ETHM-1 Plus

Ethernetowy moduł komunikacyjny

CE

Wersja oprogramowania 2.07

ethm1_plus_pl 12/20

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
www.satel.pl

WAŻNE

Moduł powinien być instalowany przez wykwalifikowany personel.

Przed przystąpieniem do montażu należy zapoznać się z instrukcją.

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

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:
https://support.satel.pl

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 Zastosowania 2
3 Płytka elektroniki 3
4 Ustawienie adresu 4
4.1 Moduł podłączony do centrali INTEGRA / INTEGRA Plus 4
4.2 Moduł podłączony do centrali VERSA 4
5 Instalacja 4
6 Konfigurowanie ustawień 6
6.1 Moduł podłączony do centrali INTEGRA / INTEGRA Plus 6
6.1.1 ETHM-1 6
6.1.2 Funkcje INT-GSM 11
6.1.3 Filtr IP 11
6.1.4 Funkcje użytkownika 13
6.1.5 Wirtualny manipulator 14
6.1.6 Makropolecenia 15
6.2 Moduł podłączony do centrali VERSA 25
6.2.1 LAN 27
6.2.2 Powiadamianie 27
7 Zdalne programowanie i obsługa centrali za pośrednictwem modułu 29
7.1 Program GUARDX 29
7.1.1 Konfigurowanie ustawień programu GUARDX 30
7.1.2 Zainicjowanie połączenia z programu GUARDX 31
7.1.3 Zainicjowanie połączenia z manipulatora (przez centralę alarmową) 32
7.1.4 Zainicjowanie połączenia przy pomocy wiadomości SMS 32
7.1.5 Nawiązanie połączenia za pośrednictwem serwera SATEL 32
7.2 Przeglądarka WWW 33
7.3 Aplikacja mobilna INTEGRA CONTROL 34
7.3.1 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (Android) 34
7.3.2 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (iOS) 36
7.3.3 Nawiązanie komunikacji 38
8 Dane techniczne 38

1 Wprowadzenie

Moduł ETHM-1 Plus umożliwia centralom alarmowym INTEGRA Plus, INTEGRA i VERSA komunikację przez sieć Ethernet. Transmisja danych jest szyfrowana przy wykorzystaniu zaawansowanego algorytmu opartego o 192-bitowy klucz.

Do modułu ETHM-1 Plus możesz podłączyć moduł INT-GSM / INT-GSM LTE. Pozwoli to na używanie sieci komórkowej danych jako zapasowego toru komunikacji i umożliwi monitoring dwutorowy (Dual path reporting).

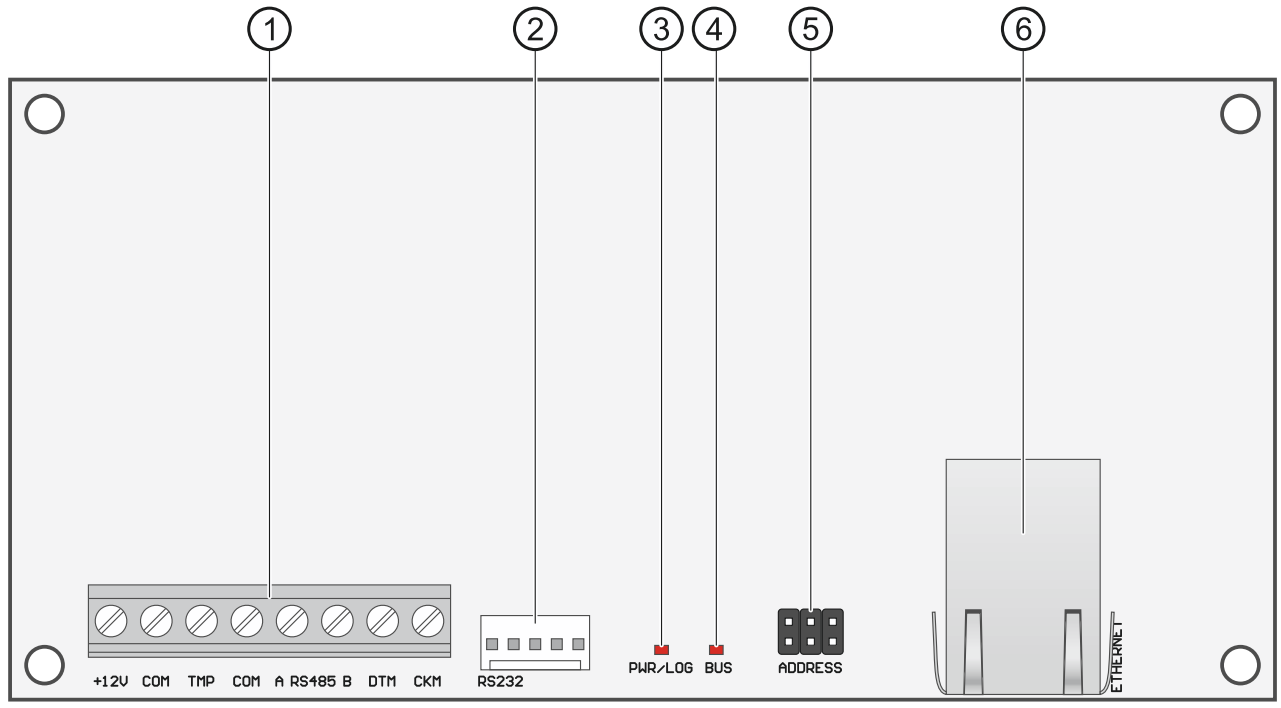
Oprogramowanie modułu może być aktualizowane przy pomocy aplikacji dostępnej na stronie www.satel.pl.

2 Zastosowania

- Konfigurowanie centrali alarmowej przy pomocy programu DLOADX z komputera posiadającego dostęp do Internetu.
  Funkcja dostępna dla central INTEGRA Plus, INTEGRA (wersja oprogramowania 1.03 lub nowsza) i VERSA (wersja oprogramowania 1.01 lub nowsza).
- Zarządzanie systemem alarmowym przy pomocy programu GUARDX z komputera posiadającego dostęp do Internetu.
  Funkcja dostępna dla central INTEGRA Plus i INTEGRA (wersja oprogramowania 1.03 lub nowsza).
- Obsługa i konfigurowanie centrali alarmowej przy pomocy przeglądarki internetowej obsługującej aplikacje JAVA.
  Funkcja dostępna dla central INTEGRA Plus i INTEGRA (wersja oprogramowania 1.03 lub nowsza).
- Obsługa i konfigurowanie centrali alarmowej przy pomocy aplikacji INTEGRA CONTROL z urządzenia mobilnego posiadającego dostęp do Internetu. Urządzenie mobilne pełni rolę dodatkowego manipulatora systemu alarmowego.
  Funkcja dostępna dla central INTEGRA Plus i INTEGRA (wersja oprogramowania 1.03 lub nowsza).
- Obsługa centrali alarmowej przy pomocy aplikacji VERSA CONTROL z urządzenia mobilnego posiadającego dostęp do Internetu.
  Funkcja dostępna dla central VERSA (wersja oprogramowania 1.04 lub nowsza).
- Przesyłanie zdarzeń z centrali alarmowej do stacji monitorującej przez sieć Ethernet. Pozwala to znacząco obniżyć koszty monitoringu.
  Funkcja dostępna dla central INTEGRA Plus, INTEGRA (wersja oprogramowania 1.04 lub nowsza) i VERSA (wersja oprogramowania 1.01 lub nowsza).
- Powiadamianie o zdarzeniach w systemie alarmowym przy pomocy wiadomości e-mail. Treść wiadomości generowana jest automatycznie (w przypadku systemu INTEGRA Plus treść jest zgodna z opisem w pamięci zdarzeń).
  Funkcja dostępna dla central INTEGRA Plus (wersja oprogramowania 1.13 lub nowsza) i VERSA (wersja oprogramowania 1.04 lub nowsza).
- Integracja centrali alarmowej z innymi systemami dzięki otwartemu protokołowi do komunikacji przez sieć Ethernet. Zastosowanie to dedykowane jest dla firm, które zajmują się integracją systemów obiektowych, i wymaga napisania własnego oprogramowania.
  Funkcja dostępna dla central INTEGRA Plus i INTEGRA (wersja oprogramowania 1.06 lub nowsza).

Dodatkowe informacje dotyczące otwartego protokołu komunikacji znajdują się na stronie www.satel.pl.

3 Płytka elektroniki



Rys. 1. Płytka elektroniki modułu.

① zaciski:

+12V - wejście zasilania +12 V DC.

COM - masa.

TMP - wejście sabotażowe (NC) – jeżeli nie jest wykorzystywane, powinno być zwarte do masy.

A RS485 B - port RS-485 umożliwiający podłączenie modułu INT-GSM / INT-GSM LTE. Moduł INT-GSM / INT-GSM LTE jest obsługiwany, jeżeli moduł ETHM-1 Plus podłączony jest do centrali INTEGRA Plus / INTEGRA (wymagana wersja oprogramowania centrali: 1.19 lub nowsza).

DTM - dane (magistrala komunikacyjna).

CKM - zegar (magistrala komunikacyjna).

② port RS-232.

③ dioda LED PWR/LOG:

świeci – obecne zasilanie,

miga – trwa komunikacja za pośrednictwem modułu.

④ dioda LED BUS sygnalizująca miganiem wymianę danych z centralą.

⑤ kołki do ustawienia adresu modułu (patrz: „Ustawienie adresu”).

⑥ gniazdo RJ-45 do podłączenia sieci Ethernet. Wyposażone jest w dwie diody LED:

zielona – świeci, gdy moduł jest podłączony do sieci,

żółta – miga podczas transmisji danych.

4 Ustawienie adresu

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.

4.1 Moduł podłączony do centrali INTEGRA / INTEGRA Plus

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 INTEGRA Plus.

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

4.2 Moduł podłączony do centrali VERSA

Ustaw w module adres 4. Do centrali nie może być podłączony manipulator o adresie 4.

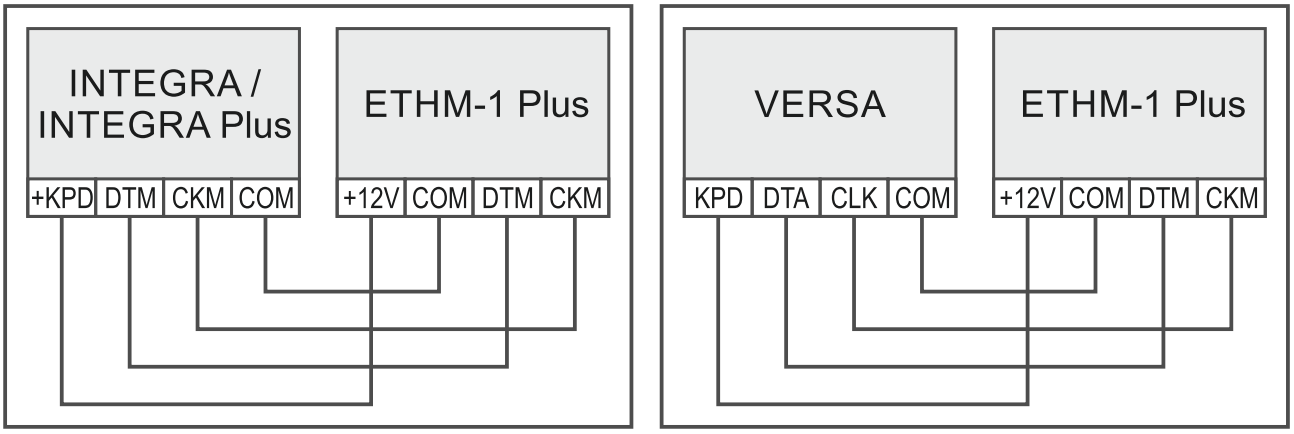
5 Instalacja

Wszystkie połączenia elektryczne należy wykonywać przy wyłączonym zasilaniu.

Urządzenie przeznaczone jest do pracy wyłącznie w lokalnych sieciach komputerowych (LAN). Nie może być podłączane bezpośrednio do publicznej sieci komputerowej (MAN, WAN). Połączenie z siecią publiczną należy realizować za pośrednictwem routera lub modemu xDSL.

Urządzenie należy instalować w pomieszczeniach zamkniętych o normalnej wilgotności powietrza.

1. Zamocuj płytkę elektroniki modułu w obudowie. Moduł powinien być montowany w tej samej obudowie, co centrala alarmowa. Ułatwi to połączenie portów RS-232 centrali i modułu, co jest wymagane, jeżeli centrala ma być konfigurowana przez sieć Ethernet przy pomocy programu DLOADX.
2. Ustaw adres modułu (patrz: „Ustawienie adresu").
3. Zaciski +12V, COM, DTM i CKM modułu połącz z zaciskami centrali alarmowej (rys. 2). Do wykonania połączenia zaleca się stosowanie kabla prostego nieekranowanego. Jeśli użyjesz kabla typu „skrętka", pamiętaj, że jedną parą skręconych przewodów nie wolno przesyłać sygnałów CKM (zegar) i DTM (dane). Przewody muszą być prowadzone w jednym kablu.
4. 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.



Rys. 2. Sposób podłączenia modułu do centrali alarmowej.

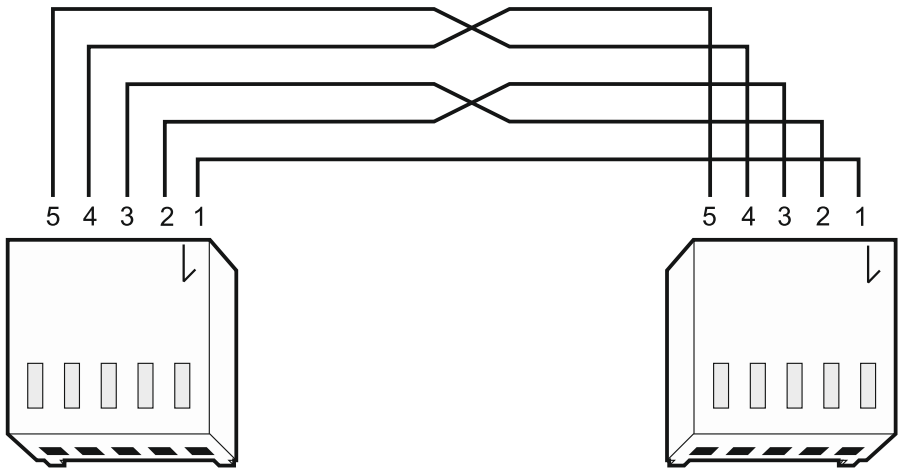
5. Podłącz moduł do sieci Ethernet. Użyj kabla zgodnego ze standardem 100Base-TX (identycznego jak przy podłączaniu do sieci komputera).
6. Włącz zasilanie systemu alarmowego.
7. Uruchom w centrali alarmowej funkcję identyfikacji (patrz: instrukcja instalatora centrali alarmowej). Moduł zostanie zidentyfikowany jako „ETHM-1" albo „ETHM+GSM" (jeżeli do portu RS-485 podłączony jest moduł INT-GSM / INT-GSM LTE).
8. Skonfiguruj moduł (patrz: „Konfiguracja").
9. Jeżeli centrala alarmowa ma być konfigurowana 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 PIN5: **PIN5/PIN5** (rys. 3)

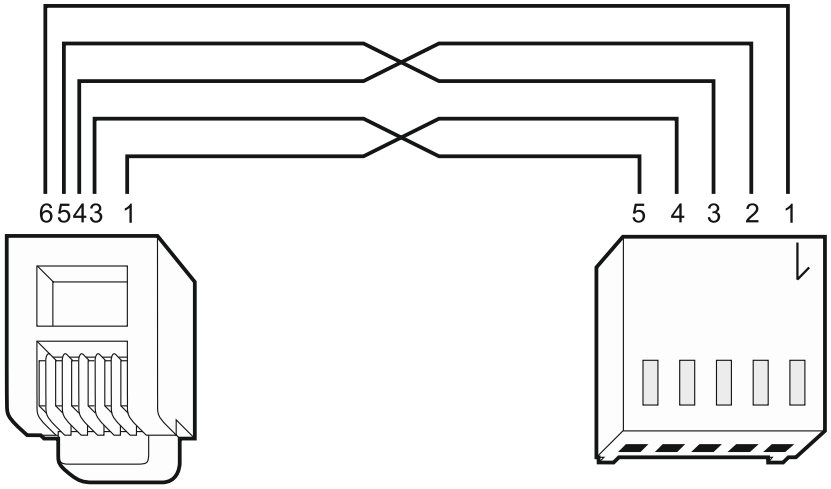
   INTEGRA z gniazdem typu RJ / INTEGRA Plus: **RJ/PIN5** (rys. 4)

   VERSA: **PIN5/RJ-TTL**

   Wymienione kable dostępne są w ofercie firmy SATEL.



Rys. 3. Schemat kabla służącego do połączenia portów RS-232 modułu ETHM-1 Plus i centrali INTEGRA z gniazdem PIN5.



