GSM:

- włączona opcja „Łączność przez serwer SATEL”.

Wymagane ustawienia programu GUARDX dla komunikacji za pośrednictwem serwera SATEL:

- zaprogramowane: numer identyfikacyjny przydzielony modułowi INT-GSM przez serwer SATEL („INT-GSM ID”), numer IMEI modułu INT-GSM („INT-GSM IMEI”) i klucz kodowania danych („Klucz GUARDX”).
1. W oknie startowym (rys. 20), w polu „Połączenie”, wybierz „TCP/IP: serwer SATEL”, a następnie kliknij na przycisk „Start”.
 2. W oknie, które wyświetli się po nawiązaniu komunikacji, wprowadź hasło administratora / użytkownika centrali.

6.2 Aplikacja mobilna INTEGRA CONTROL

System alarmowy INTEGRA / INTEGRA Plus można obsługiwać i konfigurować z urządzenia mobilnego po zainstalowaniu aplikacji INTEGRA CONTROL. Aplikację możesz pobrać ze sklepu internetowego „Google play” (urządzenia z systemem Android) lub „App Store” (urządzenia z systemem iOS). Na stronie www.satel.pl znajdziesz odsyłacze do lokalizacji, z których można pobrać aplikacje.

Aplikacja INTEGRA CONTROL umożliwia nawiązanie połączenia za pośrednictwem serwera SATEL (Usługa Zestawiania Połączeń).

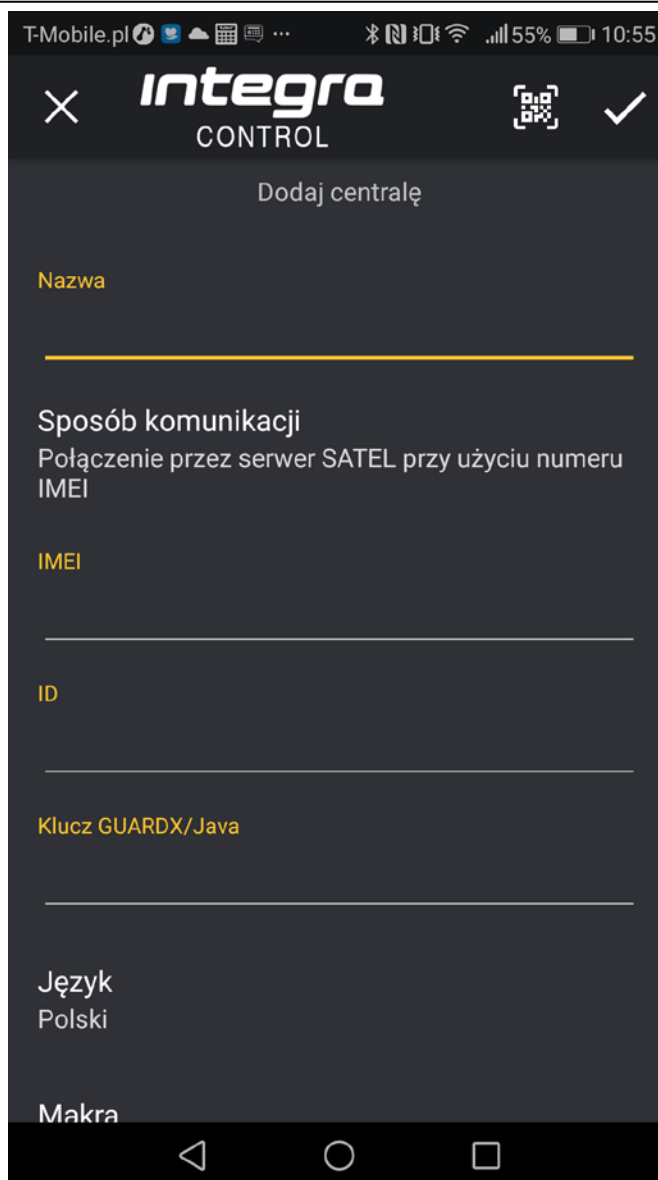


Jeżeli moduł INT-GSM jest podłączony do modułu ETHM-1 Plus, łączność za pośrednictwem modułu INT-GSM (przez GPRS) jest używana tylko, gdy nie uda się nawiązać połączenia przez Ethernet (patrz instrukcja modułu ETHM-1 Plus).

Wymagane ustawienia modułu INT-GSM:

- włączone opcje „INTEGRA CONTROL” i „Łączność przez serwer SATEL”,
- zaprogramowany klucz kodowania danych („Klucz GUARDX”).

6.2.1 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (Android)



Rys. 24. Aplikacja INTEGRA CONTROL (system Android): ekran „Dodaj centralę” przed wprowadzeniem danych.

