



---

# **ACCO SOFT**

## **Program do konfiguracji systemu kontroli dostępu ACCO NET**

**Instrukcja obsługi**

ACCO NET 1.6  
Wersja programu 1.17.10

---

acco soft\_pl 08/19

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](http://www.satel.pl)

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>

W instrukcji mogą wystąpić następujące symbole:



- uwaga;



- uwaga krytyczna.

## Zmiany wprowadzone w wersji oprogramowania 1.17.10

### Kontrolery

#### Funkcjonalność:

- Opcja: Kontroler umożliwia dodawanie identyfikatorów,
- Ustawienia terminali: Opcje dostępu i sterowania.

## SPIS TREŚCI

1.	Wprowadzenie.....	4
2.	Instalacja.....	4
2.1	Wymagania systemowe .....	4
2.2	Instalacja programu ACCO Soft.....	4
3.	Pierwsze uruchomienie programu ACCO Soft .....	4
3.1	Logowanie do programu.....	4
4.	Opis programu ACCO Soft.....	5
4.1	Menu główne programu.....	5
4.1.1	Lista awarii / alarmów .....	6
4.1.2	Licencje .....	7
4.1.2.1	Okno „Licencje integracji” .....	7
4.1.2.2	Uzyskanie licencji .....	10
4.1.2.3	Wczytywanie licencji .....	11
4.2	Struktura systemu .....	12
4.2.1	Lista obiektów i central .....	12
4.2.1.1	Restart centrali.....	13
4.2.2	Obiekty .....	13
4.2.2.1	Dodanie obiektu .....	13
4.2.2.2	Programowanie obiektów.....	13
4.2.2.3	Usunięcie obiektu .....	15
4.2.3	Centrale.....	15
4.2.3.1	Dodanie centrali ACCO-NT podłączonej do sieci Ethernet.....	15
4.2.3.2	Dodanie centrali ACCO-NT przed podłączeniem jej do sieci Ethernet .....	15
4.2.3.3	Programowanie centrali .....	16
4.2.3.4	Zdalna aktualizacja oprogramowania centrali .....	17
4.2.3.5	Usunięcie centrali .....	18
4.2.4	Kontrolery.....	18
4.2.4.1	Identyfikacja kontrolerów podłączonych do systemu .....	19
4.2.4.2	Dodanie kontrolera przed podłączeniem go do systemu .....	19
4.2.4.3	Okno „Podsumowanie” .....	19
4.2.4.4	Tabela z listą kontrolerów .....	20
4.2.4.5	Programowanie kontrolera.....	22
4.2.4.6	Zdalna aktualizacja oprogramowania kontrolera.....	38
4.2.4.7	Usunięcie kontrolera .....	39
4.2.5	Strefy.....	40
4.2.5.1	Utworzenie strefy .....	40
4.2.5.2	Tabela z listą stref.....	40
4.2.5.3	Programowanie stref.....	41
4.2.5.4	Usunięcie strefy .....	44
4.2.6	Integracja.....	44
4.2.6.1	Konfigurowanie systemu alarmowego .....	45
4.2.6.2	Dodanie systemu alarmowego.....	46
4.2.6.3	Tabela z listą systemów alarmowych.....	46
4.2.6.4	Konfigurowanie ustawień dotyczących integracji .....	47
4.2.6.5	Przypisanie stref .....	48
4.2.6.6	Usunięcie systemu alarmowego .....	48
4.2.7	Ekspandery .....	49
4.2.7.1	Dodanie ekspandera.....	49
4.2.7.2	Ustawienia ekspandera.....	49
4.2.7.3	Usunięcie ekspandera .....	49
4.2.8	Wejścia.....	49
4.2.8.1	Numeracja wejść w systemie.....	50

4.2.8.2	Programowanie wejść.....	50
4.2.9	Wyjścia.....	52
4.2.9.1	Numeracja wyjść w systemie.....	52
4.2.9.2	Programowanie wyjść.....	52
4.2.10	Ścieżki przejść.....	55
4.2.10.1	Utworzenie ścieżki przejścia.....	55
4.2.10.2	Programowanie ścieżki przejścia.....	55
4.2.10.3	Usunięcie ścieżki przejścia.....	56
4.2.11	Status.....	56
4.2.11.1	Awarie centrali.....	57
4.2.11.2	Stan zasilania centrali.....	58
4.2.11.3	Zakładka „Wejścia”.....	58
4.2.11.4	Zakładka „Wyjścia”.....	58
4.2.12	Import.....	58
4.2.12.1	Import danych z pliku w formacie CSV.....	58
4.2.12.2	Import danych z pliku z rozszerzeniem kkd.....	59
5.	Załącznik 1 „Opis działania integracji systemów”.....	61
6.	Załącznik 2 „Obsługa zintegrowanych stref”.....	62
6.1	Przykłady.....	63
6.1.1	Przykład 1.....	63
6.2	Sygnalizacja blokowania przejścia / strefy przez urządzenia systemu kontroli dostępu.....	64
6.2.1	Sygnalizacja optyczna.....	64
6.2.1.1	Priorytety stanów systemu ACCO NET.....	64
6.2.1.2	Manipulatory.....	65
6.2.1.3	Klawiatura z czytnikiem kart zbliżeniowych.....	65
6.2.1.4	Czytniki kart zbliżeniowych.....	65
6.2.1.5	Czytnik pastylek DALLAS.....	66
6.2.2	Sygnalizacja dźwiękowa.....	66

## 1. Wprowadzenie

---

Program ACCO Soft służy do programowania i konfiguracji systemu kontroli dostępu ACCO NET. Komunikacja między programem a systemem odbywa się zdalnie za pośrednictwem sieci Ethernet.

Dane zapisywane są do wszystkich obecnych w systemie central, modułów kontroli dostępu oraz ekspanderów.

## 2. Instalacja

---

### 2.1 Wymagania systemowe

---

Program ACCO Soft wymaga do pracy środowiska Java w wersji 7 lub wyższej. Pobierz jego najnowszą wersję ze strony <http://www.java.com/pl/download/> i zainstaluj na komputerze.

### 2.2 Instalacja programu ACCO Soft

---

1. Uruchom przeglądarkę internetową.
2. Wpisz adres: `https://[adres komputera, na którym zainstalowany został ACCO Server]` i zaloguj się do aplikacji ACCO Web jako Administrator (domyślne: login „admin” i hasło „admin”). Jeżeli komunikacja będzie się odbywać za pośrednictwem innego portu niż domyślny, adres systemu wpisz w następujący sposób: `https://[adres serwera:numer portu]`.
3. Kliknij na polecenie „Programy” w menu po lewej stronie ekranu. Wyświetlone zostaną odsyłacze do plików instalacyjnych programów ACCO-NT Conf, ACCO Soft i Map Editor.
4. Kliknij na odsyłacz ACCO Soft i zapisz plik instalacyjny na dysku.
5. Uruchom plik instalacyjny i postępuj zgodnie z wyświetlanymi poleceniami.