Rys. 4. Schemat kabla służącego do połączenia portów RS-232 modułu ETHM-1 Plus i centrali INTEGRA / INTEGRA Plus z gniazdem typu RJ.

6 Konfigurowanie ustawień

Ustawienia modułu różnią się w zależności od centrali, do której moduł jest podłączony.

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.

6.1 Moduł podłączony do centrali INTEGRA / INTEGRA Plus

Ustawienia modułu możesz skonfigurować przy pomocy:

- programu DLOADX: →okno „Struktura" →zakładka „Sprzęt" →gałąź „Manipulatory" →*[nazwa modułu],*
- manipulatora: ▶TRYB SERWISOWY ▶STRUKTURA ▶SPRZĘT ▶MANIPULATORY ▶USTAWIENIA ▶*[nazwa modułu].*

Wszystkie ustawienia możesz skonfigurować tylko przy pomocy programu DLOADX.

Jeżeli moduł został zidentyfikowany jako „ETHM+GSM" (do modułu ETHM-1 Plus podłączony jest moduł INT-GSM / INT-GSM LTE), moduł INT-GSM / INT-GSM LTE przejmuje zadania modułu ETHM-1 Plus w przypadku braku sieci Ethernet. Zadania te są realizowane przez sieć komórkową danych. W związku z tym wiele opcji i parametrów dotyczy obu modułów. Pamiętaj o tym podczas konfigurowania ustawień.

6.1.1 ETHM-1

Nazwa – indywidualna nazwa urządzenia (do 16 znaków).

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

Ustawienia sieciowe

Uzyskaj adres IP automatycznie (DHCP) [Użyć DHCP] – jeżeli opcja jest włączona, moduł automatycznie pobiera z serwera DHCP dane dotyczące adresu IP, maski podsieci i bramy (parametrów tych wówczas się nie programuje).

Adres IP przydzielony modułowi możesz odczytać:

- *w manipulatorze: przy pomocy funkcji użytkownika **IP/MAC/IMEI/ID** dostępnej w podmenu TESTY. Opis korzystania z funkcji znajdziesz w instrukcji użytkownika centrali alarmowej.*
- *w programie DLOADX: poniżej parametrów i opcji modułu (rys. 5 i 6).*

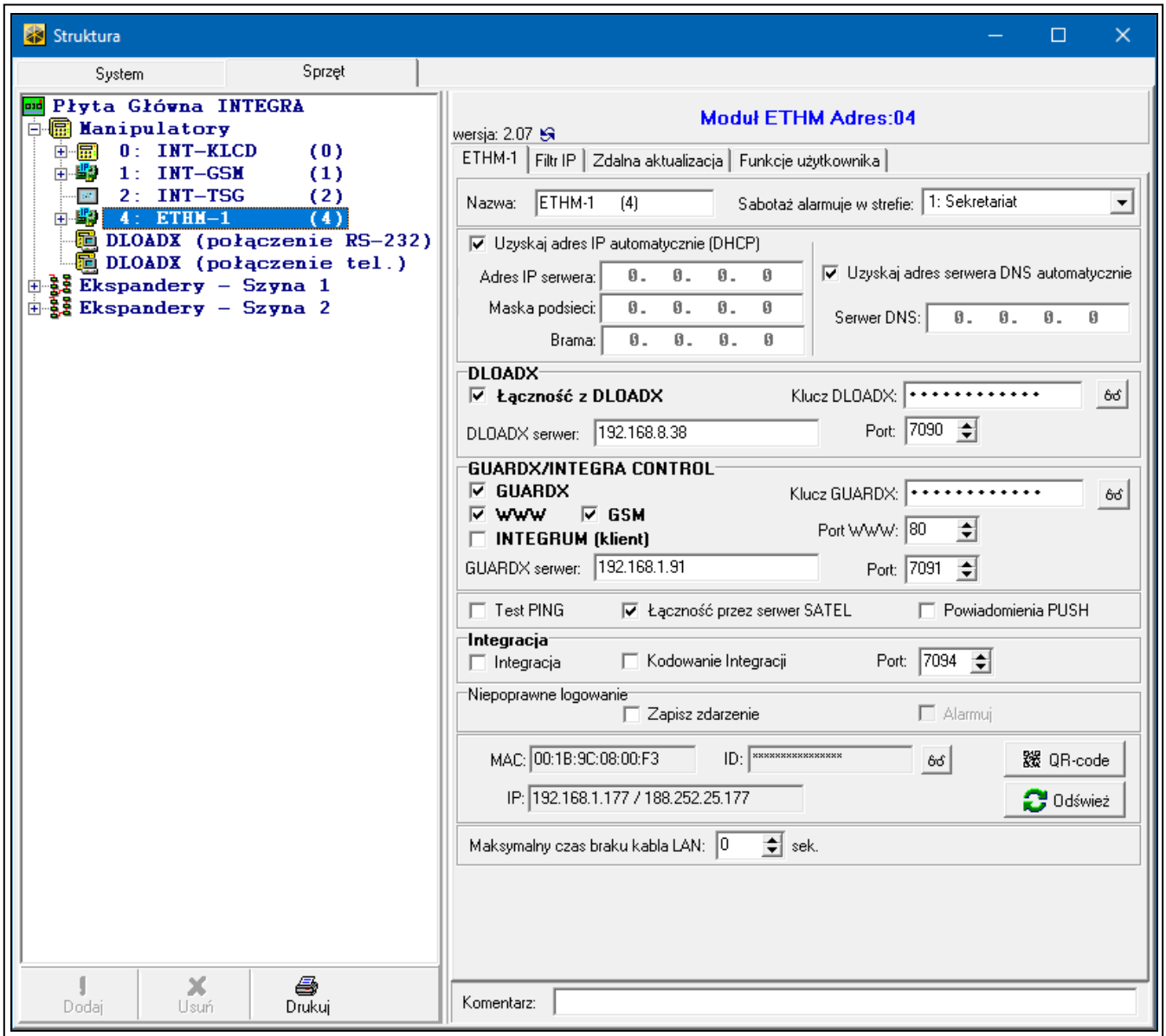
Adres IP serwera – adres IP modułu.

Maska podsieci – maska podsieci, w której pracuje moduł.

Brama – adres IP urządzenia sieciowego, za pośrednictwem którego pozostałe urządzenia z danej sieci lokalnej komunikują się z urządzeniami w innych sieciach.

Uzyskaj adres serwera DNS automatycznie [Użyć DHCP-DNS] – jeżeli opcja jest włączona, adres IP serwera DNS jest pobierany automatycznie z serwera DHCP. Opcja dostępna, jeśli opcja UZYSKAJ ADRES IP AUTOMATYCZNIE (DHCP) jest włączona.

Serwer DNS – adres IP serwera DNS, którego ma używać moduł. Można go zaprogramować, jeżeli opcja UZYSKAJ ADRES SERWERA DNS AUTOMATYCZNIE jest wyłączona.



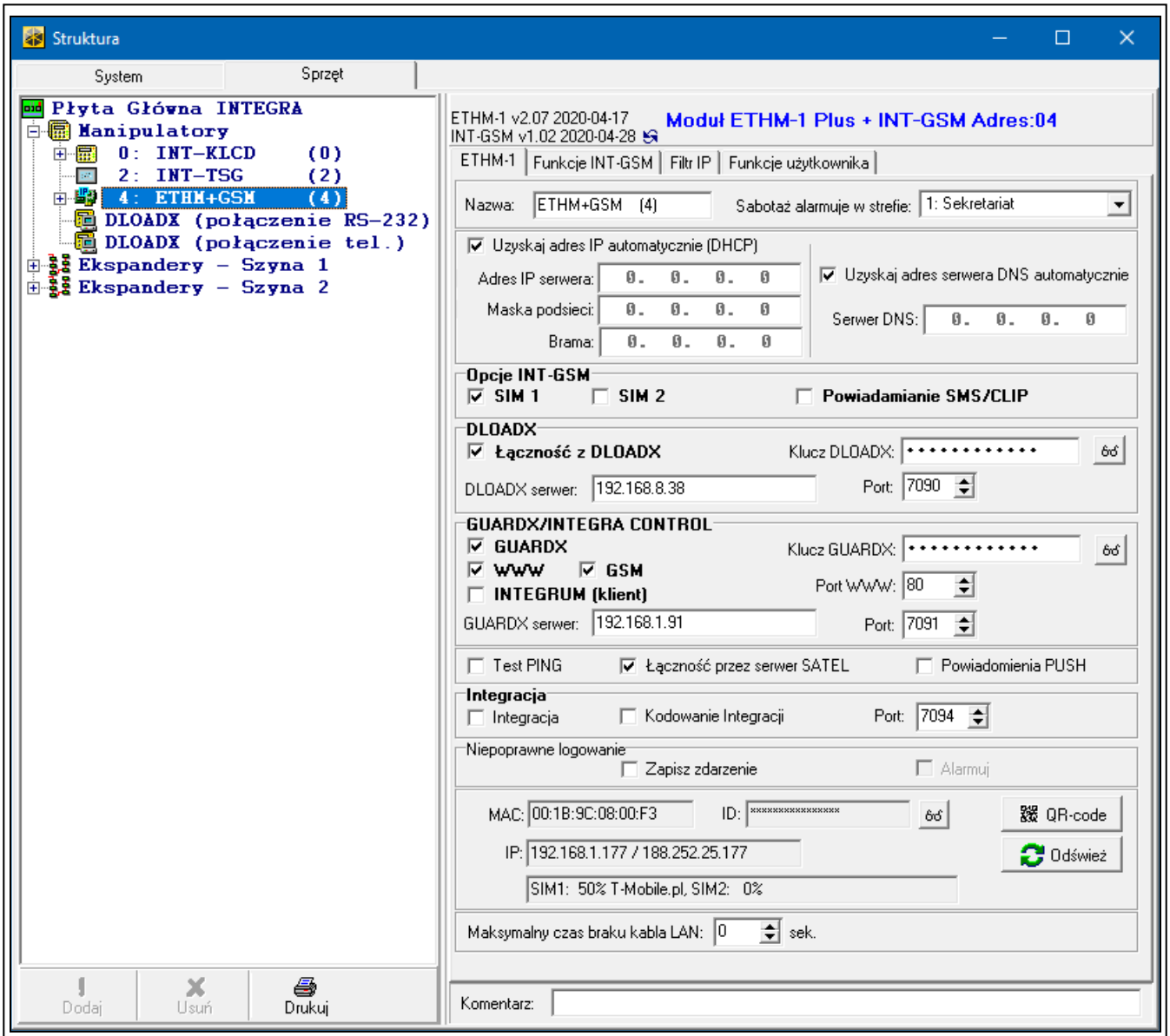
Rys. 5. Program DLOADX: ustawienia modułu podłączonego do centrali INTEGRA / INTEGRA Plus (moduł zidentyfikowany jako „ETHM-1”).

Opcje INT-GSM

Opcje dotyczące modułu INT-GSM / INT-GSM LTE są dostępne, gdy moduł INT-GSM / INT-GSM LTE jest podłączony do modułu ETHM-1 Plus (moduł zidentyfikowany jako „ETHM+GSM").

SIM 1 / **SIM 2** [SIM1 / SIM2] – jeżeli opcja jest włączona, moduł INT-GSM / INT-GSM LTE 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/CLIP [Powiadam. SMS] – jeżeli opcja jest włączona, moduł INT-GSM / INT-GSM LTE może powiadamiać o zdarzeniach dotyczących systemu alarmowego przy pomocy SMS/CLIP.



Rys. 6. Program DLOADX: ustawienia modułu podłączonego do centrali INTEGRA / INTEGRA Plus (moduł zidentyfikowany jako „ETHM+GSM" – do modułu ETHM-1 Plus podłączony jest moduł INT-GSM).

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

DLOADX serwer [Adres DLOADX] – adres komputera z programem DLOADX. Jeżeli komunikacja odbywa się w sieci rozległej, 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).

WWW [Z Internetu] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między przeglądarką internetową a centralą alarmową za pośrednictwem modułu. Opcja jest niedostępna, gdy włączona jest opcja INTEGRUM (KLIENT).

GSM [Z GSM] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między aplikacją INTEGRA CONTROL / serwerem INTEGRUM a centralą alarmową za pośrednictwem modułu. Opcja jest niedostępna, gdy włączona jest opcja INTEGRUM (KLIENT).

INTEGRUM (klient) [INTEGRUM] – jeżeli opcja jest włączona, moduł inicjuje łączność z serwerem INTEGRUM, aby ustanowić komunikację między centralą a serwerem INTEGRUM. Ten sposób nawiązania komunikacji jest wspierany przez serwer INTEGRUM w wersji 2.0 (lub nowszej). Adres serwera INTEGRUM wprowadź w polu GUARDX SERWER, a numer portu komunikacyjnego w polu PORT. Gdy opcja jest włączona, opcje GUARDX, WWW i GSM są niedostępne (moduł nie obsługuje programu GUARDX / przeglądarki internetowej / aplikacji INTEGRA CONTROL).

GUARDX serwer [Adres GUARDX] – adres komputera z programem GUARDX lub serwera INTEGRUM. Jeżeli komunikacja odbywa się w sieci rozległej, musi to być adres publiczny. Możesz wpisać adres IP lub nazwę domeny.

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 szyfrowania danych podczas komunikacji z:

- programem GUARDX,
- aplikacją JAVA w przeglądarce internetowej,
- aplikacją INTEGRA CONTROL w urządzeniu mobilnym,
- systemem INTEGRUM.

Port WWW – numer portu TCP używanego do komunikacji z przeglądarką internetową. Możesz wprowadzić wartość z zakresu od 1 do 65535. Musi ona być różna od wprowadzonej dla pozostałych portów. Domyślnie: 80.

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

- programem GUARDX,

- aplikacją JAVA w przeglądarce internetowej,
- aplikacją INTEGRA CONTROL w urządzeniu mobilnym,
- systemem INTEGRUM.

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

Port nie może być wykorzystywany przez wiele usług w tym samym czasie. Z portu może korzystać tylko jedna usługa (np. jeżeli trwa komunikacja z serwerem INTEGRUM, nie można połączyć się z centralą przy pomocy programu GUARDX, przeglądarki internetowej i aplikacji INTEGRA CONTROL).

Test PING

Test PING – jeżeli opcja jest włączona, moduł może testować komunikację przy pomocy komendy ping wysyłanej do wskazanego urządzenia sieciowego. Parametry dotyczące testowania komunikacji programuje się w centrali alarmowej:

manipulator: ▶TRYB SERWISOWY ▶OPCJE ▶TEST PING,

program DLOADX: →okno „Struktura” →zakładka „Sprzęt” →gałąź ”Manipulatory”.

Serwer SATEL

Łączność przez serwer SATEL [Serwer SATEL] – jeżeli opcja jest włączona, moduł łączy się z serwerem SATEL i za pośrednictwem serwera SATEL można nawiązać komunikację z centralą (Usługa Zestawiania Połączeń). Ten sposób komunikacji nie wymaga dodatkowego konfigurowania urządzenia sieciowego, za pośrednictwem którego moduł łączy się z siecią publiczną.

Nawiązanie komunikacji z serwerem SATEL wymaga użycia serwera DNS.

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

Powiadomienia PUSH – jeżeli opcja jest włączona, aplikacja INTEGRA CONTROL może informować o zdarzeniach w systemie alarmowym przy pomocy powiadomień push.

Integracja

Integracja – jeżeli opcja jest włączona, moduł może być używany do integracji centrali alarmowej z innymi systemami.

Kodowanie integracji [Int. kodowana] – gdy opcja jest włączona, komunikacja z innymi systemami jest kodowana. Klucz kodowania integracji programuje się w centrali alarmowej:

manipulator: ▶TRYB SERWISOWY ▶OPCJE ▶KLUCZ INTEGRAC.,

program DLOADX: →okno „Opcje” →zakładka „Serwis”.

Port [Port integracji] – numer portu TCP używanego do integracji. Możesz wprowadzić wartość z zakresu od 1 do 65535. Musi ona być różna od wprowadzonej dla pozostałych portów. Domyślnie: 7094.

Niepoprawne logowanie

Zapisz zdarzenie [Włam. – zdarz.] – jeżeli opcja jest włączona, wszystkie nieautoryzowane próby połączenia z modułem są zapisywane w pamięci zdarzeń.

Alarmuj [Włam. – alarm] – gdy opcja jest włączona, nieautoryzowana próba połączenia z modułem wywoła alarm sabotażowy. Opcja dostępna, jeśli opcja ZAPISZ ZDARZENIE jest włączona.

Informacje

MAC – adres sprzętowy modułu.

ID – indywidualny numer identyfikacyjny przydzielony modułowi 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 ZMIEŃ ID dostępnej w manipulatorze (▶TRYB SERWISOWY ▶STRUKTURA ▶SPRZĘT ▶MANIPULATORY ▶USTAWIENIA ▶[nazwa modułu] ▶ZMIEŃ ID). Po skasowaniu dotychczasowego numeru ID moduł otrzyma nowy. Aplikacje INTEGRA CONTROL używające starego numeru ID nie będą mogły połączyć się z centralą.

IP – adres lokalny / adres publiczny modułu.