Po pierwszym uruchomieniu aplikacji wyświetlony zostanie ekran „Dodaj centralę”. Pozwala on skonfigurować ustawienia wymagane do nawiązania połączenia z centralą.

1. Wprowadź nazwę dla systemu alarmowego. Nazwa ułatwia identyfikację systemu podczas korzystania z aplikacji (możesz zdefiniować ustawienia dla wielu systemów alarmowych).
2. Skonfiguruj ustawienia komunikacji z modułem INT-GSM. Ustawienia mogą zostać skonfigurowane automatycznie (patrz: „Konfiguracja automatyczna – kod QR” s. 38) lub możesz wprowadzić je ręcznie (patrz: „Konfiguracja ręczna” s. 38).

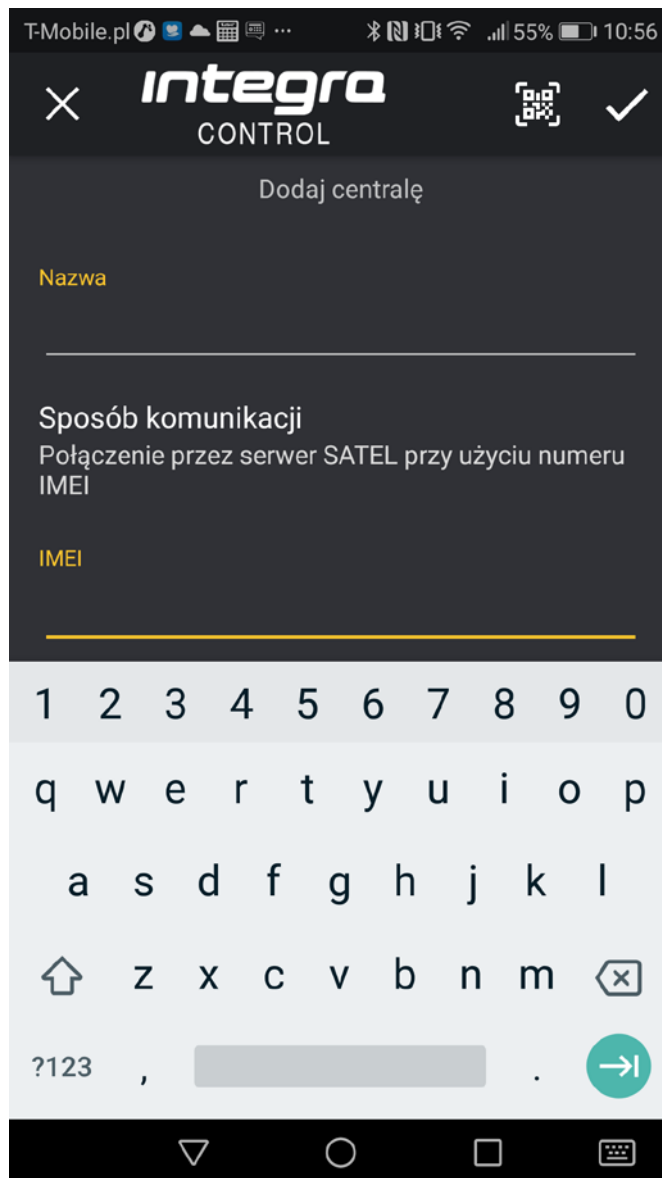
3. Określ sposób postępowania z makropoleceniami. Ustawienia domyślne przewidują importowanie makropoleceń z modułu (zostaną pobrane podczas pierwszego połączenia). Jeżeli makropolecenia nie mają być importowane lub mają być importowane z pliku, dotknij ekran w obszarze „Makra” i zmień ustawienia. Jeżeli wybierzesz import z pliku, będziesz musiał wskazać lokalizację pliku z makropoleceniami.
4. Dotknij , żeby zapisać ustawienia.

Konfiguracja automatyczna – kod QR

Dotknij , żeby uruchomić skaner kodu QR. Przy pomocy skanera odczytaj ustawienia komunikacji z kodu QR (patrz: s. 12).

Jeżeli ustawienia komunikacji zostaną skonfigurowane w jednym urządzeniu mobilnym, można te ustawienia łatwo skopiować do innego urządzenia mobilnego. Wystarczy wyświetlić kod QR w urządzeniu, w którym ustawienia komunikacji z danym modułem już są skonfigurowane, i odczytać go w drugim urządzeniu.

Konfiguracja ręczna



Rys. 25. Aplikacja INTEGRA CONTROL (system Android): ekran „Dodaj centralę” z przykładowymi ustawieniami dla komunikacji przez serwer SATEL.