*Po każdej aktualizacji systemu ACCO NET, pobierz i zainstaluj najnowszą wersję programu ACCO Soft.*

## 3. Pierwsze uruchomienie programu ACCO Soft

---

### 3.1 Logowanie do programu

---

Dostęp do programu chroniony jest hasłem. Przy pierwszym uruchomieniu programu dostęp uzyskuje się na podstawie danych fabrycznych: loginu „admin” oraz hasła „admin” (nie trzeba ich wpisywać, wystarczy kliknąć na przycisk „Połącz”).

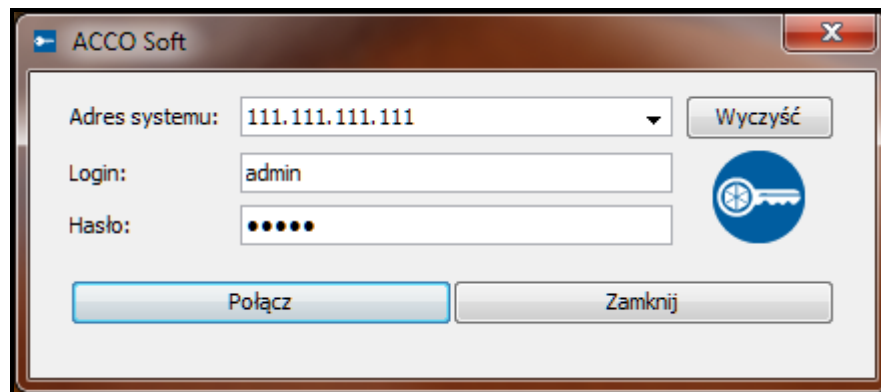
W polu „Adres systemu” wpisz adres sieciowy komputera, na którym został zainstalowany ACCO Server. Adres może zostać wprowadzony w formie adresu IP (4 liczby dziesiętne oddzielone kropkami) lub w postaci nazwy.

W przypadku, gdy port (RMI), na którym będzie się odbywać komunikacja pomiędzy ACCO Server a programem ACCO Soft, jest inny niż domyślny port 2500, po adresie IP i dwukropku należy wpisać port, na którym będzie się odbywać komunikacja.



*Fabryczne hasło dostępu do programu należy zmienić przed rozpoczęciem użytkownika systemu.*


*Dostęp do wszystkich funkcji programu posiada Administrator systemu ACCO NET. Uprawnienia pozostałych użytkowników określa się przy pomocy aplikacji ACCO Web (patrz: instrukcja obsługi ACCO Web).*



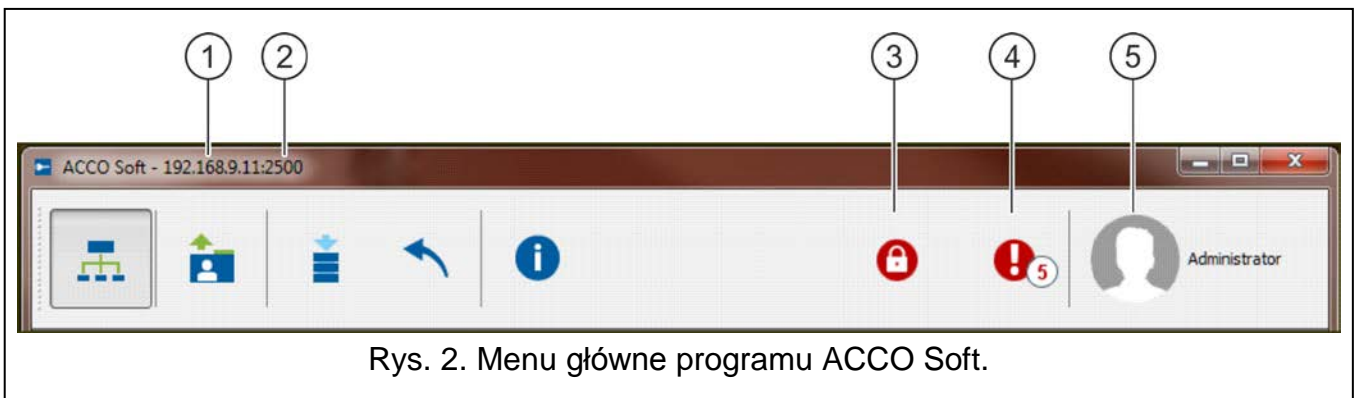
Rys. 1. Okno logowania po uruchomieniu programu ACCO Soft.

## 4. Opis programu ACCO Soft




Jeśli w menu głównym programu będzie się wyświetlać przycisk , oznacza to, że w danym momencie ktoś inny konfiguruje ustawienia systemu ACCO NET.

### 4.1 Menu główne programu



Rys. 2. Menu główne programu ACCO Soft.

Objaśnienia do rysunku 2:

- ① adres sieciowy komputera, na którym jest zainstalowany ACCO Server.
- ② numer portu, na którym odbywa się komunikacja pomiędzy ACCO Server a programem ACCO Soft.
- ③ przycisk informujący o blokadzie bazy danych. Gdy najedziesz na niego wskaźnikiem myszki, wyświetli się informacja o tym, że inny użytkownik rozpoczął edycję i nie zapisał wprowadzonych zmian.  
Informacje o blokadzie wyświetlą się też w komunikacie, który pojawi się:
  - gdy będziesz zalogowany do programu, a inny użytkownik rozpocznie edycję,
  - gdy uruchomisz program, a inny użytkownik będzie edytować dane.
- ④ przycisk informujący o bieżących awariach / alarmach w systemie. Obok wyświetla się ich liczba. Lista awarii / alarmów wyświetli się po kliknięciu wskaźnikiem myszki na przycisk (patrz: rozdział „Lista awarii / alarmów”). W przypadku, gdy program ACCO Soft nie będzie miał połączenia z ACCO Server wyświetlany jest w tym miejscu przycisk  informujący o braku komunikacji.
- ⑤ nazwa i zdjęcie zalogowanego użytkownika.

## Przyciski:



- kliknij, żeby otworzyć okno do konfiguracji systemu.



- kliknij, żeby zaimportować dane dotyczące użytkowników z plików z rozszerzeniem kkd (z programu ACCO-SOFT-LT) oraz z plików w formacie CSV.



- kliknij, żeby zapisać wprowadzone zmiany.