[Sygnał sieci komórkowej] – informacja o poziomie sygnału komórkowego i operatorze sieci komórkowej. Informacja wyświetlana, gdy moduł INT-GSM / INT-GSM LTE jest podłączony do modułu ETHM-1 Plus (moduł zidentyfikowany jako „ETHM+GSM").

QR-code – 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 i przekazać użytkownikom. Kod QR upraszcza konfigurowanie ustawień aplikacji INTEGRA CONTROL.

Odśwież – kliknij, aby odświeżyć wszystkie informacje.

Maksymalny czas braku kabla LAN – jeżeli przez zaprogramowany czas nie będzie sieci Ethernet, moduł zgłosi awarię. Opóźnienie zgłaszania awarii zapobiega informowaniu o krótkotrwałych brakach sieci Ethernet.

6.1.2 Funkcje INT-GSM

Ustawienia te dotyczą modułu INT-GSM / INT-GSM LTE. Są dostępne, gdy moduł INT-GSM / INT-GSM LTE jest podłączony do modułu ETHM-1 Plus (moduł zidentyfikowany jako „ETHM+GSM"). Opis tych ustawień znajdziesz w instrukcji modułu INT-GSM / INT-GSM LTE.

6.1.3 Filtr IP

Moduł podłączony do centrali INTEGRA / INTEGRA Plus z wersją oprogramowania 1.15 (lub nowszą) oferuje filtr IP. Używając filtrowania IP możesz podnieść poziom bezpieczeństwa systemu alarmowego. Nawiązanie połączenia z modułem ethernetowym (centralą alarmową) będzie możliwe tylko z określonych adresów IP lub podsieci. Filtrowanie IP nie dotyczy komunikacji za pośrednictwem serwera SATEL.

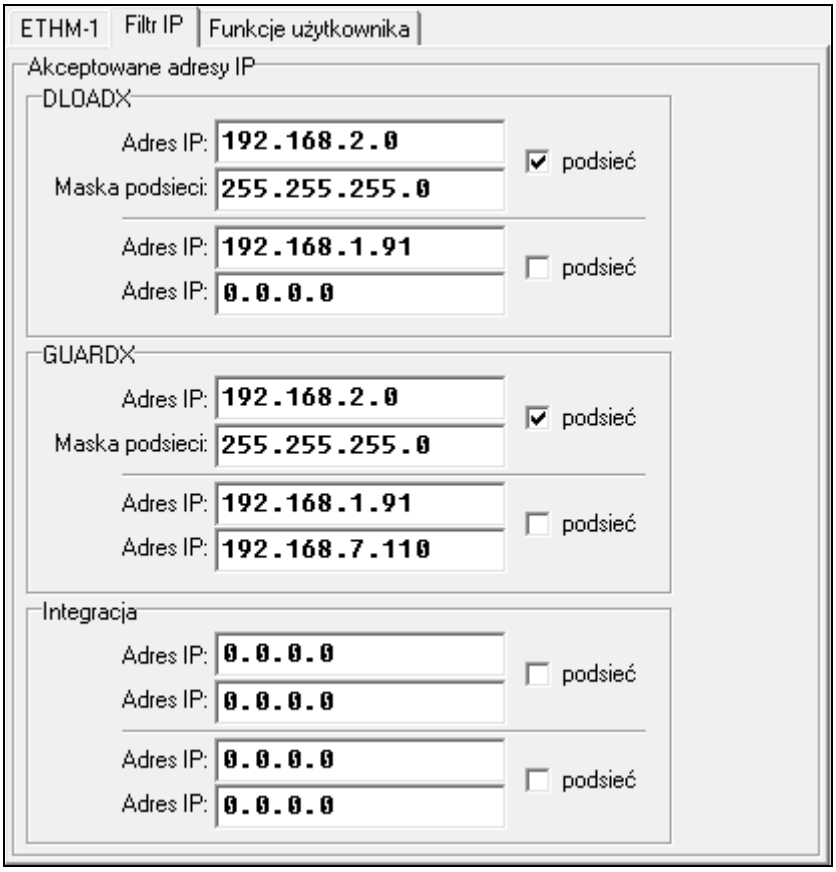
Możesz skonfigurować filtrowanie IP dla połączeń przychodzących:

- z programu DLOADX,
- z programu GUARDX (dotyczy także przeglądarki WWW, aplikacji mobilnej i systemu INTEGRUM),
- w ramach integracji.

W każdym przypadku możesz zdefiniować zasady filtrowania w jednej z poniższych konfiguracji:

- do 4 dozwolonych adresów IP,
- 1 dozwolona podsieć i do 2 dozwolonych adresów IP,
- do 2 dozwolonych podsieci.

Funkcja filtrowania jest aktywna po wpisaniu wartości w dowolnym z czterech pól dostępnych dla danego typu połączeń przychodzących.



Rys. 7. Program DLOADX: zakładka „Filtr IP”.

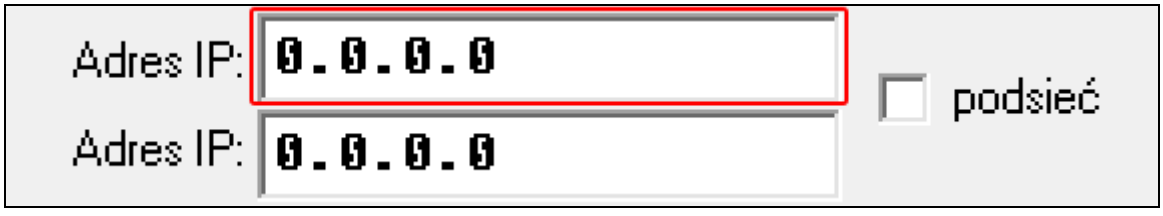
Adres IP – jeżeli opcja PODSIEĆ jest wyłączona: adres sieciowy, z którego można nawiązać połączenie z modułem ethernetowym. Jeżeli opcja PODSIEĆ jest włączona: adres IP służący do określenia podsieci, z której można nawiązać połączenie z modułem ethernetowym.

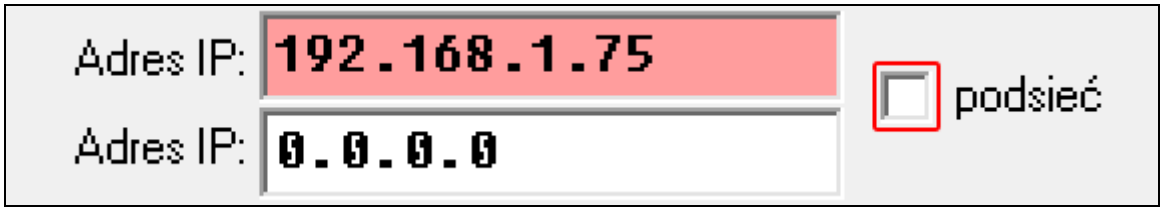
podsieć – jeżeli opcja jest włączona, możesz określić podsieć, z której moduł będzie odbierał połączenia przychodzące.

Maska podsieci – maska służąca do wyodrębnienia w adresie IP części określającej podsieć.

Filtrowanie według adresu IP

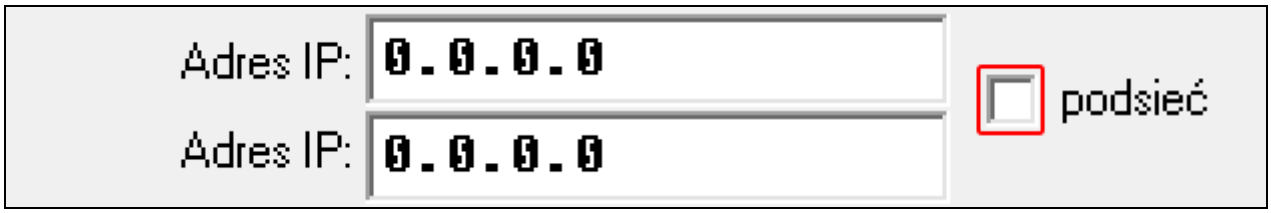
W polu ADRES IP wprowadź adres sieciowy, z którego ma być możliwe nawiązanie połączenia z modułem (centralą). Opcja PODSIEĆ z prawej strony pola nie może być zaznaczona.

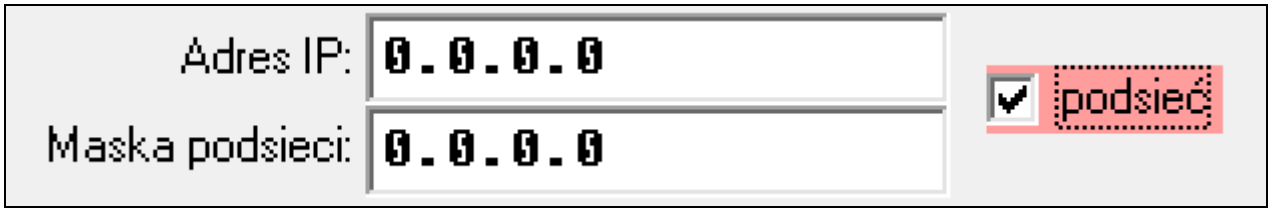




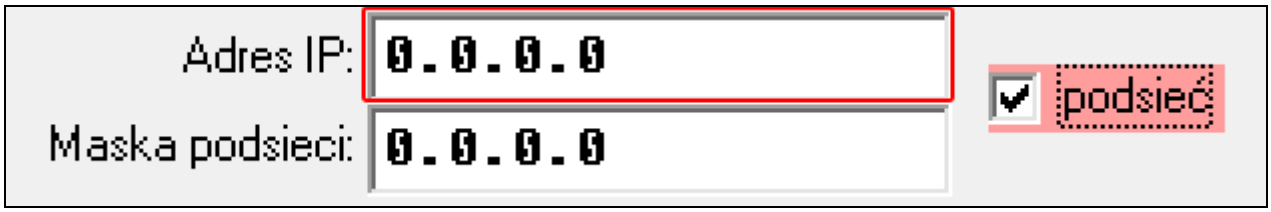
Filtrowanie według podsieci

1. Zaznacz opcję PODSIEĆ. Opis jednego z pól ADRES IP zmieni się na MASKA PODSIECI. Pola ADRES IP i MASKA PODSIECI tworzą od tej chwili parę.

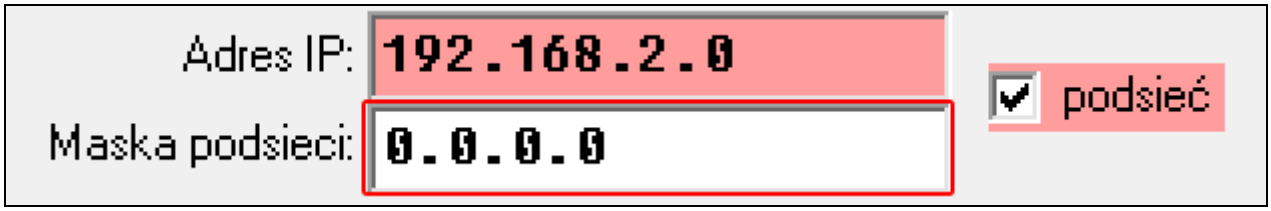


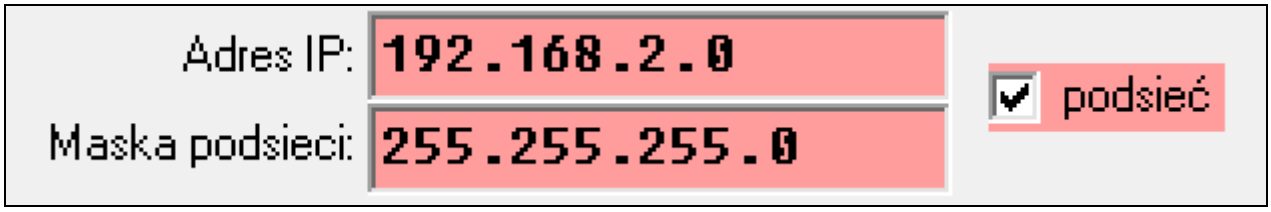


2. Wprowadź adres, który posłuży do określenia podsieci.



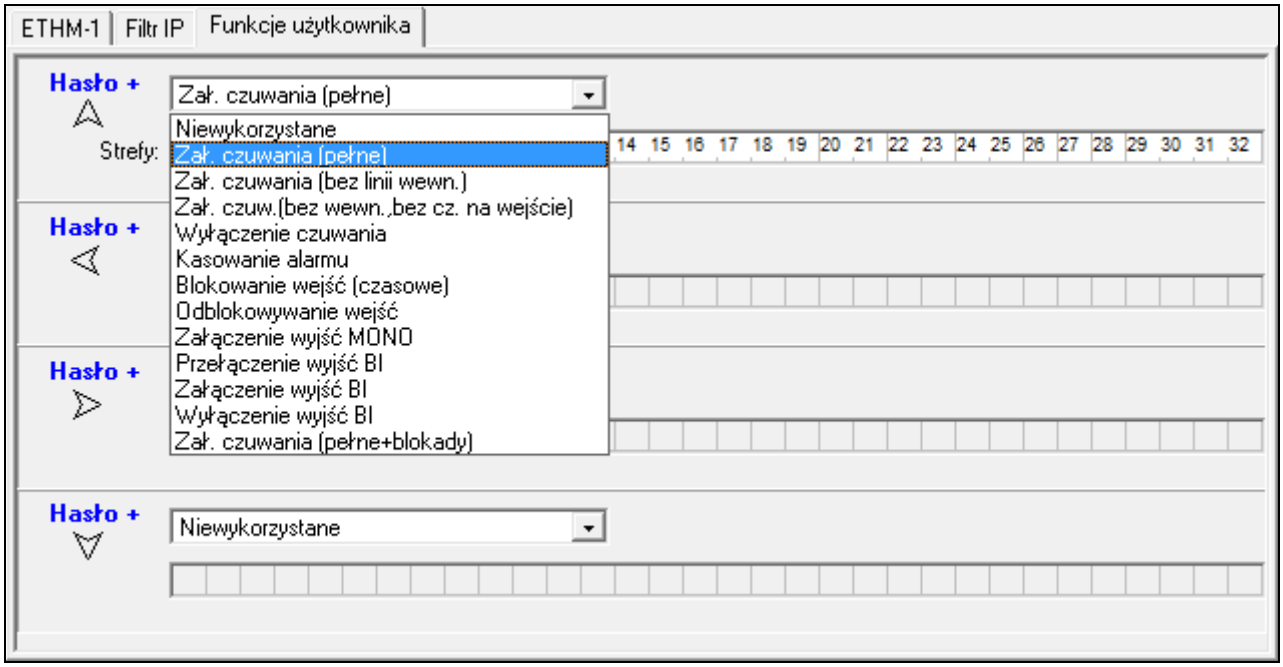
3. Wprowadź maskę, która posłuży do wyodrębnienia w adresie IP części określającej podsieć.





6.1.4 Funkcje użytkownika

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



Rys. 8. Program DLOADX: zakładka „Funkcje użytkownika”.