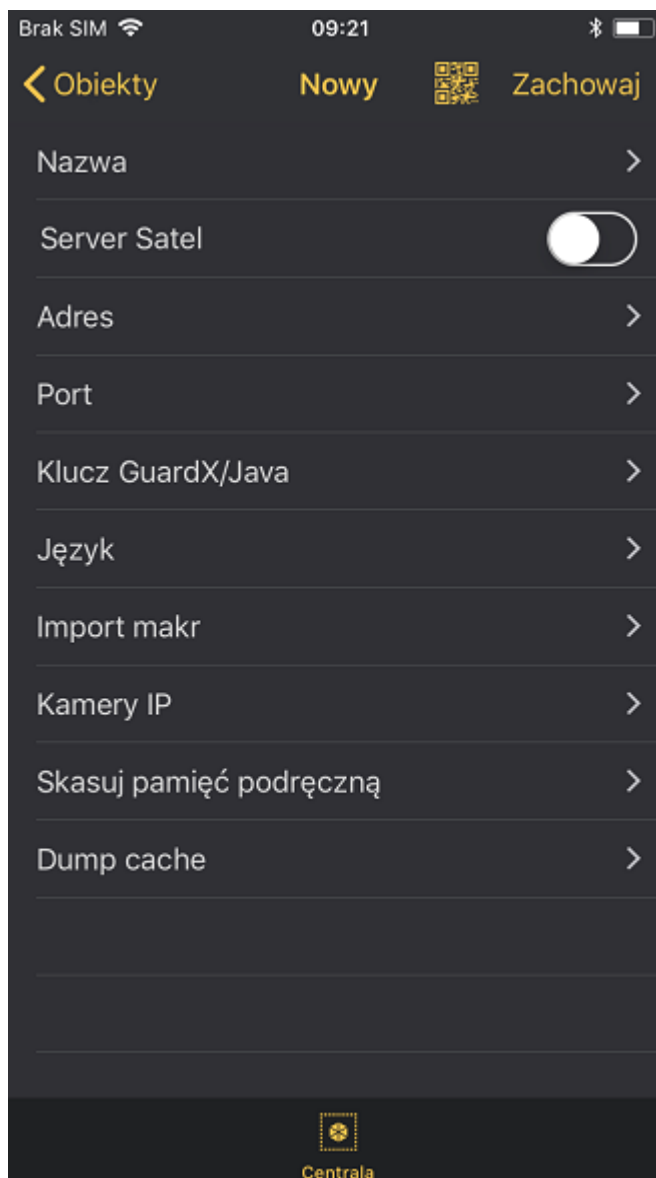
1. Dotknij ekran w obszarze „Sposób komunikacji”, żeby wybrać „Połączenie przez serwer SATEL przy użyciu numeru IMEI”, jako sposób komunikacji.
2. Wprowadź numer IMEI telefonu GSM modułu.
3. Wprowadź numer ID modułu INT-GSM (identyfikator przydzielony modułowi przez serwer SATEL).



Użytkownik może sprawdzić numery IMEI i ID przy pomocy manipulatora (funkcja użytkownika IP/MAC/IMEI/ID dostępna w podmenu TESTY – patrz instrukcja użytkownika centrali alarmowej).

4. Wprowadź klucz kodowania danych – identyczny, jak w module („Klucz GUARDX”).

6.2.2 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (iOS)



Rys. 26. Aplikacja INTEGRA CONTROL (system iOS): ekran „Nowy” przed wprowadzeniem danych.

Po pierwszym uruchomieniu aplikacji wyświetlona zostanie zakładka „Systemy”.

1. Dotknij „Edycja”.
2. Dotknij „Nowy”.

3. Wprowadź nazwę dla systemu alarmowego. Nazwa służy do identyfikacji systemu podczas korzystania z aplikacji (możesz zdefiniować ustawienia dla wielu systemów alarmowych).
4. Skonfiguruj ustawienia komunikacji z modulem INT-GSM. Ustawienia mogą zostać skonfigurowane automatycznie (patrz: „Konfiguracja automatyczna – kod QR” s. 40) lub możesz wprowadzić je ręcznie (patrz: „Konfiguracja ręczna” s. 40).
5. Określ język centrali alarmowej.
6. Określ sposób postępowania z makropoleceniami. Ustawienia domyślne przewidują importowanie makropoleceń z modułu (zostaną pobrane podczas pierwszego połączenia). Jeżeli makropolecenia nie mają być importowane lub mają być importowane z pliku, dotknij ekran w obszarze „Import makr” i zmień ustawienia.
7. Dotknij „Zachowaj”, żeby zapisać ustawienia.