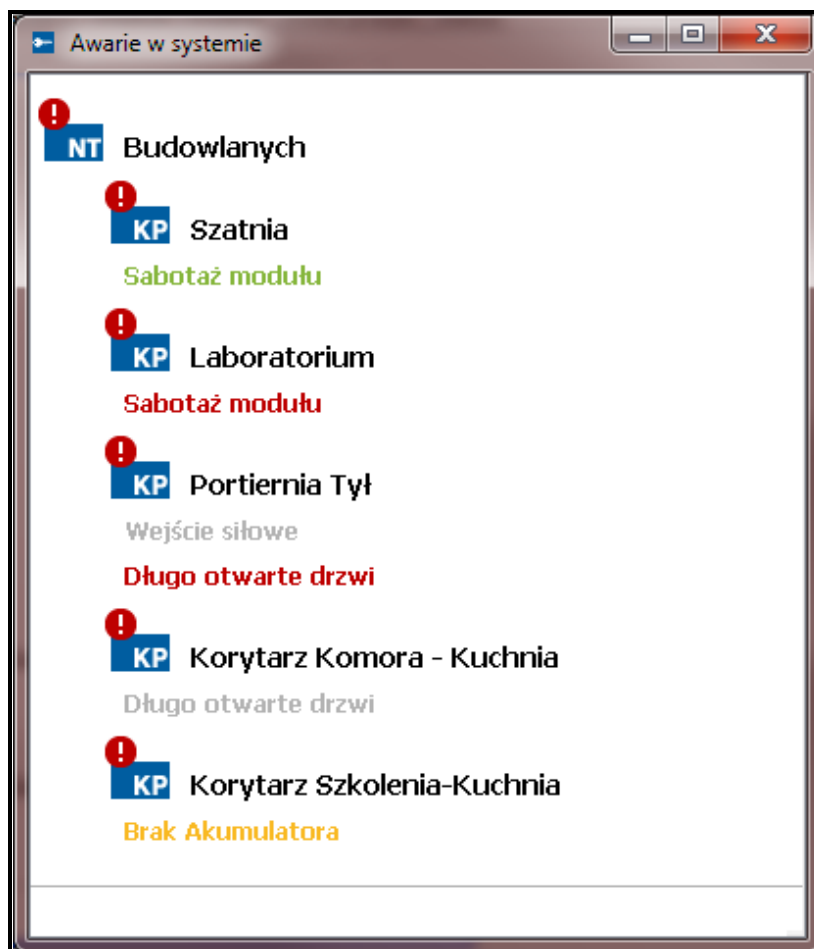


- kliknij, żeby cofnąć wszystkie wprowadzone zmiany od czasu ostatniego zapisu.



- kliknij, żeby otworzyć okno z informacjami dotyczącymi wersji systemu ACCO NET, programu ACCO Soft, a także wersji oraz adresów sieciowych serwera i bazy danych. Okno to umożliwia ponadto dostęp do licencji: programów ACCO Soft i ACCO Server oraz integracji systemów (patrz: rozdział „Licencje”).

## 4.1.1 Lista awarii / alarmów



Rys. 3. Przykładowa lista bieżących awarii w systemie.

W oknie w postaci drzewka pokazane są urządzenia wchodzące w skład systemu kontroli dostępu. Pod nazwą urządzenia, w którym doszło do awarii / alarmu, wyświetli się odpowiedni komunikat. Kolor komunikatu ma następujące znaczenie:

**czerwony** – alarm;




**pomarańczowy** – awaria;  
**zielony** – potwierdzony alarm / awaria;  
**szary** – pamięć alarmu / awarii.

#### 4.1.2 Licencje



Rys. 4. Okno z informacjami dotyczącymi wersji systemu ACCO NET, programów i bazy danych oraz z przyciskami umożliwiającymi dostęp do licencji.

W oknie, które otworzy się po kliknięciu na przycisk  w menu głównym programu, znajdują się „Informacje o licencjach” i następujące przyciski:

**Pokaż** [przy licencji ACCO Soft] – kliknij, żeby otworzyć okno z umową licencyjną do programu ACCO Soft.

**Pokaż** [przy licencji ACCO Server] – kliknij, żeby otworzyć okno z umową licencyjną do programu ACCO Server.

**Zarządzaj** [przy licencji integracji] – kliknij, żeby otworzyć okno „Licencje integracji”.

##### 4.1.2.1 Okno „Licencje integracji”

Patrz też rozdział „Integracja”.

Do centrali kontroli dostępu ACCO-NT można przypisać centrale alarmowe INTEGRA lub INTEGRA PLUS. Integracja centrali ACCO-NT z jednym systemem alarmowym jest darmowa. Klucz licencyjny jest konieczny, jeżeli centrala ACCO-NT ma być zintegrowana z więcej niż jedną centralą alarmową. Klucz generowany jest dla konkretnej centrali ACCO-NT. Określa maksymalną liczbę central alarmowych, które mogą być przez nią obsługiwane.

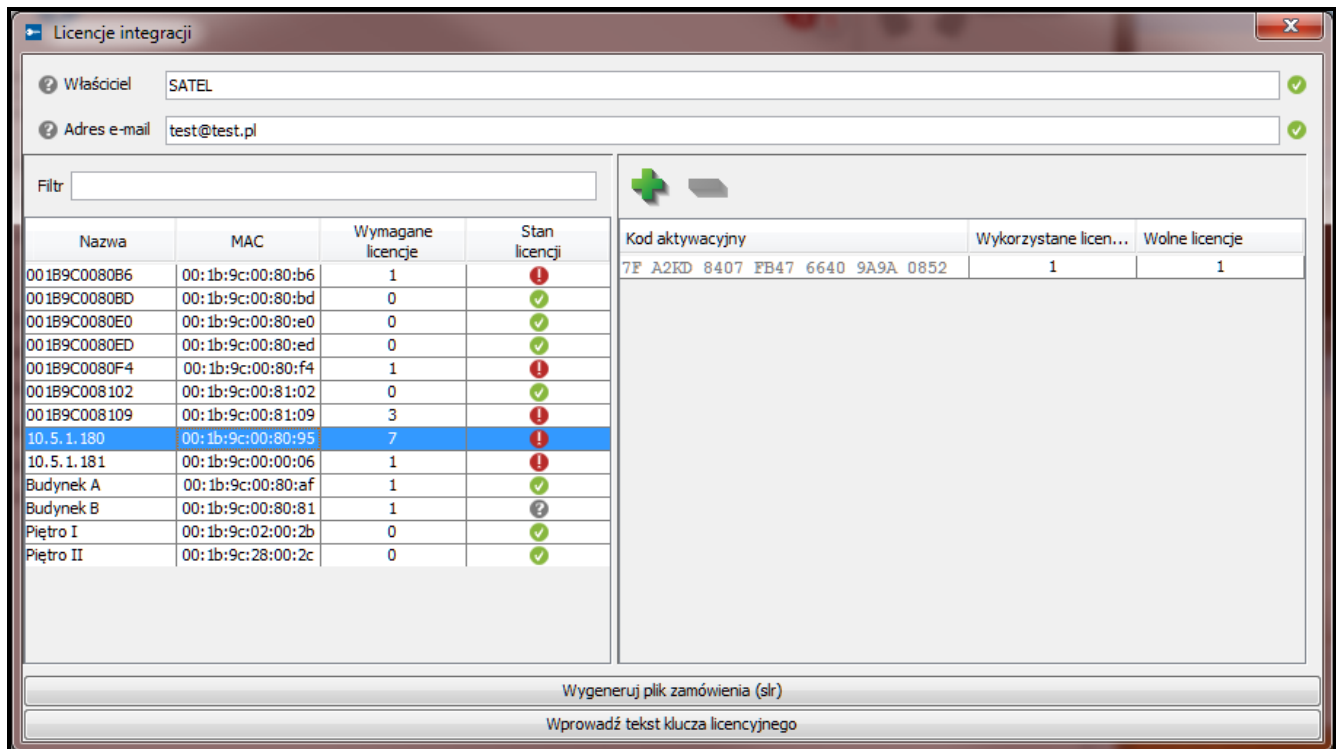
**Właściciel** – nazwa firmy / imię i nazwisko osoby, dla której ma zostać wygenerowany klucz licencyjny.