6.1.5 Wirtualny manipulator

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

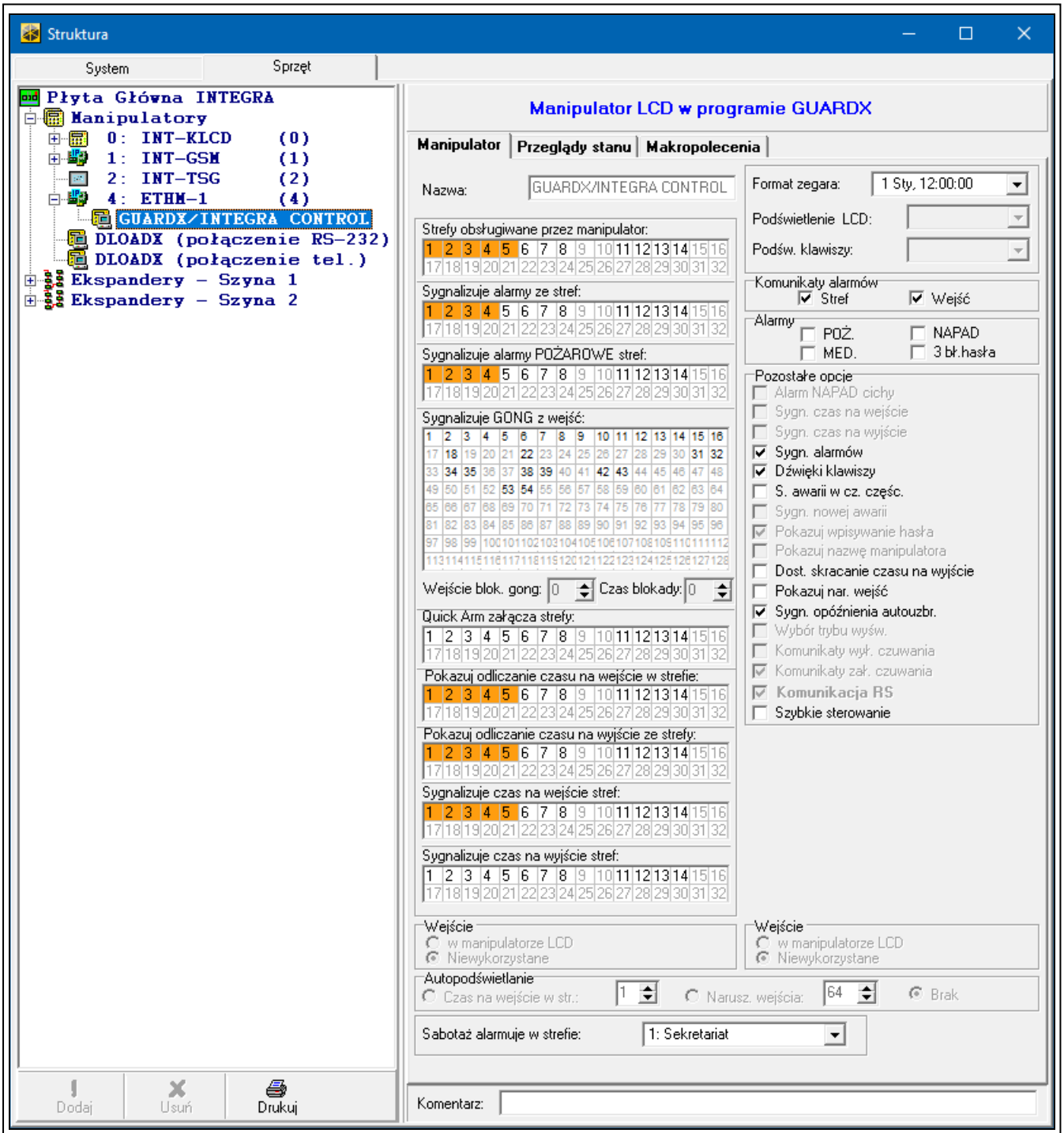
Parametry i opcje wirtualnego manipulatora dostępnego w programie DLOADX można zaprogramować przy pomocy:

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

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

- manipulatora: ▶TRYB SERWISOWY ▶STRUKTURA ▶SPRZĘT ▶MANIPULATORY ▶USTAWIENIA ▶GUARDX ADRES n [n = adres modułu],
- programu DLOADX: →okno „Struktura” →zakładka „Sprzęt” →gałąź „Manipulatory” →*[nazwa modułu]* →gałąź „GUARDX/INTEGRA CONTROL” (rys. 9).

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).



Rys. 9. Program DLOADX: parametry i opcje wirtualnego manipulatora dostępnego w programie GUARDX, przeglądarce WWW lub urządzeniu mobilnym.

6.1.6 Makropolecenia

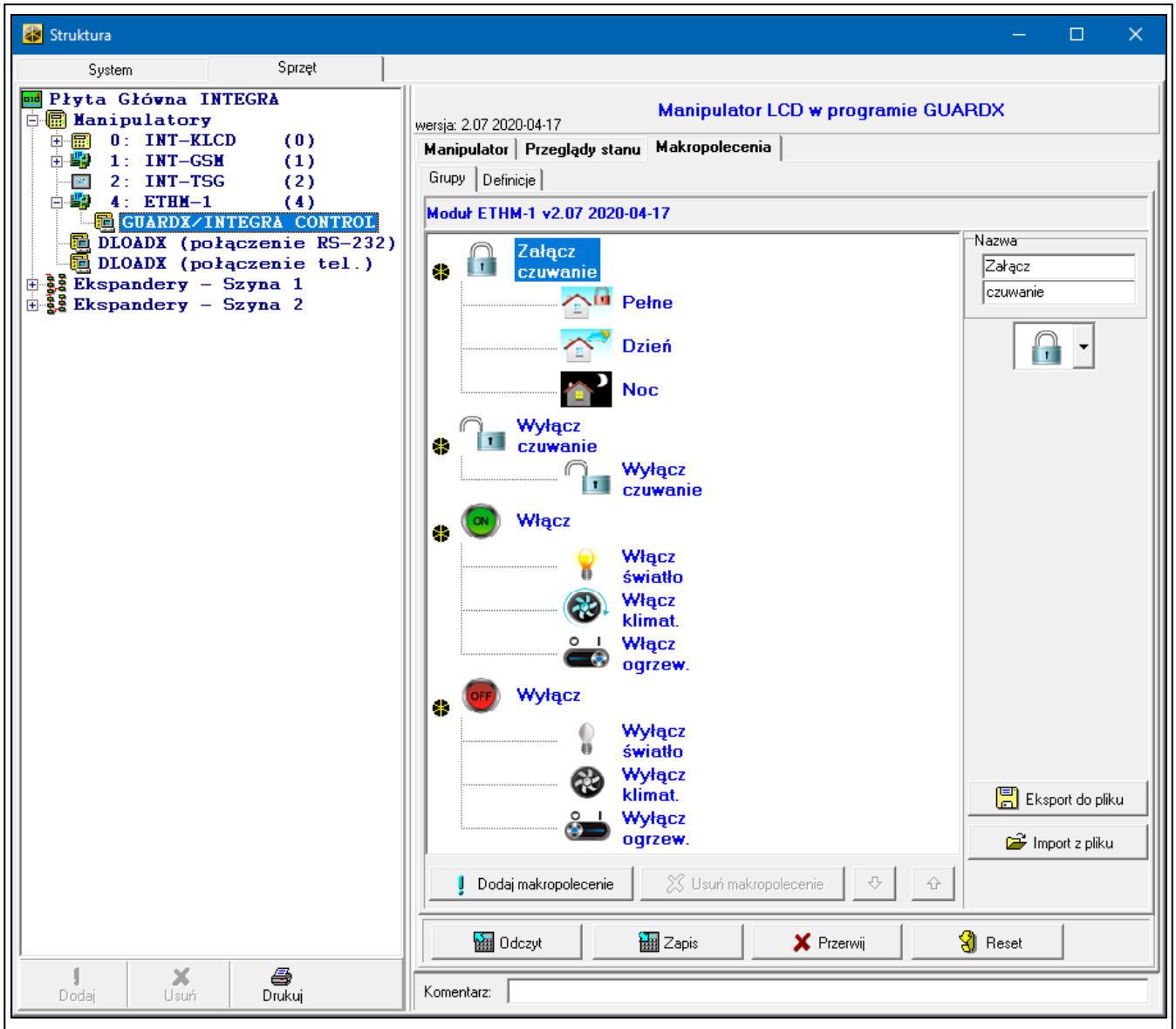
Aplikacja INTEGRA CONTROL pozwala na sterowanie systemem alarmowym przy pomocy makropoleceń, co umożliwia szybkie i łatwe uruchamianie szeregu różnych funkcji po dotknięciu zaledwie kilku klawiszy. Makropolecenia można zdefiniować w programie DLOADX (→okno „Struktura" →zakładka „Sprzęt" →gałąź „Manipulatory"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

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

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 ETHM-1 Plus, 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.*

Grupy



Rys. 10. Program DLOADX: zakładka „Grupy".

Makropolecenia, które mają być dostępne dla użytkowników aplikacji mobilnej, 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.

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

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

Usuń makropolecenie – kliknij, żeby usunąć z grupy zaznaczone makropolecenie.

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

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

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).

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

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

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.

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 pojawią się komunikaty informujące o wykonaniu polecenia lub o błędzie (wciąż wyświetlany będzie ekran, z którego uruchomiono makropolecenie).

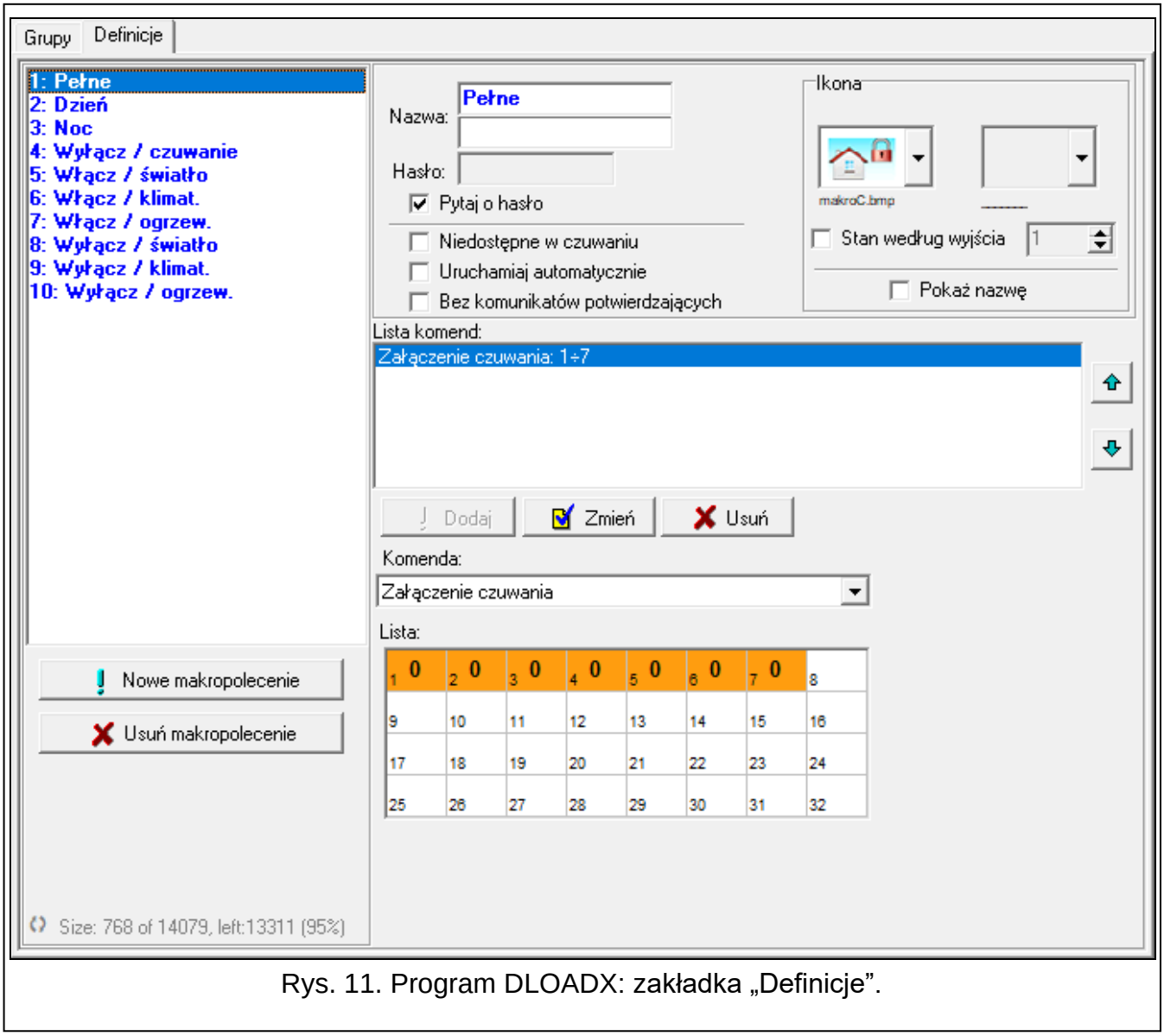
Ikona

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.



Rys. 11. Program DLOADX: zakładka „Definicje”.

Komendy

Lista komend – komendy przypisane do aktualnie zaznaczonego makropolecenia. Przyciski  i  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:

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.

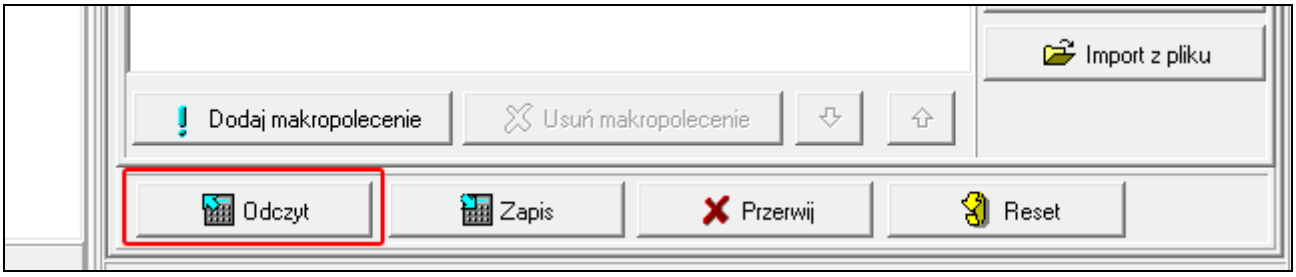
Wejścia nie mogą mieć włączonej opcji UŻYTKOWNIK NIE BLOKUJE.

Wyjścia muszą być typu 24. PRZEŁĄCZNIK MONO, 25. PRZEŁĄCZNIK BI, 105. ROLETA W GÓRĘ, 106. ROLETA W DÓŁ lub PRZEKAŹNIK TELEFONICZNY (nie muszą być przypisane do żadnej grupy wyjść).

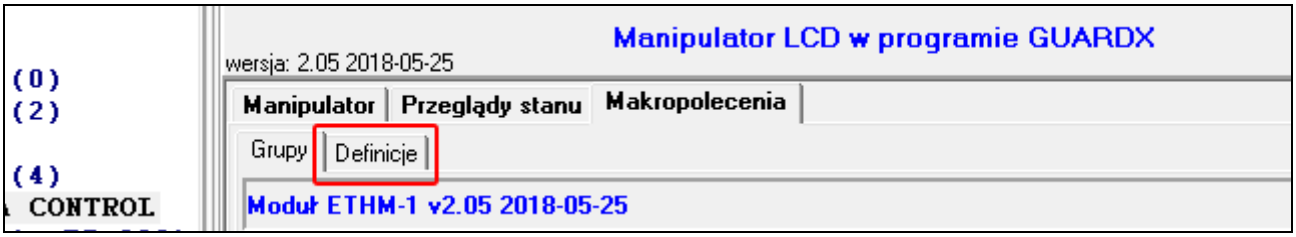
Przy pomocy aplikacji INTEGRA CONTROL można sterować systemem KNX, jeżeli do centrali podłączony jest moduł INT-KNX.

Definiowanie makropoleceń

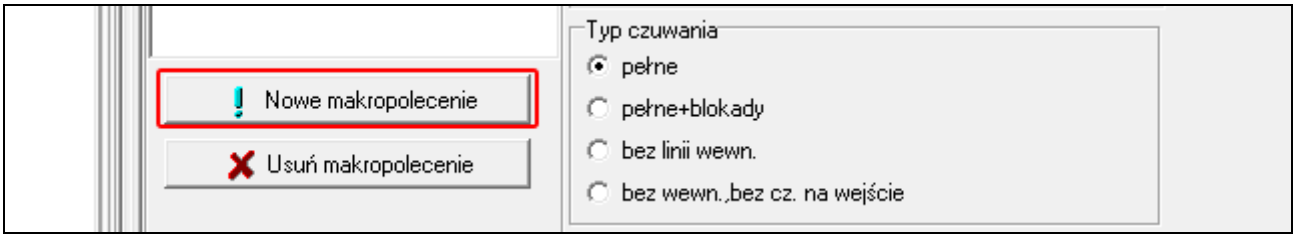
1. Kliknij na przycisk „Odczyt”, żeby odczytać z modułu dane dotyczące makropoleceń.



2. Kliknij na zakładkę „Definicje”.

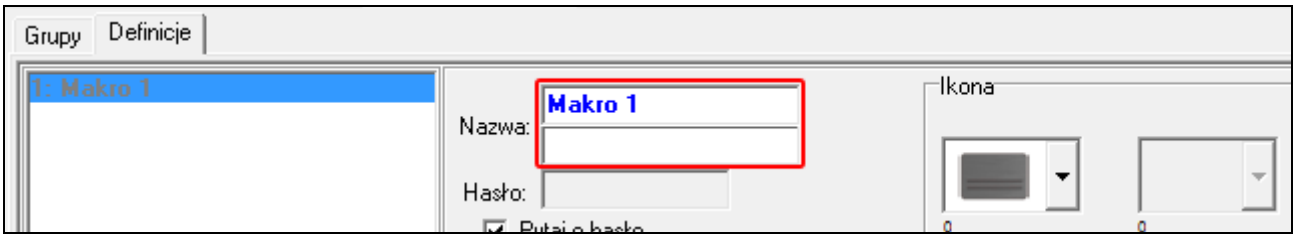


3. Kliknij na przycisk „Nowe makropolecenie”. Na liście pojawi się nowe makropolecenie.

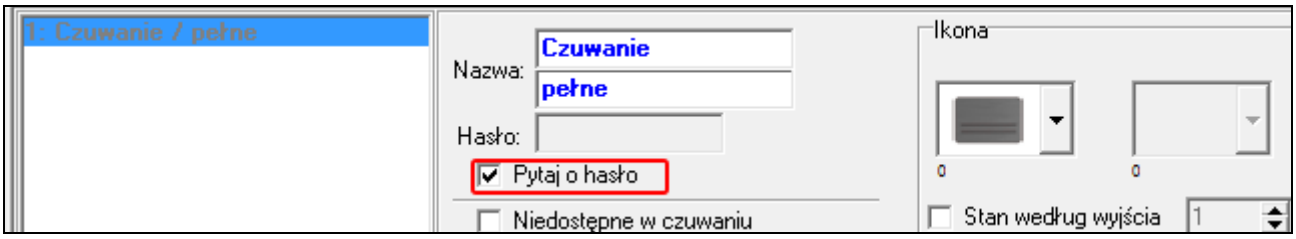




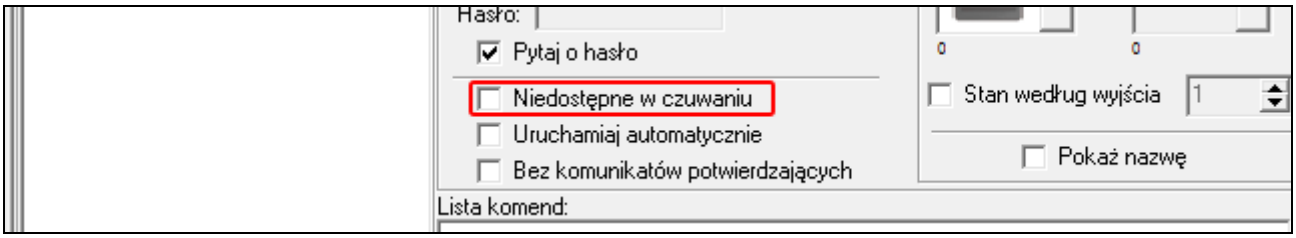
4. Wprowadź nazwę nowego makropolecenia.