Konfiguracja automatyczna – kod QR

Dotknij , żeby uruchomić skaner kodu QR. Przy pomocy skanera odczytaj ustawienia komunikacji z kodu QR (patrz: s. 12).

Jeżeli ustawienia komunikacji zostaną skonfigurowane w jednym urządzeniu mobilnym, można te ustawienia łatwo skopiować do innego urządzenia mobilnego. Wystarczy wyświetlić kod QR w urządzeniu, w którym ustawienia komunikacji z danym modulem już są skonfigurowane, i odczytać go w drugim urządzeniu.

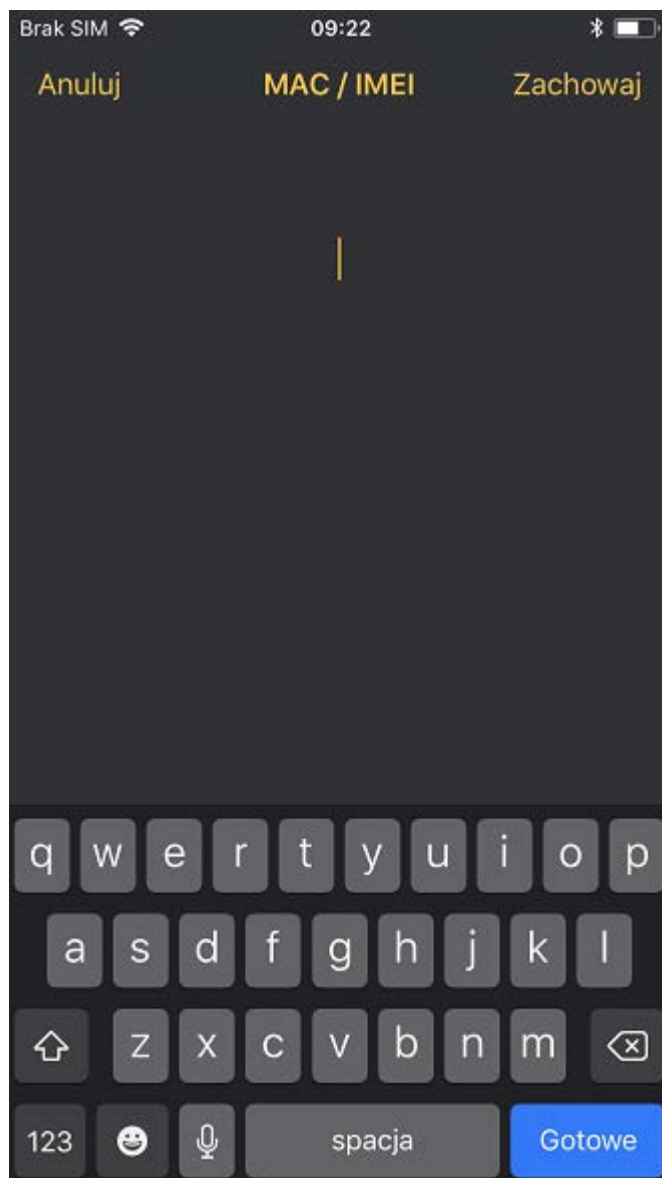
Konfiguracja ręczna

1. Włącz opcję „Server Satel”, żeby aplikacja mogła łączyć się za pośrednictwem serwera SATEL.
2. Wprowadź numer IMEI telefonu GSM modułu INT-GSM.
3. Wprowadź numer ID modułu INT-GSM (identyfikator przydzielony modułowi przez serwer SATEL).



Użytkownik może sprawdzić numery IMEI i ID przy pomocy manipulatora (funkcja użytkownika IP/MAC/IMEI/ID dostępna w podmenu TESTY – patrz instrukcja użytkownika centrali alarmowej).

4. Wprowadź klucz kodowania danych – identyczny, jak w module („Klucz GUARDX”).



Rys. 27. Aplikacja INTEGRA CONTROL (system iOS): ekran „MAC / IMEI”.

6.2.3 Nawiązanie komunikacji

Dotknij nazwę systemu alarmowego. Na wyświetlaczu pojawi się wirtualny manipulator.



Rys. 28. Aplikacja INTEGRA CONTROL (system Android): wirtualny manipulator.

7. Dane techniczne

Napięcie zasilania	12 V DC $\pm 15\%$
Pobór prądu w stanie gotowości	130 mA
Maksymalny pobór prądu	250 mA
Klasa środowiskowa wg EN50130-5	II
Zakres temperatur pracy	-10...+55°C
Maksymalna wilgotność	93 $\pm$ 3%
Wymiary płytki elektroniki	80 x 57 mm
Masa	38 g