**Adres e-mail** – adres e-mail, na który ma zostać wysłany klucz licencyjny.

##### Tabela z listą central ACCO-NT w systemie ACCO NET

**Filtr** – po kliknięciu na pole wpisz część nazwy lub adresu MAC centrali. Dane są filtrowane po wpisaniu każdego znaku.

**Nazwa** – indywidualna nazwa centrali.



Rys. 5. Okno „Licencje integracji”.

**MAC** – numer identyfikacyjny karty sieciowej Ethernet (MAC) centrali.

**Wymagane licencje** – liczba licencji wymagana na potrzeby integracji. Odpowiada ona liczbie dodanych systemów alarmowych (patrz: rozdział "Integracja"), po odjęciu jednego (jeden system alarmowy nie wymaga licencji).

**Stan licencji** – w polu mogą być wyświetlane następujące informacje:

- ?
- ! – licencja zaszyfrowana (ikona zostanie wyświetlona, jeśli wprowadzony tekst klucza licencyjnego dla danej centrali ACCO-NT nie został odszyfrowany z powodu braku komunikacji pomiędzy ACCO Server a centralą ACCO-NT lub po restarcie programu ACCO Server, gdy program nie nawiązał jeszcze połączenia z daną centralą ACCO-NT),
- ! – liczba posiadanych licencji jest niewystarczająca,
- ✓ – liczba posiadanych licencji jest wystarczająca.

### Tabela z listą kodów aktywacyjnych

Po kliknięciu na centralę ACCO-NT zostanie wyświetlona tabela z listą kodów aktywacyjnych:



– kliknij, żeby dodać kod aktywacyjny.



– kliknij, żeby usunąć zaznaczony wcześniej kod aktywacyjny.

**Kod aktywacyjny** – numer kodu aktywacyjnego, który możesz zakupić u autoryzowanego dystrybutora firmy SATEL. Kod składa się z 26 znaków (cyfr i liter). Określa on liczbę licencji, które można uzyskać dla zintegrowanych systemów alarmowych.

**Wykorzystane licencje** – liczba wykorzystanych licencji na systemy alarmowe.

**Wolne licencje** – liczba niewykorzystanych licencji na systemy alarmowe.

## Przyciski

**Wygeneruj plik zamówienia (.slr)** – kliknij, żeby otworzyć okno „Licencje – podsumowanie”, które umożliwi wygenerowanie pliku zamówienia na klucz licencyjny (patrz: rozdział „Okno „Licencje – podsumowanie””).

**Wprowadź tekst klucza licencyjnego** – kliknij, żeby otworzyć okno „Wprowadź tekst klucza licencyjnego”, w którym możesz wkleić tekst klucza licencyjnego (patrz: rozdział „Okno „Wprowadź tekst klucza licencyjnego””).

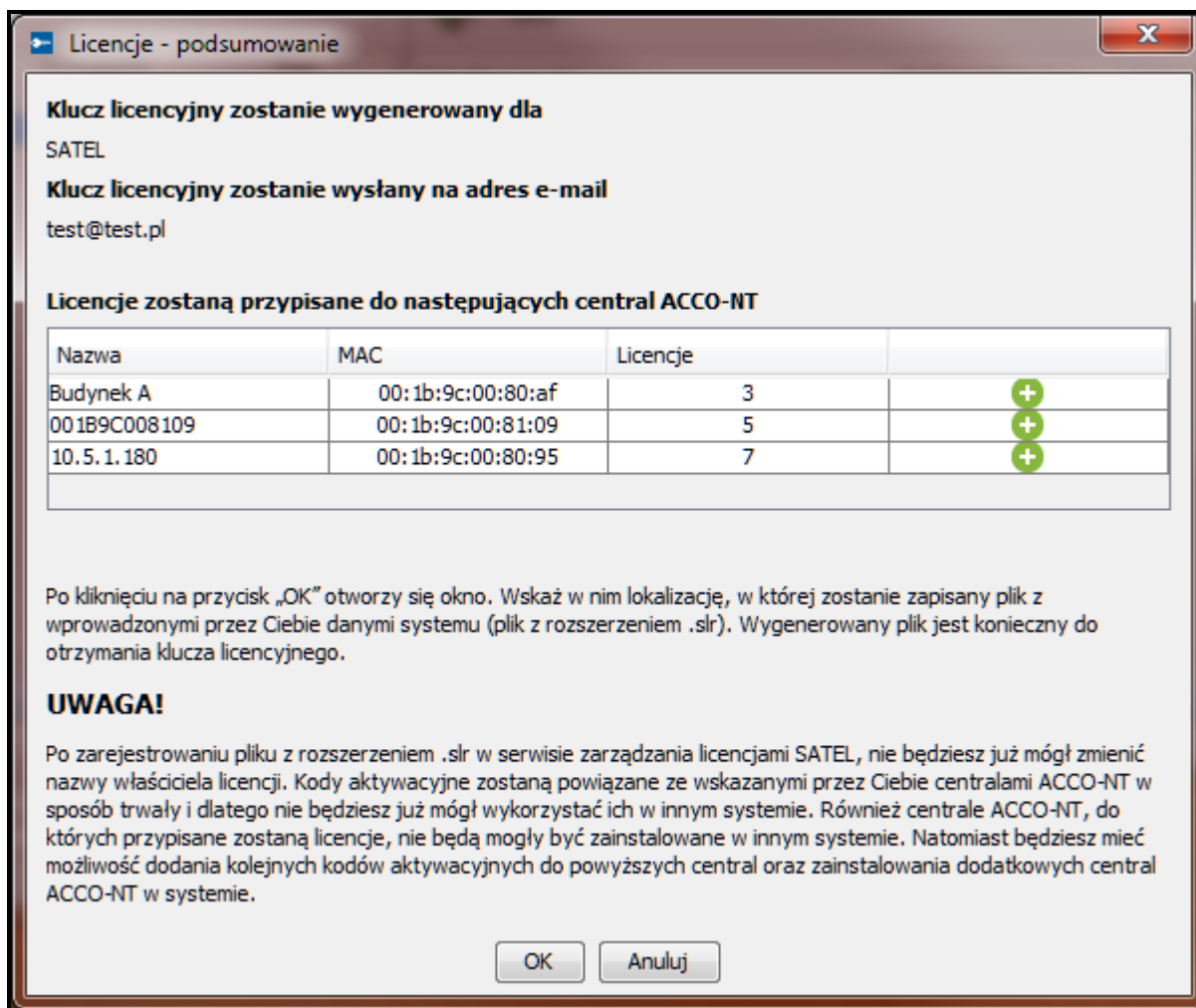
## Okno „Licencje – podsumowanie”