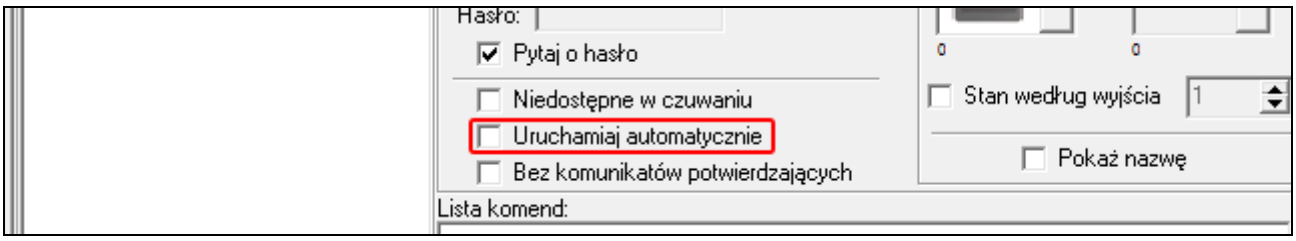
5. Jeżeli uruchomienie makropolecenia ma być każdorazowo poprzedzane autoryzacją użytkownika, włącz opcję PYTAJ O HASŁO.



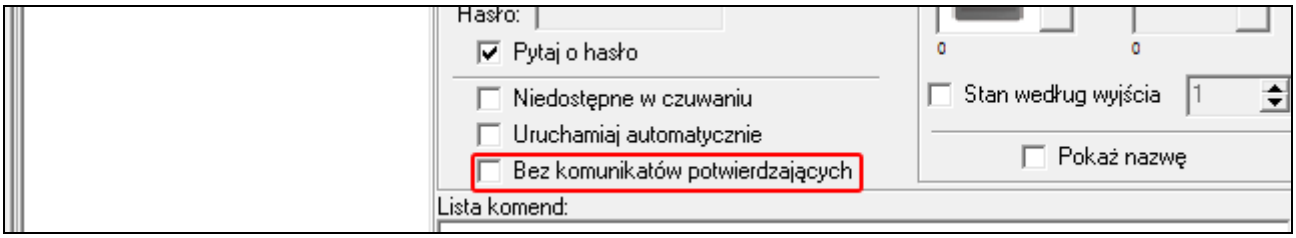
6. Jeżeli makropolecenie ma być niedostępne, gdy czuwa dowolna ze stref obsługiwanych przez manipulator, włącz opcję NIEDOSTĘPNE W CZUWANIU.



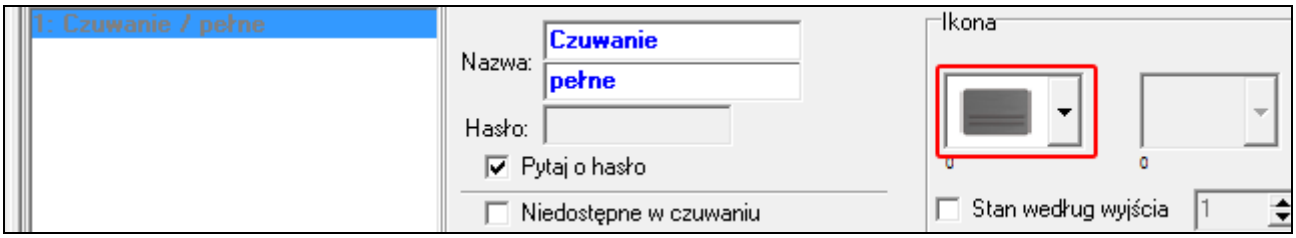
7. Jeżeli makropolecenie ma być dostępne bez wchodzenia do grupy, włącz opcję URUCHAMIAJ AUTOMATYCZNIE.



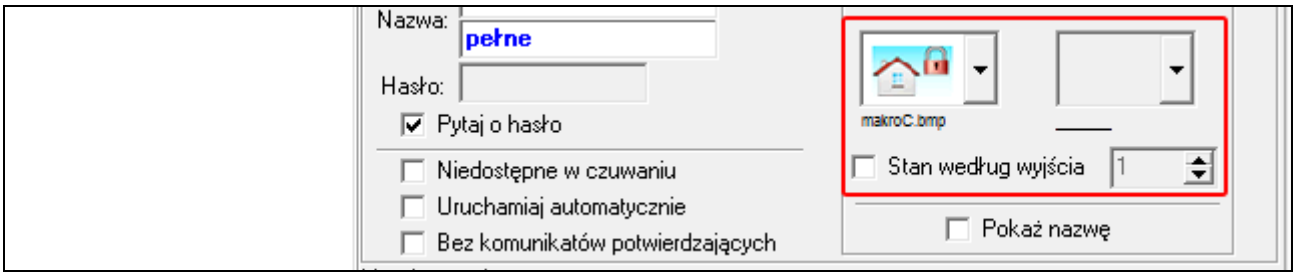
8. Jeżeli po uruchomieniu makropolecenia nie mają być wyświetlane komunikaty potwierdzające, włącz opcję BEZ KOMUNIKATÓW POTWIERDZAJĄCYCH.



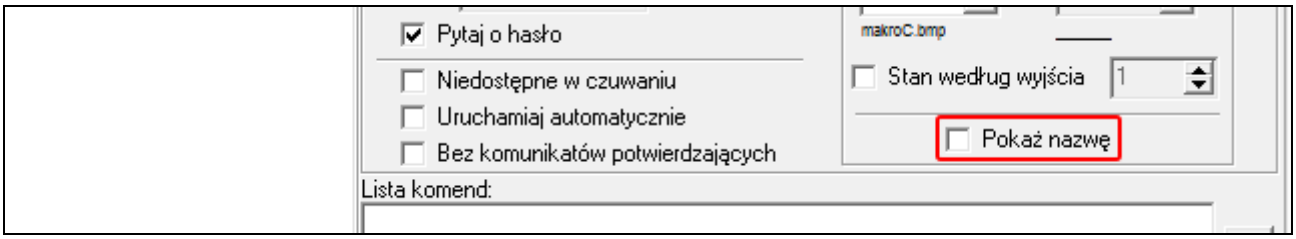
9. Kliknij na przycisk  i wybierz ikonę dla makropolecenia.



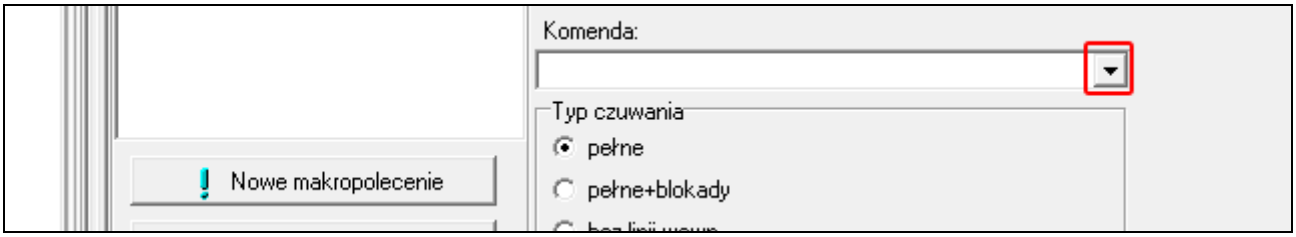
10. Jeżeli ikona ma się zmieniać w zależności od stanu wybranego wyjścia:
   - włącz opcję STAN WEDŁUG WYJŚCIA,
   - wskaż numer wyjścia,
   - wybierz ikony.

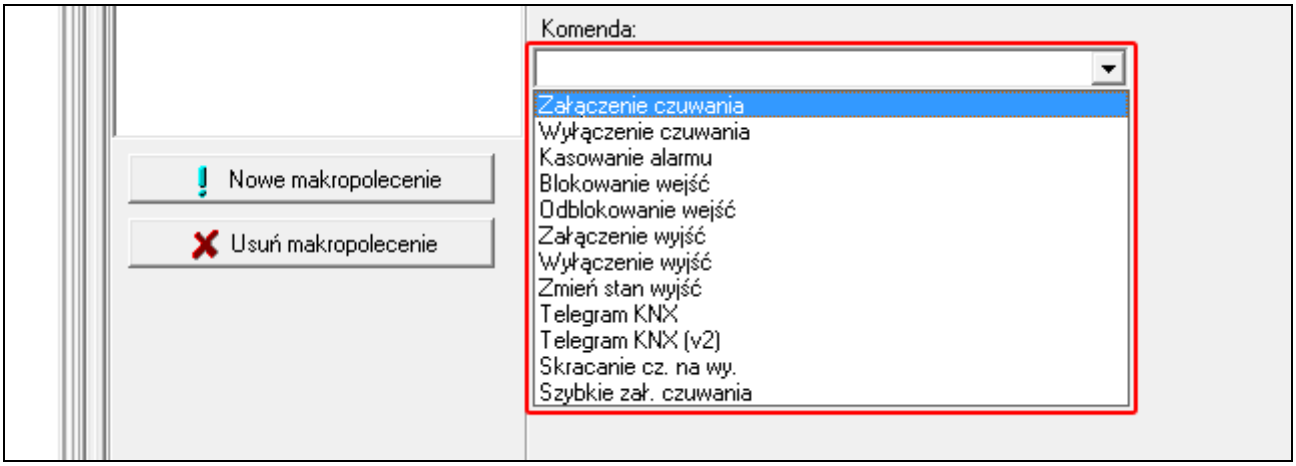


11. Jeżeli ma być wyświetlana nazwa makropolecenia, włącz opcję POKAŻ NAZWĘ.

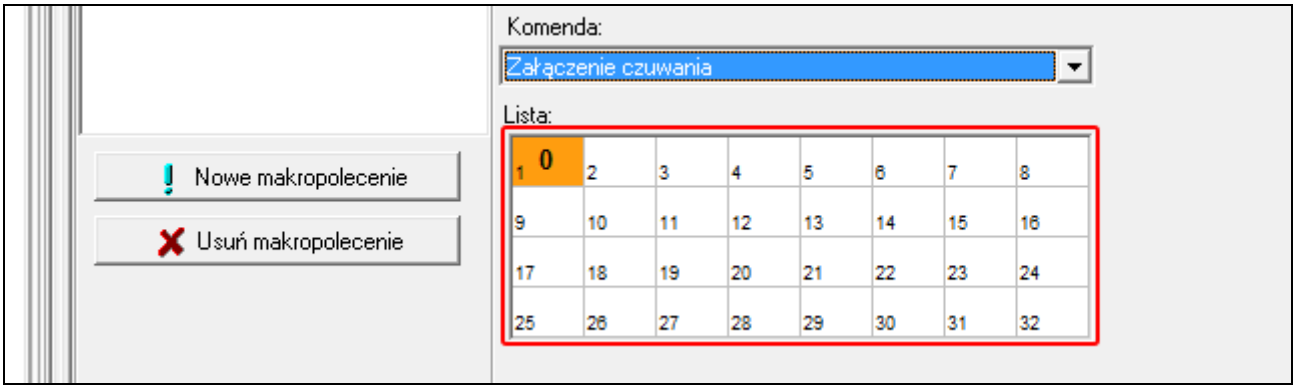


12. Kliknij na przycisk ▼ i wybierz funkcję, którą ma uruchamiać nowe makropolecenie.

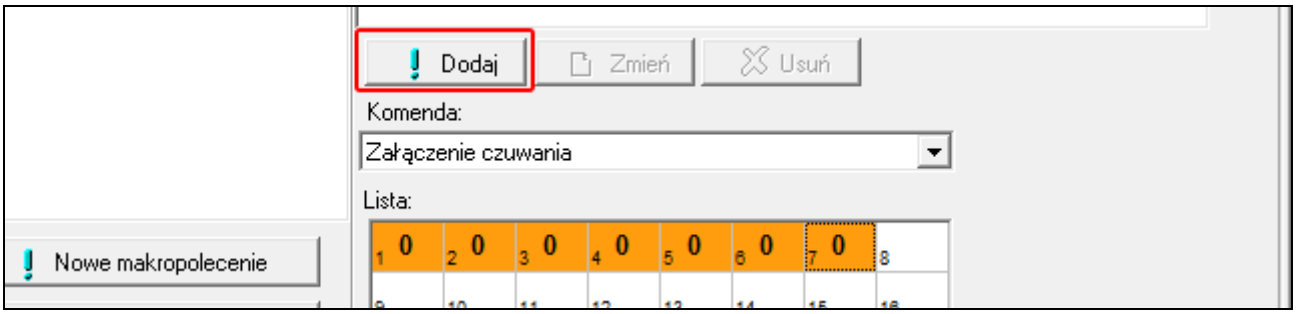


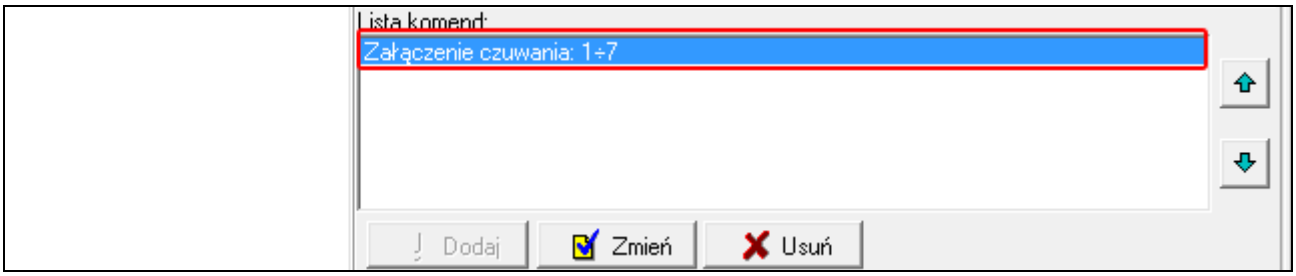


13. Skonfiguruj parametry komendy.

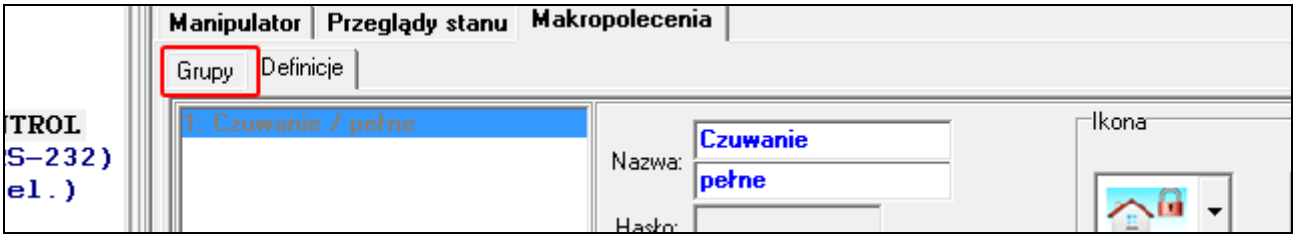


14. Kliknij na przycisk „Dodaj”. Na liście komend przypisanych do makropolecenia pojawi się nowa. Po kliknięciu na komendę możesz jeszcze zmodyfikować jej parametry (po dokonaniu zmian kliknij na przycisk „Zmień”).