W oknie wyświetlane jest zestawienie na podstawie danych z okna „Licencje integracji”. Informacje te zostaną zapisane w pliku z rozszerzeniem .slr, na podstawie którego zostanie wygenerowany tekst klucza licencyjnego.

W tabeli z listą central ACCO-NT, do których zostaną przypisane licencje, w ostatniej kolumnie, wyświetlane są następujące informacje:

- + – nowa licencja,
- ✓ – licencja niezmieniona,
- ✓+ – zmodyfikowana licencja.

**OK** – kliknij na przycisk, żeby wygenerować plik zamówienia na klucz licencyjny. Otworzy się okno, w którym możesz wskazać, gdzie zapisać plik (z rozszerzeniem .slr) zawierający wyświetlone dane (patrz: rozdział „Uzyskanie licencji”).

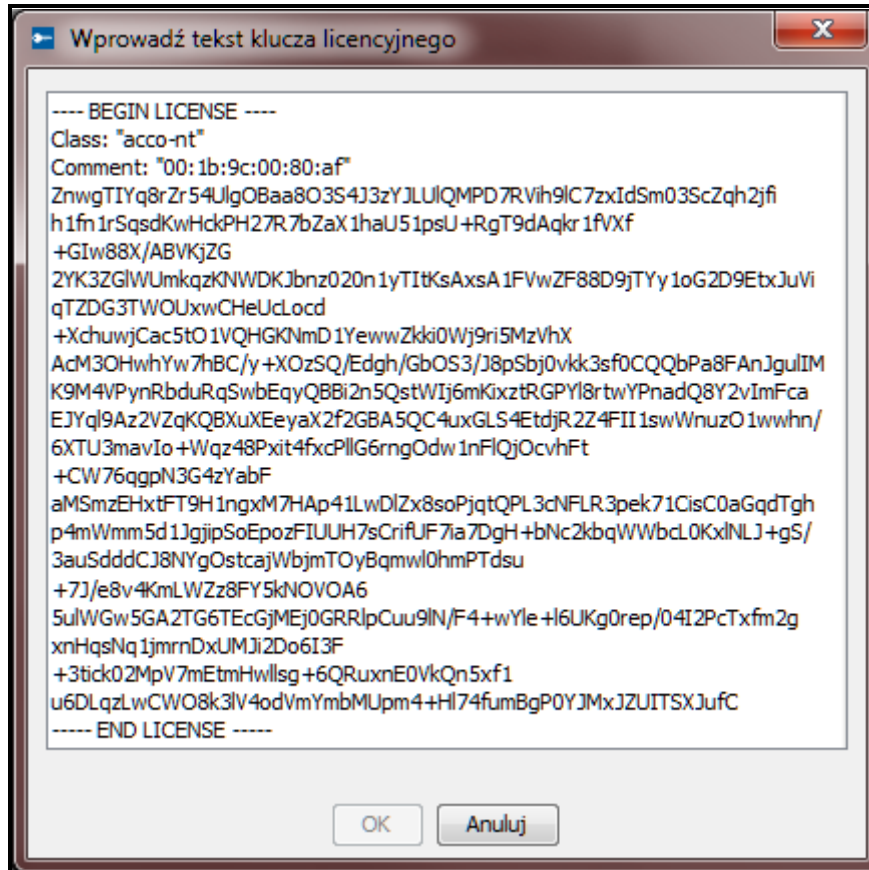


Rys. 6. Okno „Licencje – podsumowanie”.

## **Okno „Wprowadź tekst klucza licencyjnego”**

W oknie należy wprowadzić tekst klucza licencyjnego otrzymany w wiadomości e-mail.

**OK** – kliknij na przycisk, żeby wczytać do systemu klucz licencyjny zawierający licencje do systemów alarmowych. Przycisk staje się aktywny po wklejeniu skopiowanego tekstu. Jeżeli tekst będzie niepoprawny, wyświetli się komunikat informujący o tym.



Rys. 7. Okno z przykładowym tekstem klucza licencyjnego.

### **4.1.2.2 Uzyskanie licencji**

1. Zgodnie z procedurą opisaną w rozdziale „Dodanie systemu alarmowego”, dodaj system lub systemy alarmowe.

2. W menu głównym programu kliknij na przycisk



3. W oknie, które się otworzy, kliknij na przycisk „Zarządzaj”.

4. W polu „Właściciel” wpisz nazwę firmy lub imię i nazwisko osoby, dla której ma zostać wygenerowany klucz licencyjny.

5. W polu „Adres e-mail” wprowadź adres, na który ma zostać wysłany klucz licencyjny.

6. W tabeli z listą central ACCO-NT zaznacz centralę, która ma obsługiwać skonfigurowane systemy alarmowe.

7. Gdy wyświetli się tabela z listą kodów aktywacyjnych, kliknij na przycisk



8. W oknie „Kod aktywacyjny” wprowadź numer kodu, który znajduje się na Twoim kuponie aktywacyjnym. Jeśli dana centrala ACCO-NT ma obsługiwać więcej systemów alarmowych niż przewiduje dodany kod, wprowadź kolejne kody.



*Nie wprowadzaj kodu aktywacyjnego na większą liczbę systemów alarmowych, niż liczba systemów alarmowych dodanych w zakładce „Integracja” (patrz: rozdział „Integracja”).*

9. Jeżeli kolejna centrala ACCO-NT ma obsługiwać systemy alarmowe, zaznacz ją i powtórz czynności opisane w punktach 7 i 8.
10. Kliknij na przycisk „Wygeneruj plik zamówienia (slr)”.
11. W oknie „Licencje – podsumowanie” sprawdź, czy wszystkie dane są prawidłowe i zapoznaj się z informacjami, które wyświetlają się w dolnej części okna.
12. Kliknij na przycisk „OK”.
13. W oknie, które się otworzy, wskaż, gdzie zapisać plik zawierający Twoje dane i dane systemu (pliku z rozszerzeniem .slr). Możesz zmienić nazwę zapisywanego pliku. Kliknij na przycisk „Zapisz”.
14. Zarejestruj wygenerowany plik w serwisie zarządzania licencjami SATEL. W tym celu uruchom przeglądarkę internetową i wpisz w niej adres: <https://license.satel.pl>.



*Po zarejestrowaniu pliku z rozszerzeniem .slr w serwisie zarządzania licencjami SATEL:*


- *nie można zmienić nazwy właściciela licencji,*
- *kody aktywacyjne zostaną powiązane ze wskazanymi przez Ciebie centralami ACCO-NT w sposób trwały i nie będzie można wykorzystać ich w innym systemie,*
- *centrale ACCO-NT, do których przypisane zostaną licencje, nie będą mogły być zainstalowane w innym systemie.*

15. Na stronie, która się otworzy, kliknij na „ACCO NET”.
16. Zostaniesz przekierowany na stronę rejestracji produktu ACCO NET.
17. Kliknij na „Wybierz plik” i w oknie, które się otworzy, wskaż lokalizację wygenerowanego wcześniej pliku.
18. Kliknij na przycisk „Rejestracja”. Wyświetli się potwierdzenie zarejestrowania pliku. Dodatkowe potwierdzenie otrzymasz również w wiadomości wysłanej na adres e-mailowy, który podałeś podczas wypełniania danych.
19. Tekst klucza licencyjnego, który będzie zawierać zamówione przez Ciebie licencje, otrzymasz w kolejnej wiadomości e-mail.

#### **4.1.2.3 Wczytywanie licencji**

1. Gdy otrzymasz klucz licencyjny, upewnij się, że komunikacja pomiędzy ACCO Server a centralą / centralami ACCO-NT, dla których ma zostać wczytany klucz licencyjny, odbywa się poprawnie.



2. W menu głównym programu kliknij na przycisk .
3. W oknie, które się otworzy, kliknij na przycisk „Zarządzaj”.
4. W oknie „Licencje integracji” kliknij na przycisk „Wprowadź tekst klucza licencyjnego”.
5. Gdy otworzy się okno „Wprowadź tekst klucza licencyjnego”, wklej skopiowany tekst klucza licencyjnego, który otrzymałeś.



*Wklejany tekst klucza licencyjnego musi rozpoczynać się od zwrotu "---- BEGIN LICENSE ----", a kończyć na zwrocie "---- END LICENSE ----".*

6. Kliknij na przycisk „OK”.
7. Gdy klucz licencyjny zostanie wczytany, w kolumnie „Stan licencji”, przy centrali / centralach, dla której / których go wczytałeś, wyświetli się odpowiednia informacja.

## 4.2 Struktura systemu

### Opis przycisków



- kliknij, żeby dodać obiekt.



- kliknij, żeby usunąć zaznaczony obiekt.



- kliknij, żeby dodać centralę.



- kliknij, żeby usunąć zaznaczoną centralę.

### 4.2.1 Lista obiektów i central

Lista prezentuje obiekty oraz przypisane do nich centrale. Wyświetlana jest również gałąź z listą central nieprzypisanych. Przy każdej centrali widnieje ikona oznaczająca:



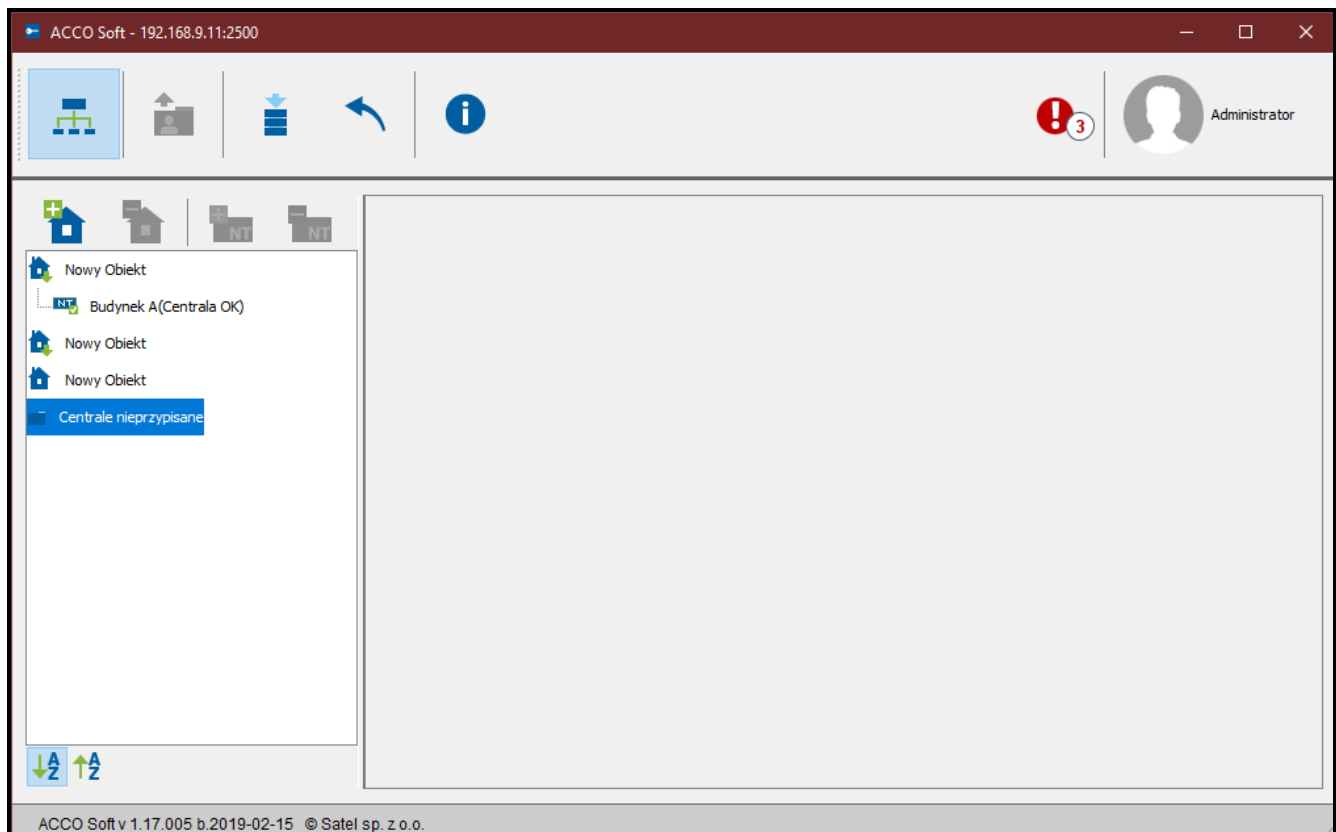
– brak połączenia z ACCO Server dłuższy niż 60 minut (biały wykrzyknik na czerwonym tle),



– brak połączenia z ACCO Server krótszy niż 60 minut (biały wykrzyknik na pomarańczowym tle),



– komunikacja z ACCO Server OK (biały symbol na zielonym tle).