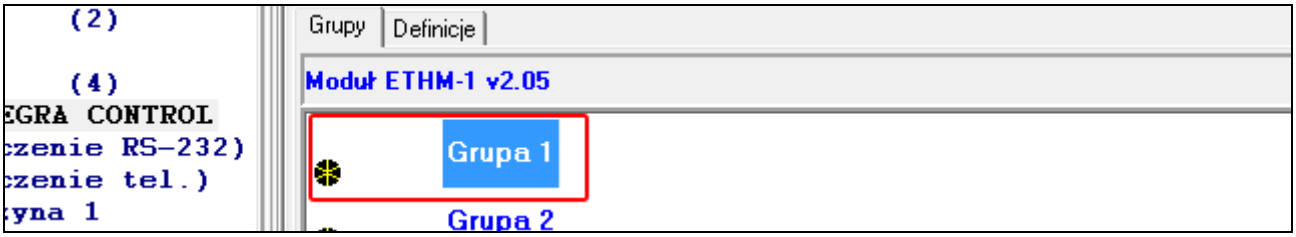




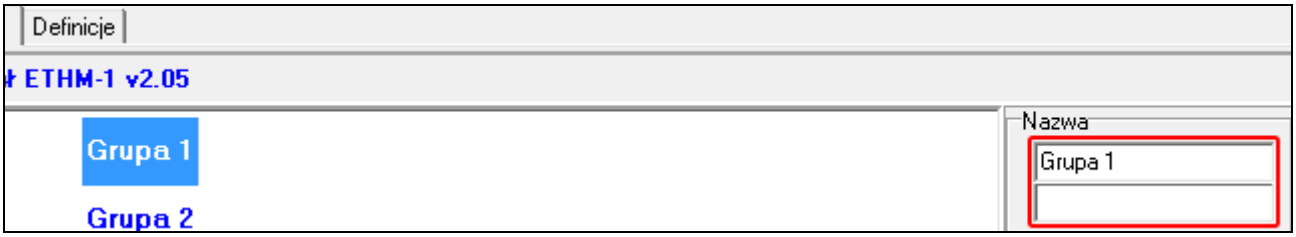
15. Powtórz czynności z punktów 12-14, jeśli chcesz dodać kolejne komendy.
16. Kliknij na zakładkę „Grupy”.



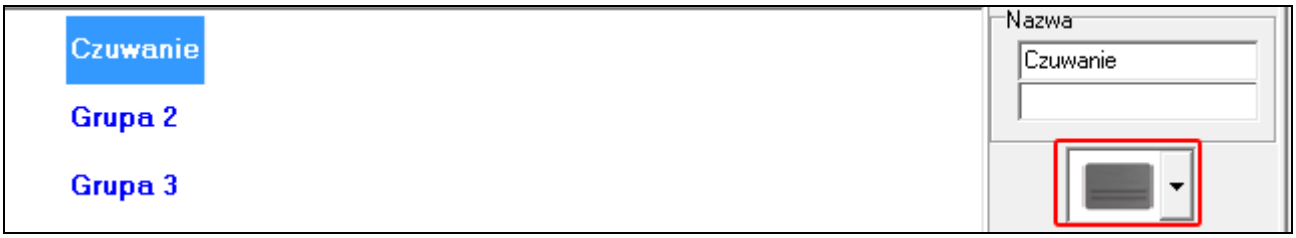
17. Kliknij na grupę, którą chcesz edytować.



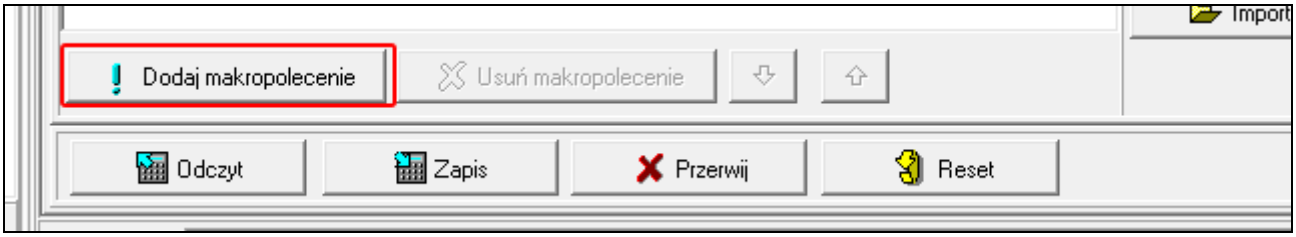
18. Wpisz nazwę grupy, jeżeli ma być wyświetlana.



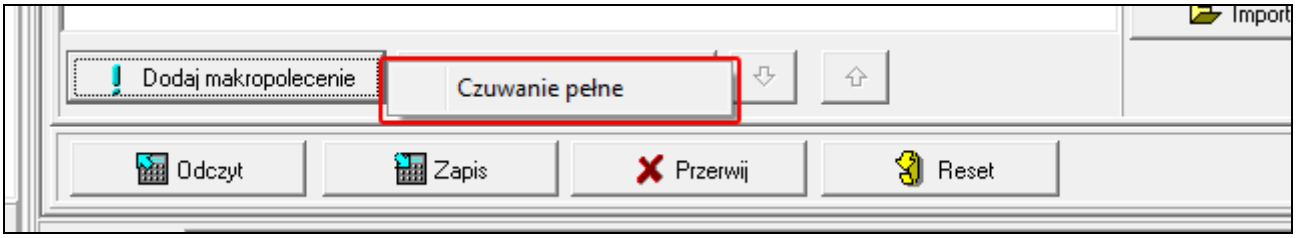
19. Kliknij na przycisk  i wybierz ikonę dla grupy makropoleceń.

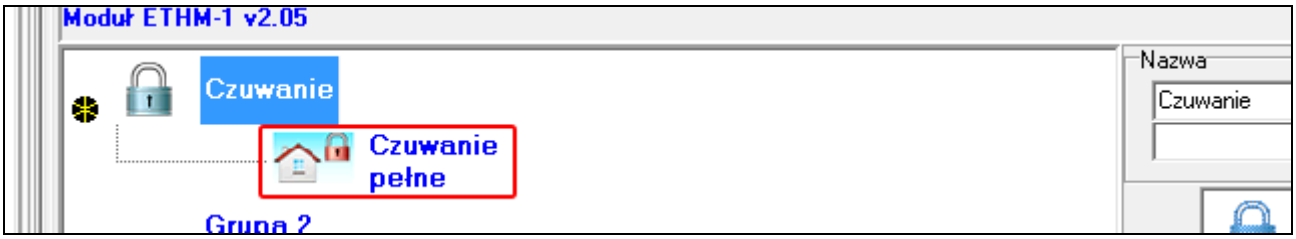


20. Kliknij na przycisk „Dodaj makropolecenie”. Wyświetlona zostanie lista wszystkich zdefiniowanych makropoleceń.

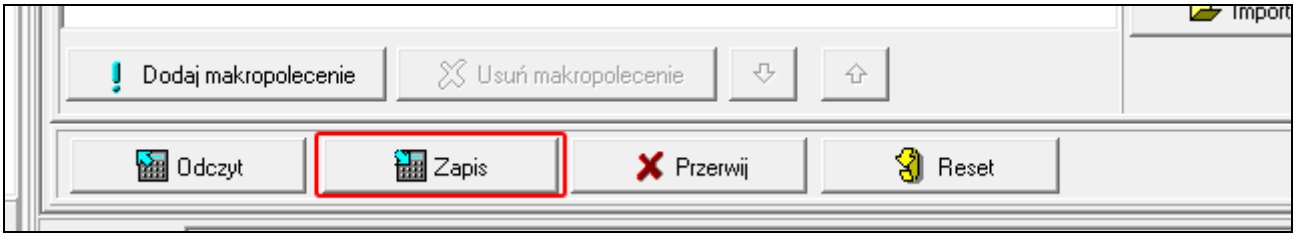


21. Kliknij na makropolecenie, żeby dodać je do grupy. Makropolecenie zostanie umieszczone na drzewie pod grupą.





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



6.2 Moduł podłączony do centrali VERSA

Ustawienia modułu możesz skonfigurować przy pomocy:

- manipulatora: ▶TRYB SERWISOWY ▶2. SPRZĘT ▶1. MANIP. I EKSP. ▶2. USTAWIENIA ▶*[nazwa modułu]*,
- programu DLOADX: →okno „VERSA – Struktura" →zakładka „Sprzęt" →gałąź „Ekspandery" →*[nazwa modułu]* (rys. 12).

Nazwa – indywidualna nazwa urządzenia (do 16 znaków).

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

Łączność DLOADX - ETHM-1 [DLOADX→ETHM-1] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między programem DLOADX a centralą alarmową za pośrednictwem modułu.

DLOADX

DLOADX serwer [DLOADX] – adres komputera z programem DLOADX. Jeżeli komunikacja odbywa się w sieci rozległej, musi to być adres publiczny. Można wpisać adres IP lub nazwę domeny.

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

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

Usługa SATEL

LAN [Serwer SATEL LAN] – jeżeli opcja jest włączona, moduł łączy się z serwerem SATEL i za pośrednictwem serwera SATEL można nawiązać komunikację z centralą (Usługa Zestawiania Połączeń). Ten sposób komunikacji nie wymaga dodatkowego konfigurowania urządzenia sieciowego, za pośrednictwem którego moduł łączy się z siecią publiczną.

i *Nawiązanie komunikacji z serwerem SATEL wymaga użycia serwera DNS.*

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

Nie zgłaszaj braku łączności z serwerem SATEL [Bez aw.SATEL] – jeżeli opcja jest włączona, brak łączności z serwerem SATEL nie wywoła awarii.

Łączność z aplikacją mobilną [Aplik. mobilna] – jeżeli opcja jest włączona, możliwe jest nawiązanie połączenia między aplikacją VERSA CONTROL a centralą alarmową za pośrednictwem modułu. Opcja dostępna, gdy włączona jest opcja LAN.

Alarm 3 błędne hasła (z aplikacji mobilnej) [Alarm 3 bł.hasła] – jeżeli opcja jest włączona, trzykrotne wprowadzenie błędnego hasła przy użyciu aplikacji VERSA CONTROL wywoła alarm.

Powiadomienia PUSH – jeżeli opcja jest włączona, aplikacja VERSA CONTROL może informować o zdarzeniach w systemie alarmowym przy pomocy powiadomień push.

Informacje

MAC – adres sprzętowy modułu.

ID – indywidualny numer identyfikacyjny przydzielony modułowi przez serwer SATEL.

Jeżeli moduł ma zostać użyty w innym systemie alarmowym, skasuj dotychczasowy numer ID. Należy to zrobić po podłączeniu do nowej centrali i nawiązaniu połączenia z serwerem SATEL, przy pomocy manipulatora, podczas programowania modułu ethernetowego, w ostatnim kroku. Po skasowaniu dotychczasowego numeru ID, moduł otrzyma nowy. Aplikacje VERSA CONTROL używające starego numeru ID nie będą mogły połączyć się z centralą.

IP – adres lokalny / adres publiczny modułu.

QR-code – 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 i przekazać użytkownikom. Kod QR upraszcza konfigurowanie ustawień aplikacji VERSA CONTROL.

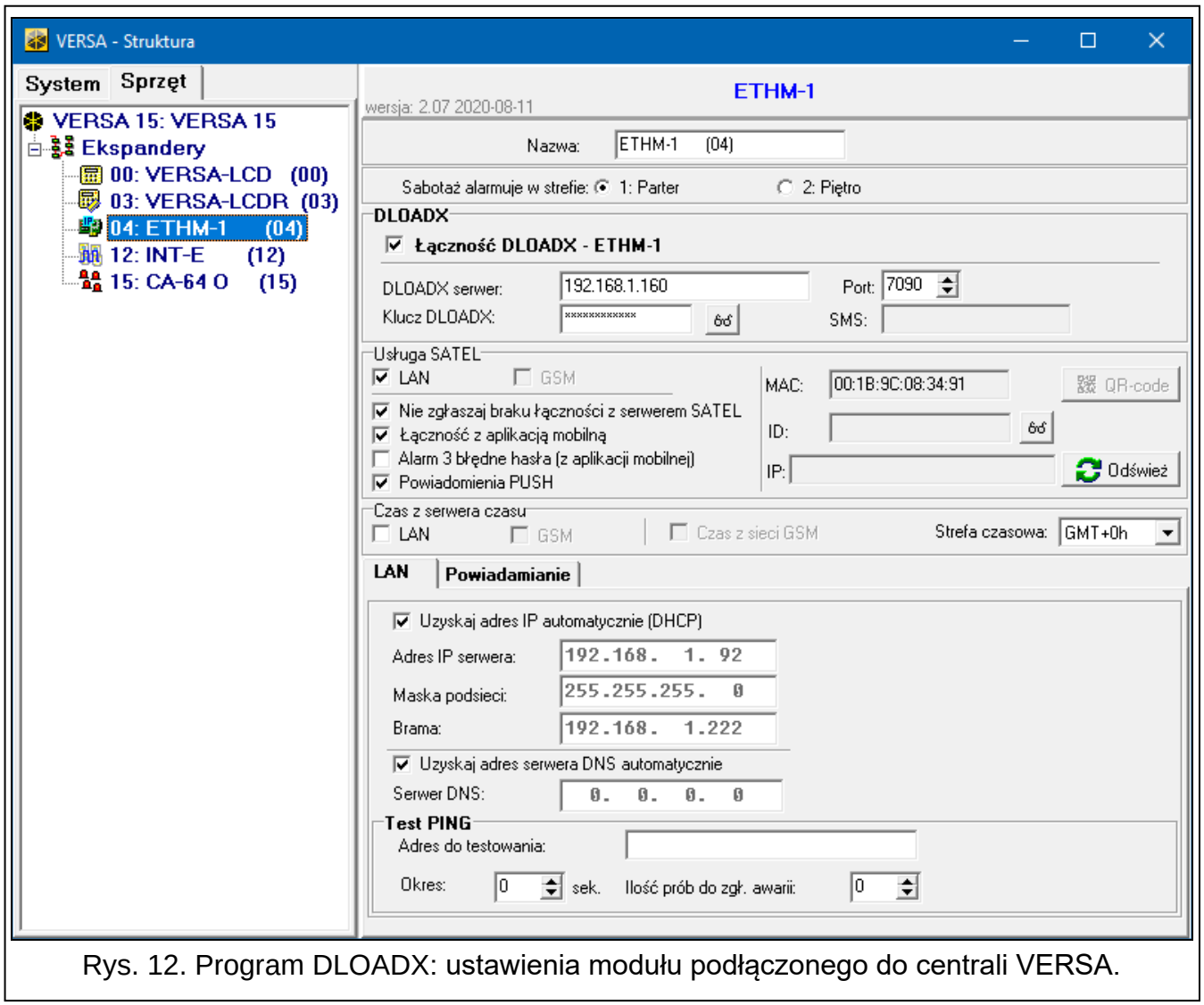
Odśwież – kliknij, aby odświeżyć wszystkie informacje.

Czas z serwera czasu

LAN [Czas z serw. LAN] – jeżeli opcja jest włączona, zegar centrali raz na dobę jest synchronizowany z serwerem czasu.

Komunikacja z serwerem czasu wymaga korzystania z serwera DNS.

Strefa czasowa – różnica między czasem uniwersalnym (GMT) a czasem w strefie. Parametr wymagany, jeżeli zegar centrali ma być synchronizowany z serwerem czasu.



Rys. 12. Program DLOADX: ustawienia modułu podłączonego do centrali VERSA.

6.2.1 LAN

Uzyskaj adres IP automatycznie (DHCP) [DHCP] – jeżeli opcja jest włączona, moduł automatycznie pobiera z serwera DHCP dane dotyczące adresu IP, maski podsieci i bramy (parametrów tych wówczas się nie programuje).

*Adres IP przydzielony modułowi możesz odczytać w manipulatorze LCD przy pomocy funkcji użytkownika **WER. MODUŁÓW** dostępnej w podmenu TESTY. Szczegółowy opis korzystania z funkcji znajduje się w instrukcji użytkownika centrali alarmowej.*

Adres IP serwera – adres IP modułu.

Maska podsieci – maska podsieci, w której pracuje moduł.

Brama – adres IP urządzenia sieciowego, za pośrednictwem którego pozostałe urządzenia z danej sieci lokalnej komunikują się z urządzeniami w innych sieciach.

Uzyskaj adres serwera DNS automatycznie [DHCP-DNS] – jeżeli opcja jest włączona, adres IP serwera DNS jest pobierany automatycznie z serwera DHCP. Opcja dostępna, jeśli opcja UZYSKAJ ADRES IP AUTOMATYCZNIE (DHCP) jest włączona.

Serwer DNS – adres IP serwera DNS, którego ma używać moduł. Można go zaprogramować, gdy opcja UZYSKAJ ADRES SERWERA DNS AUTOMATYCZNIE jest wyłączona.