Rys. 8. Lista obiektów i central.

W nawiasie za nazwą centrali wyświetlana jest informacja na temat jej stanu:

- Nieznany stan centrali,
- Brak komunikacji,

- Centrala OK,
- Przywracanie ustawień pełne,
- Przywracanie ustawień konfiguracji centrali,
- Pobieranie konfiguracji (przekazywanie przez ACCO Server do centrali wprowadzonych zmian w konfiguracji systemu),
- Rejestracja kontrolerów,
- Identyfikacja (podczas wyszukiwania kontrolerów),
- Rozsyłanie użytkowników (rozsyłanie danych dotyczących użytkowników do kontrolerów),
- Wymiana programu kontrolera,
- Niezgodne klucze kodowania (dotyczy klucza, jakim kodowane będą dane przesyłane pomiędzy ACCO Server a centralą),
- Wprowadzanie zmian do pamięci centrali,
- Wprowadzanie zmian do pamięci kontrolerów.
- Przyciski znajdujące się pod listą obiektów i central:



– kliknij, żeby uszeregować wszystkie obiekty z listy według nazw – od A do Z.



– kliknij, żeby uszeregować wszystkie obiekty z listy według nazw – od Z do A.


#### 4.2.1.1 Restart centrali

1. Jeśli chcesz zrestartować centralę, zaznacz wybrane urządzenie na liście.
2. Kliknij prawym przyciskiem myszki.
3. Gdy wyświetli się polecenie „Restart urządzenia”, kliknij na nie.



*Opcja „Restart urządzenia” jest dostępna tylko, gdy między centralą a ACCO Server odbywa się poprawna komunikacja.*

*W przypadku jakichkolwiek problemów z komunikacją, a tym samym i z restartem centrali, wyświetli się informujący o tym komunikat.*

4. Ikony wyświetlane przy nazwie centrali będą informować na bieżąco o przebiegu procesu restartu centrali.
5. Ponowne pojawienie się ikony  oznacza, że centrala została zrestartowana.

## 4.2.2 Obiekty

### 4.2.2.1 Dodanie obiektu

- Kliknij na przycisk . Nowy obiekt pojawi się na liście (patrz: rozdział „Lista obiektów i central”).

### 4.2.2.2 Programowanie obiektów

Kliknij na wybrany obiekt na liście obiektów, żeby go zaprogramować. Parametry obiektu wyświetlone zostaną w zakładkach „Ustawienia obiektu” oraz „Zarządzanie centralami”.

#### Parametry obiektu

##### Zakładka „Ustawienia obiektu”

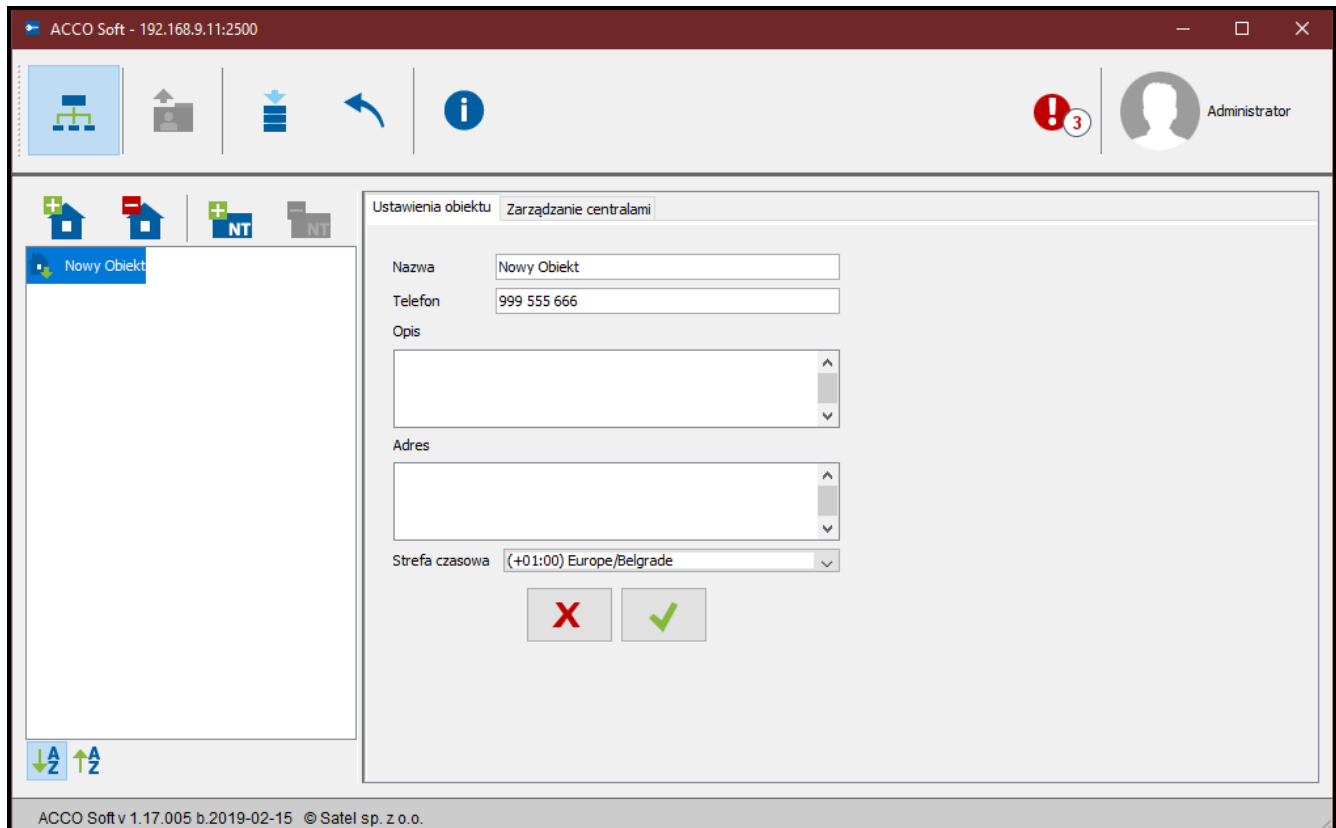
**Nazwa** – indywidualna nazwa obiektu (do 32 znaków).