Test PING

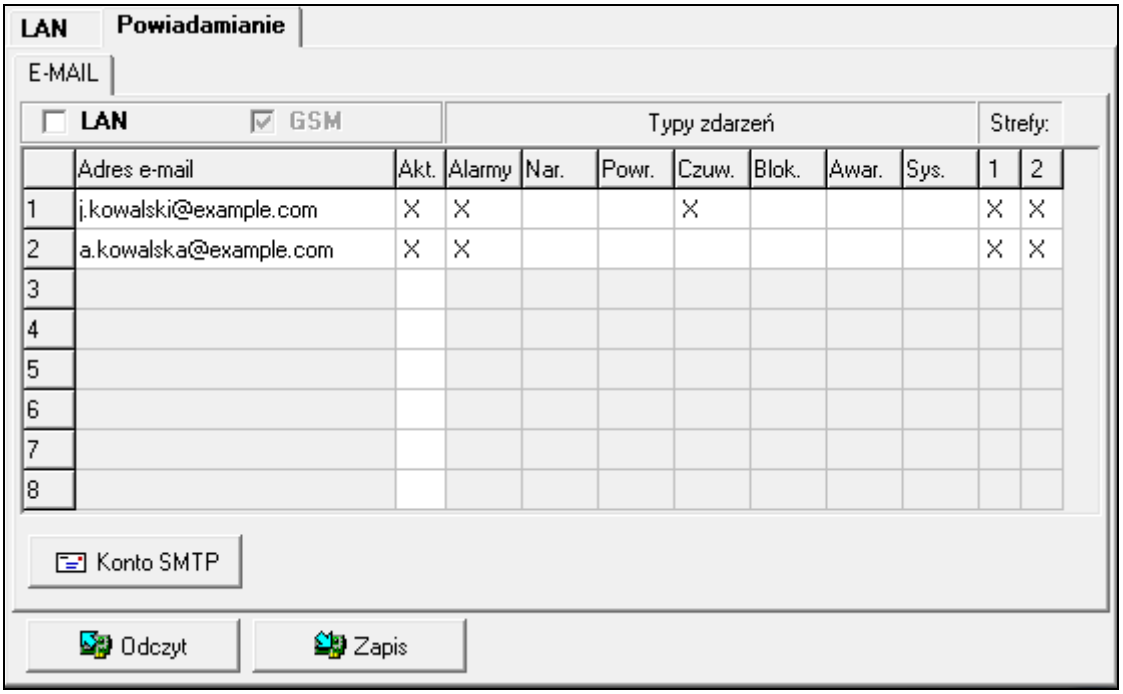
Adres do testowania [PING] – adres urządzenia, do którego moduł ma wysyłać komendę ping w celu testowania komunikacji. Można wpisać adres IP lub nazwę domeny.

Okres [Okres test.PING] – odstęp czasu między kolejnymi testami komunikacji przy pomocy komendy ping. Zaprogramowanie wartości 0 oznacza wyłączenie testu komunikacji.

Ilość prób do zgł. awarii [Ilość prób PING] – liczba nieudanych testów komunikacji (moduł nie uzyskał odpowiedzi na wysłaną komendę ping), po której zgłoszona zostanie awaria. Zaprogramowanie wartości 0 oznacza wyłączenie testu komunikacji.

6.2.2 Powiadamianie

E-MAIL



Rys. 13. Program DLOADX: konfigurowanie powiadamiania e-mail.

Przed wprowadzeniem jakichkolwiek zmian kliknij na przycisk „Odczyt”, a po wprowadzeniu zmian – na przycisk „Zapis” (dane dotyczące powiadamiania e-mail nie są odczytywane po kliknięciu w menu głównym programu DLOADX na przycisk , ani zapisywane po kliknięciu na przycisk).

LAN – jeżeli opcja jest włączona, centrala może powiadamiać o wystąpieniu określonych zdarzeń przy pomocy wiadomości e-mail.

Adres e-mail – adres poczty elektronicznej, na który wysyłane mają być wiadomości w celu powiadomienia o zdarzeniach.

Wiadomość wysyłana jest do wielu odbiorców, dlatego adresaci są ukrywani. Jeżeli adresat ma być widoczny, przed adresem poczty umieść @ (np. @j.kowalski@example.com).

Akt. – po włączeniu opcji możliwe będzie wysyłanie wiadomości na dany adres e-mail w celu powiadomienia o zdarzeniach.

Typy zdarzeń – określ, o jakich zdarzeniach ma być powiadamiany dany adres e-mail.

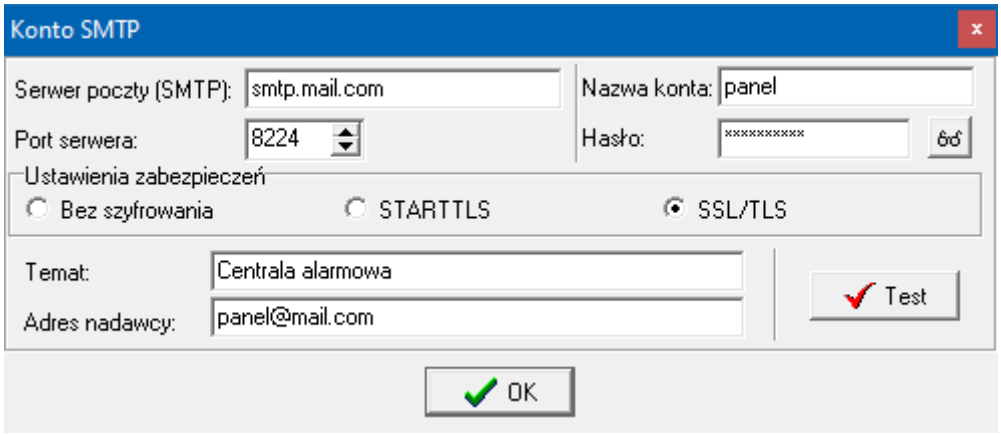
Strefy – określ, o zdarzeniach w jakich strefach ma być powiadamiany dany adres e-mail.

Konto SMTP – kliknij, aby otworzyć okno „Konto SMTP”.

Odczyt – kliknij, aby odczytać dane dotyczące powiadamiania e-mail.

Zapis – kliknij, aby zapisać dane dotyczące powiadamiania e-mail.

Konto SMTP



Rys. 14. Program DLOADX: okno „Konto SMTP”. Prezentowane ustawienia są przykładowe.

Wymagane jest posiadanie konta pocztowego, żeby jego parametry wprowadzić w programie DLOADX na potrzeby powiadamiania e-mail.

Serwer poczty (SMTP) – adres serwera poczty wychodzącej.

Port serwera – numer portu poczty wychodzącej.

Nazwa konta – nazwa konta pocztowego używana przy autoryzacji przez serwer SMTP (login do konta pocztowego).

Hasło – hasło używane przy autoryzacji przez serwer SMTP.

Ustawienia zabezpieczeń – można określić, czy i jak poczta wychodząca jest szyfrowana:

Bez szyfrowania – poczta wychodząca nie jest szyfrowana.

STARTTLS – poczta wychodząca będzie szyfrowana przy pomocy protokołu STARTTLS.

SSL/TLS – poczta wychodząca będzie szyfrowana przy pomocy protokołu SSL/TLS.

Temat – temat wiadomości e-mail. Umieszczany będzie w każdej wysyłanej wiadomości e-mail.

Adres nadawcy – adres poczty elektronicznej, który w wysyłanej wiadomości e-mail będzie umieszczany jako adres nadawcy. Jeżeli pole będzie puste, jako adres nadawcy traktowana będzie nazwa konta pocztowego.

7 Zdalne programowanie i obsługa centrali za pośrednictwem modułu

Moduł umożliwia komunikację z centralą przez sieć Ethernet. Jeżeli do modułu ETHM-1 Plus podłączony jest moduł INT-GSM / INT-GSM LTE, zapasowym torem łączności jest sieć komórkowa danych (moduł zidentyfikowany jako „ETHM+GSM").

Po trzech kolejnych próbach nawiązania komunikacji z modułem przy użyciu błędnego klucza, moduł przez ok. 20 minut nie będzie reagował na próby nawiązania komunikacji z danego adresu IP.

Program GUARDX, przeglądarka internetowa, aplikacja INTEGRA CONTROL i system INTEGRUM nie mogą łączyć się z centralą INTEGRA / INTEGRA Plus w tym samym czasie (np. jeżeli trwa komunikacja z serwerem INTEGRUM, nie można połączyć się z centralą przy pomocy programu GUARDX, przeglądarki internetowej i aplikacji INTEGRA CONTROL).

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

7.1 Program GUARDX

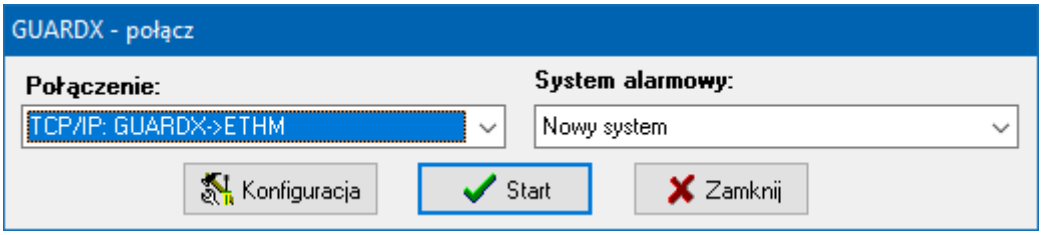
Połączenie między programem GUARDX a centralą alarmową za pośrednictwem modułu ETHM-1 Plus można nawiązać w jeden z poniższych sposobów:

1. Zainicjowanie połączenia z programu GUARDX. Jeżeli komunikacja odbywa się w sieci rozległej, moduł ethernetowy musi mieć publiczny adres IP.
2. Zainicjowanie połączenia z manipulatora (przez centralę alarmową). System alarmowy może być zarządzany zdalnie tylko za wiedzą użytkownika centrali, z adresu zaprogramowanego w centrali. Jeżeli komunikacja odbywa się w sieci rozległej, komputer z programem GUARDX musi mieć publiczny adres IP.
3. Zainicjowanie połączenia przy pomocy wiadomości SMS. Komputer z programem GUARDX musi mieć publiczny adres IP. Do modułu ETHM-1 Plus musi być podłączony moduł INT-GSM / INT-GSM LTE.
4. Nawiązanie połączenia za pośrednictwem serwera SATEL (Usługa Zestawiania Połączeń). Centralę alarmową można obsługiwać z dowolnej lokalizacji. Nie jest wymagany publiczny adres IP ani dla modułu, ani dla komputera z programem GUARDX.

Wymagane ustawienia modułu dla wszystkich sposobów nawiązania łączności:

- włączona opcja GUARDX,
- zaprogramowany klucz szyfrowania danych (KLUCZ GUARDX).

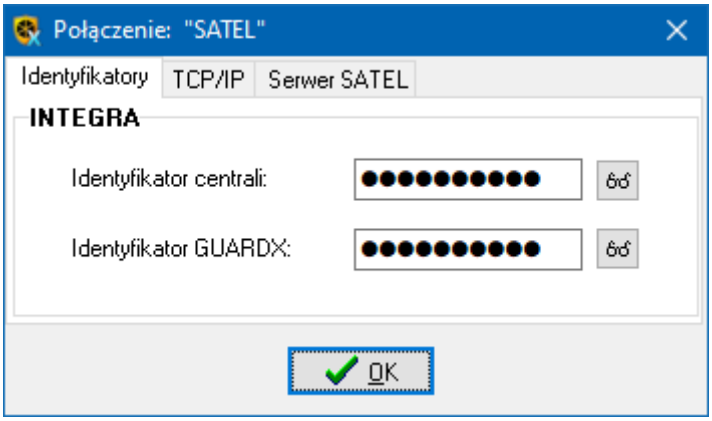
7.1.1 Konfigurowanie ustawień programu GUARDX



Rys. 15. Program GUARDX: okno startowe.

1. W oknie startowym programu GUARDX w polu „Połączenie” wybierz sposób komunikacji: „TCP/IP: GUARDX->ETHM” „TCP/IP: GUARDX<-ETHM/INT-GSM” lub „TCP/IP: serwer SATEL” (rys. 15).
2. Kliknij na przycisk „Konfiguracja”. Wyświetlone zostanie okno „Nazwa systemu”.
3. Wprowadź nazwę systemu i kliknij na przycisk „OK”. Wyświetlone zostanie okno „Połączenie”.

Zakładka „Identyfikatory”



Rys. 16. 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).

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

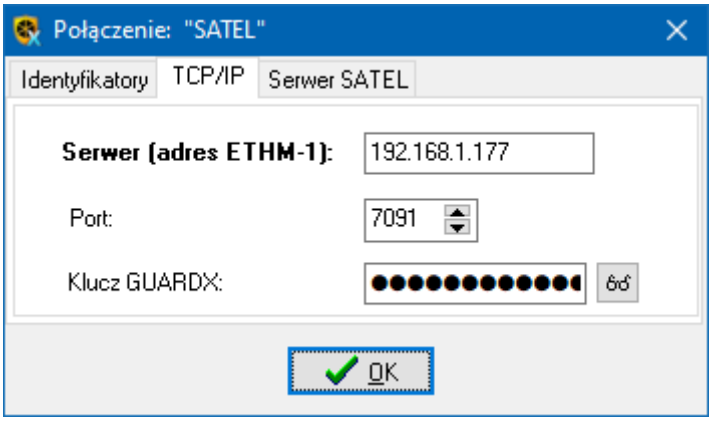
Zakładka „TCP/IP”

Poniższe ustawienia dotyczą komunikacji bezpośrednio z modułem.

Serwer (adres ETHM-1) – adres modułu ethernetowego. Jeżeli moduł ethernetowy nie znajduje się w tej samej sieci lokalnej, co komputer z programem GUARDX, musi to być adres publiczny. Możesz wpisać adres IP lub nazwę domeny.

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

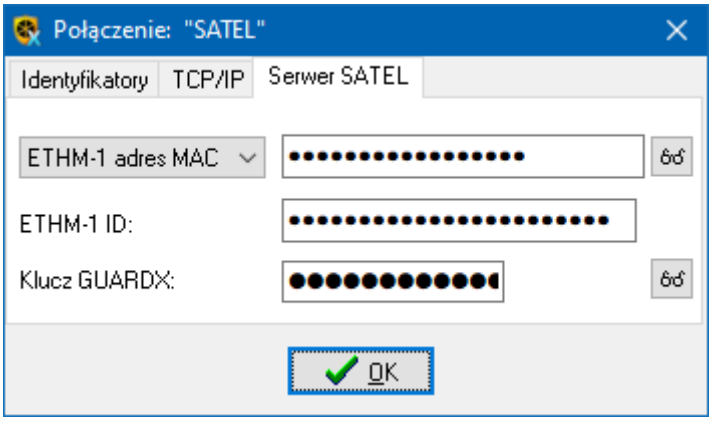
Klucz GUARDX – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do szyfrowania danych podczas komunikacji między centralą a komputerem z programem GUARDX.



Rys. 17. Program GUARDX: zakładka „TCP/IP” w oknie „Połączenie”.

Zakładka „Serwer SATEL”

Poniższe ustawienia dotyczą komunikacji za pośrednictwem serwera SATEL.



Rys. 18. Program GUARDX: zakładka „Serwer SATEL” w oknie „Połączenie”.

Wybierz wariant „ETHM-1 adres MAC”.

ETHM-1 adres MAC – adres sprzętowy modułu ethernetowego.

ETHM-1 ID – indywidualny numer identyfikacyjny przydzielony modułowi przez serwer SATEL.

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

7.1.2 Zainicjowanie połączenia z programu GUARDX

Wymagane ustawienia modułu:

- zaprogramowany numer portu TCP używanego do komunikacji.

Wymagane ustawienia programu GUARDX dla komunikacji bezpośrednio z modułem:

- zaprogramowane: adres modułu ETHM-1 Plus (SERWER (ADRES ETHM-1)), numer portu TCP używanego do komunikacji i klucz szyfrowania danych (KLUCZ GUARDX).

1. W oknie startowym (rys. 15), w polu „Połączenie”, wybierz „TCP/IP: GUARDX->ETHM”, a następnie kliknij na przycisk „Start”.
2. W oknie, które wyświetli się po nawiązaniu komunikacji, wprowadź hasło administratora / użytkownika centrali.

7.1.3 Zainicjowanie połączenia z manipulatora (przez centralę alarmową)

Wymagane ustawienia modułu:

- zaprogramowane: adres komputera z programem GUARDX (GUARDX SERWER) i numer portu TCP używanego do komunikacji.

Wymagane ustawienia programu GUARDX dla komunikacji bezpośrednio z modułem:

- zaprogramowane: numer portu TCP używanego do komunikacji i klucz szyfrowania danych (KLUCZ GUARDX).

1. W oknie startowym (rys. 15), w polu „Połączenie” wybierz „TCP/IP: GUARDX<-ETHM/INT-GSM”, a następnie kliknij na przycisk „Start”.
2. Poproś użytkownika o uruchomienie funkcji ETHM-1 →GUARDX ([*hasło*]✱ ▶DOWNLOADING ▶ETHM-1 →GUARDX). Funkcja jest dostępna dla serwisu, administratora oraz użytkownika posiadającego uprawnienie URUCHAMIANIE FUNKCJI DOWNLOAD.
3. W oknie, które wyświetli się po nawiązaniu komunikacji, wprowadź hasło administratora / użytkownika centrali.

7.1.4 Zainicjowanie połączenia przy pomocy wiadomości SMS

Wymagane ustawienia modułu:

- zaprogramowane: adres komputera z programem GUARDX (GUARDX SERWER) i numer portu TCP używanego do komunikacji,
- zaprogramowane polecenie sterujące, którego przesłanie w wiadomości SMS zainicjuje nawiązanie łączności z programem GUARDX (SMS INICJUJĄCY POŁĄCZENIE Z GUARDX).

Wymagane ustawienia programu GUARDX dla komunikacji bezpośrednio z modułem:

- zaprogramowane: numer portu TCP używanego do komunikacji i klucz szyfrowania danych (KLUCZ GUARDX).

1. W oknie startowym (rys. 15), w polu „Połączenie” wybierz „TCP/IP: GUARDX<-ETHM/INT-GSM”, a następnie kliknij na przycisk „Start”.
2. Wyślij do modułu INT-GSM / INT-GSM LTE 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 (adres IP lub nazwa domeny); „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.

7.1.5 Nawiązanie połączenia za pośrednictwem serwera SATEL

Wymagane ustawienia modułu:

- włączona opcja ŁĄCZNOŚĆ PRZEZ SERWER SATEL.

Wymagane ustawienia programu GUARDX dla komunikacji za pośrednictwem serwera SATEL:

- zaprogramowane: numer identyfikacyjny przydzielony modułowi przez serwer SATEL (ETHM-1 ID), adres MAC modułu (ETHM-1 ADRES MAC) i klucz szyfrowania danych (KLUCZ GUARDX).

1. W oknie startowym (rys. 15), 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.

7.2 Przeglądarka WWW

Wymagane ustawienia modułu:

- włączona opcja WWW,
- zaprogramowany klucz szyfrowania danych (KLUCZ GUARDX),
- zaprogramowany numer portu TCP używanego do komunikacji z przeglądarką internetową (PORT WWW),
- zaprogramowany numer portu TCP używanego do komunikacji z aplikacją JAVA w przeglądarce internetowej (PORT).

W komputerze musi być zainstalowana Wirtualna Maszyna Javy (Java Virtual Machine). Można ją pobrać ze strony www.java.com

Zaleca się instalację Wirtualnej Maszyny Javy w wersji 32-bitowej.

1. Uruchom przeglądarkę WWW.
2. W polu adresu wpisz adres IP modułu ETHM-1 Plus, a następnie naciśnij klawisz ENTER.

Jeżeli do komunikacji między modułem a przeglądarką internetową ma być użyty inny port niż 80, po wprowadzeniu adresu wpisz dwukropek i numer portu.

3. Kiedy wyświetli się strona logowania (rys. 19), w odpowiednich polach wpisz:
   - klucz szyfrowania danych (KLUCZ GUARDX),
   - numer portu TCP (identyczny z zaprogramowanym w module dla komunikacji z aplikacją JAVA w przeglądarce internetowej – wyjątkiem jest sytuacja, kiedy komunikacja odbywa się za pośrednictwem urządzenia sieciowego, na którym następuje przekierowanie na inny port).



Rys. 19. Przeglądarka WWW: strona logowania.

4. Kliknij na „LOGIN”.
5. W przeglądarce wyświetlony zostanie wirtualny manipulator (rys. 20).



Rys. 20. Przeglądarka WWW: wirtualny manipulator.

7.3 Aplikacja mobilna INTEGRA CONTROL

System alarmowy INTEGRA / INTEGRA Plus można obsługiwać i konfigurować z urządzenia mobilnego po zainstalowaniu aplikacji INTEGRA CONTROL. Jeżeli w chronionym obiekcie są zainstalowane kamery IP, przy pomocy aplikacji możesz podglądać obraz z tych kamer.

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 może połączyć się bezpośrednio z modułem ETHM-1 Plus (moduł musi mieć publiczny adres IP) lub nawiązać połączenie za pośrednictwem serwera SATEL (Usługa Zestawiania Połączeń – moduł nie potrzebuje publicznego adresu IP).

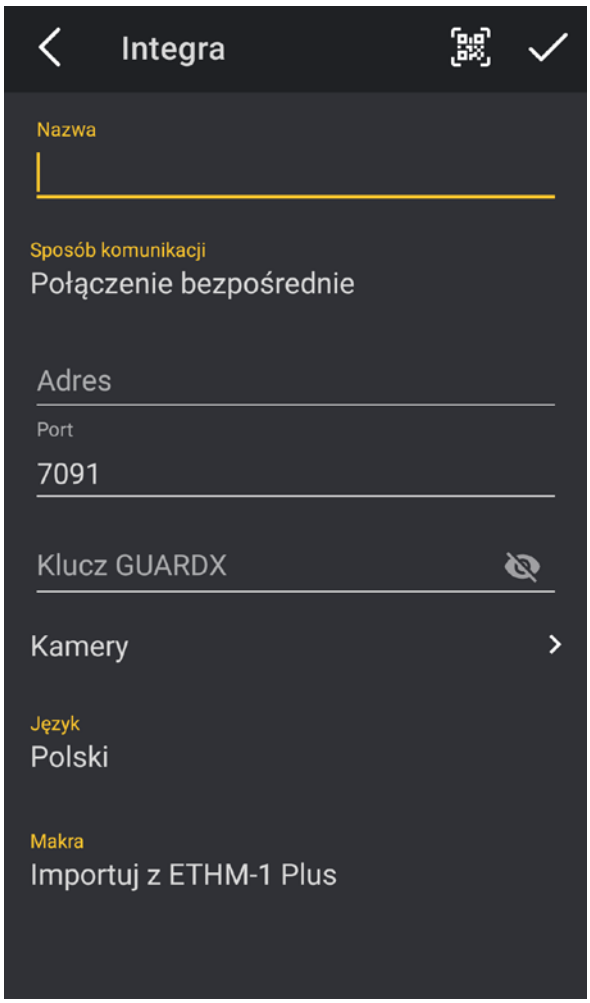
Wymagane ustawienia modułu dla obu sposobów nawiązania połączenia:

- włączona opcja INTEGRA CONTROL,
- zaprogramowany klucz szyfrowania danych (KLUCZ GUARDX),
- włączona opcja ŁĄCZNOŚĆ PRZEZ SERWER SATEL, jeżeli połączenie ma być nawiązywane za pośrednictwem serwera SATEL,
- numer portu TCP używanego do komunikacji, jeżeli połączenie ma być nawiązywane bezpośrednio z modułem.

Do skonfigurowania w aplikacji INTEGRA CONTROL ustawień komunikacji przez serwer SATEL można użyć kodu QR (patrz: s. 11). Jeżeli ustawienia 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.

7.3.1 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (Android)

Po pierwszym uruchomieniu aplikacji wyświetlony zostanie ekran dodawania centrali alarmowej. Pozwala on skonfigurować ustawienia wymagane do nawiązania połączenia z centralą.



Rys. 21. Aplikacja INTEGRA CONTROL (system Android): ekran dodawania centrali alarmowej.

1. Skonfiguruj ustawienia komunikacji. Ustawienia możesz wprowadzić ręcznie (patrz: „Ręczne wprowadzenie ustawień komunikacji”) lub możesz je wczytać za pomocą kodu QR (patrz: „Wczytanie ustawień komunikacji przy użyciu kodu QR”).
2. Wprowadź nazwę dla systemu alarmowego. Nazwa ułatwia identyfikację systemu alarmowego podczas korzystania z aplikacji (możesz zdefiniować ustawienia dla wielu systemów alarmowych).
3. Jeżeli przy pomocy aplikacji chcesz podglądać obraz z kamer IP, wprowadź adresy kamer. Jeżeli nie chcesz używać aplikacji do podglądu obrazu z kamer IP, pomiń ten krok. Możesz dodać nowe kamery IP i zmienić ustawienia już dodanych kamer w dowolnym momencie korzystania z aplikacji.
4. Określ język centrali alarmowej.
5. 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. W przypadku, gdy wybierzesz import z pliku, będziesz musiał wskazać lokalizację pliku z makropoleceniami.
6. Dotknij ✓, żeby zapisać ustawienia.

Ręczne wprowadzenie ustawień komunikacji

Użytkownik systemu alarmowego może użyć manipulatora, aby znaleźć dane wymagane podczas konfigurowania ustawień komunikacji (funkcja użytkownika IP/MAC/IMEI/ID dostępna w podmenu TESTY – patrz instrukcja użytkownika centrali alarmowej).

Komunikacja bezpośrednio z modułem

1. Wybierz sposób komunikacji „Połączenie bezpośrednie”.
2. Wprowadź adres sieciowy modułu.
3. Wprowadź numer portu TCP.
4. Wprowadź klucz szyfrowania danych – identyczny, jak w module (KLUCZ GUARDX).

Komunikacja przez serwer SATEL

1. Wybierz sposób komunikacji „Połączenie przez serwer SATEL przy użyciu adresu MAC”.
2. Wprowadź adres MAC modułu.
3. Wprowadź numer ID modułu (identyfikator przydzielony modułowi przez serwer SATEL).
4. Wprowadź klucz szyfrowania danych – identyczny, jak w module (KLUCZ GUARDX).

Wczytanie ustawień komunikacji przy użyciu kodu QR

Skanowanie kodu QR przy użyciu aparatu

1. Dotknij .
2. Dotknij „Skanuj kod QR”.
3. Zezwól na używanie aparatu przez aplikację.
4. Zeskanuj kod QR.
5. Wprowadź hasło zabezpieczające kod QR i dotknij „OK”.

Wczytanie kodu QR z pliku

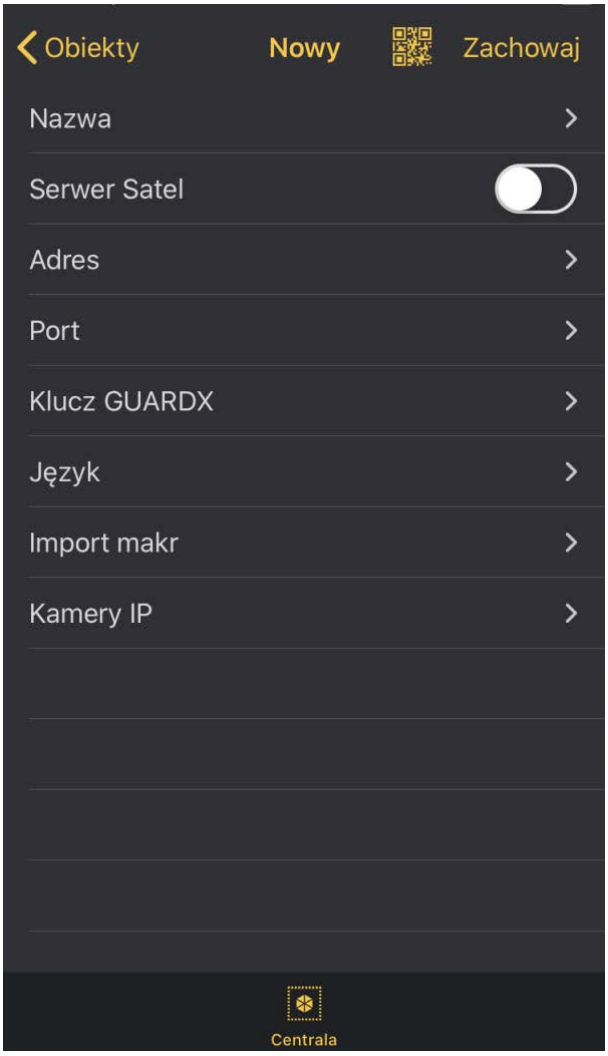
1. Dotknij .
2. Dotknij „Wybierz obraz”.
3. Zezwól aplikacji na dostęp do plików urządzenia mobilnego.
4. Wybierz obraz z kodem QR.
5. Wprowadź hasło zabezpieczające kod QR i dotknij „OK”.

7.3.2 Konfigurowanie ustawień w aplikacji INTEGRA CONTROL (iOS)

Po pierwszym uruchomieniu aplikacji wyświetlony zostanie ekran „Obiekty”.

1. Dotknij „Nowy”. Wyświetlony zostanie ekran dodawania centrali alarmowej.
2. Skonfiguruj ustawienia komunikacji. Ustawienia możesz wprowadzić ręcznie (patrz: „Ręczne wprowadzenie ustawień komunikacji”) lub możesz je wczytać za pomocą kodu QR (patrz: „Wczytanie ustawień komunikacji przy użyciu kodu QR”).
3. Wprowadź nazwę dla systemu alarmowego. Nazwa służy do identyfikacji systemu podczas korzystania z aplikacji (możesz zdefiniować ustawienia dla wielu systemów alarmowych).
4. Określ język centrali alarmowej.
5. 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.

6. Jeżeli przy pomocy aplikacji chcesz podglądać obraz z kamer IP, wprowadź adresy kamer. Jeżeli nie chcesz używać aplikacji do podglądu obrazu z kamer IP, pomiń ten krok. Możesz dodać nowe kamery IP i zmienić ustawienia już dodanych kamer w dowolnym momencie korzystania z aplikacji.
7. Dotknij „Zachowaj”, żeby zapisać ustawienia.



Rys. 22. Aplikacja INTEGRA CONTROL (system iOS): ekran dodawania centrali alarmowej.

Ręczne wprowadzenie ustawień komunikacji

Użytkownik systemu alarmowego może użyć manipulatora, aby znaleźć dane wymagane podczas konfigurowania ustawień komunikacji (funkcja użytkownika IP/MAC/IMEI/ID dostępna w podmenu TESTY – opis funkcji znajdziesz w instrukcji użytkownika centrali alarmowej).

Komunikacja bezpośrednio z modułem

1. Wprowadź adres sieciowy modułu.
2. Wprowadź numer portu TCP.
3. Wprowadź klucz szyfrowania danych – identyczny, jak w module (KLUCZ GUARDX).

Komunikacja przez serwer SATEL

1. Włącz opcję „Serwer Satel”.
2. Wprowadź adres MAC modułu.

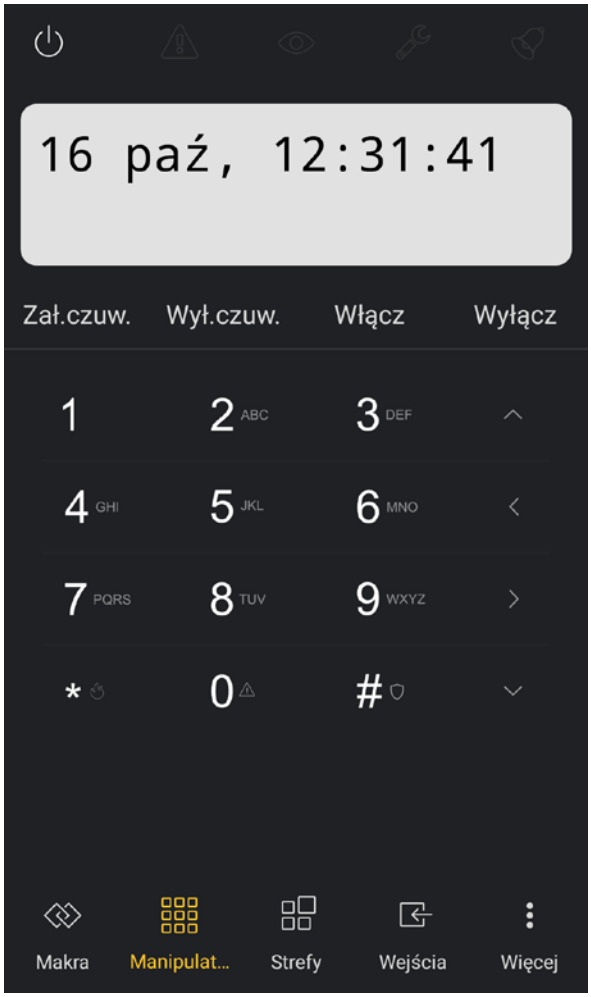
3. Wprowadź numer ID modułu (identyfikator przydzielony modułowi przez serwer SATEL).
4. Wprowadź klucz szyfrowania danych – identyczny, jak w module (KLUCZ GUARDX).

Wczytanie ustawień komunikacji przy użyciu kodu QR

1. Dotknij .
2. Zezwól na używanie aparatu przez aplikację.
3. Zeskanuj kod QR.
4. Wprowadź hasło zabezpieczające kod QR i dotknij „OK”.

7.3.3 Nawiązanie komunikacji

Dotknij nazwę systemu alarmowego. Po nawiązaniu połączenia z centralą, aplikacja poprosi o wpisanie hasła użytkownika. Po wprowadzeniu hasła wyświetlony zostanie ekran „Makra” (w systemie iOS można określić, który ekran będzie wyświetlany jako pierwszy po kolejnym nawiązaniu komunikacji).



Rys. 23. Aplikacja INTEGRA CONTROL (system Android): wirtualny manipulator.

8 Dane techniczne

Napięcie zasilania ..... 12 V DC ±15%
Pobór prądu w stanie gotowości .....70 mA
Maksymalny pobór prądu.....80 mA

Klasa środowiskowa wg EN50130-5	II
Zakres temperatur pracy	-10...+55°C
Maksymalna wilgotność	93±3%
Wymiary	68 x 140 mm
Masa	64 g