**Telefon** – numer telefonu obiektu.

**Opis** – w polu można dodatkowo opisać obiekt.

**Adres** – adres obiektu.

**Strefa czasowa** – należy wskazać strefę czasową, czyli różnicę między czasem uniwersalnym (GMT) a czasem w strefie, w której znajduje się dany obiekt. Pozwoli to prawidłowo zapisywać czas zdarzeń do bazy danych, odpowiednio prezentować zdarzenia w aplikacji ACCO Web oraz wyświetlać właściwy czas na manipulatorach podłączonych do kontrolerów.



Rys. 9. Zakładka „Ustawienia obiektu”.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



– kliknij, żeby zatwierdzić wprowadzone zmiany.

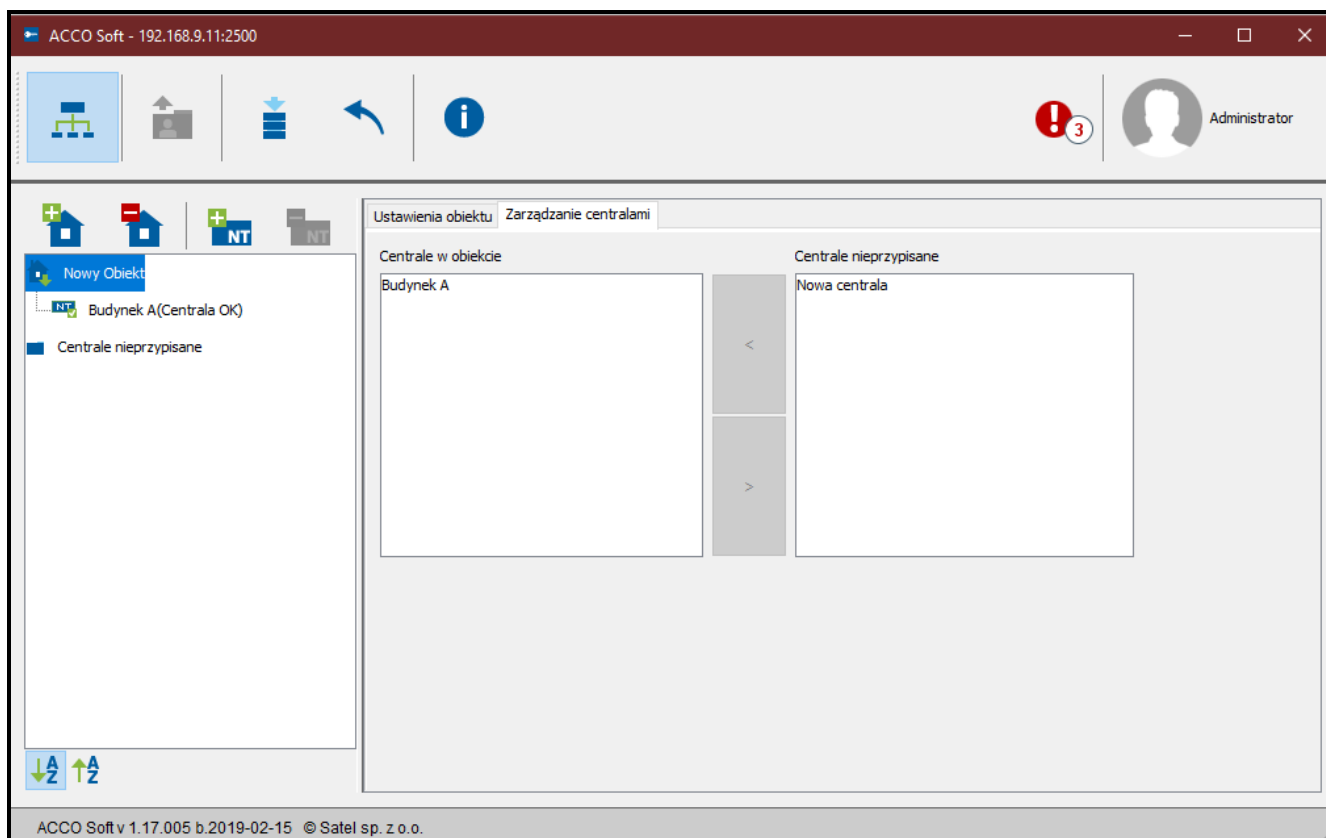
### Zakładka „Zarządzanie centralami”

**Centrale w obiekcie** – lista central przypisanych do obiektu.

**Centrale nieprzypisane** – lista central, które nie zostały jeszcze przypisane do żadnego obiektu.

Przyciski ze strzałkami służą do przenoszenia central pomiędzy listami – z listy central w obiekcie na listę central nieprzypisanych i odwrotnie.






Rys. 10. Zakładka „Zarządzanie centralami”.

#### 4.2.2.3 Usunięcie obiektu

1. Jeżeli chcesz usunąć pojedynczy obiekt, zaznacz kursorem wybrany obiekt na liście obiektów.
2. Jeśli chcesz usunąć za jednym razem kilka obiektów, zaznacz kursorem jeden z obiektów i trzymając wciśnięty klawisz Ctrl wybierz kolejne zaznaczając je lewym przyciskiem myszki.
3. W przypadku, gdy chcesz usunąć wszystkie obiekty jednocześnie, zaznacz kursorem jeden z obiektów i naciśnij jednocześnie klawisze Ctrl+A.



4. Kliknij wskaźnikiem myszki na przycisk .
5. Gdy wyświetli się pytanie, czy usunąć obiekt, kliknij „Tak”. Przypisane do usuniętego obiektu centrale zostaną przeniesione do kategorii central nieprzypisanych.
6. Zapisz wprowadzone zmiany.


### 4.2.3 Centrale

#### 4.2.3.1 Dodanie centrali ACCO-NT podłączonej do sieci Ethernet

1. Zaznacz na liście obiekt, do którego chcesz przypisać dodawaną centralę.
2. Przejdź do zakładki „Zarządzanie centralami”.
3. Zaznacz centralę na liście „Centrale nieprzypisane”. Prezentowane na niej są centrale, które połączyły się z ACCO Server (jako nazwa wyświetlany jest adres MAC centrali).
4. Kliknij na strzałkę, żeby przenieść centralę na listę „Centrale w obiekcie”.
5. Gdy wyświetli się pytanie, czy zapisać konfigurację, kliknij „Tak”.
6. Centrala wyświetli się na liście obiektów i central jako przypisana do dodanego obiektu.

#### 4.2.3.2 Dodanie centrali ACCO-NT przed podłączeniem jej do sieci Ethernet

1. Zaznacz na liście obiekt, do którego chcesz przypisać dodawaną centralę.

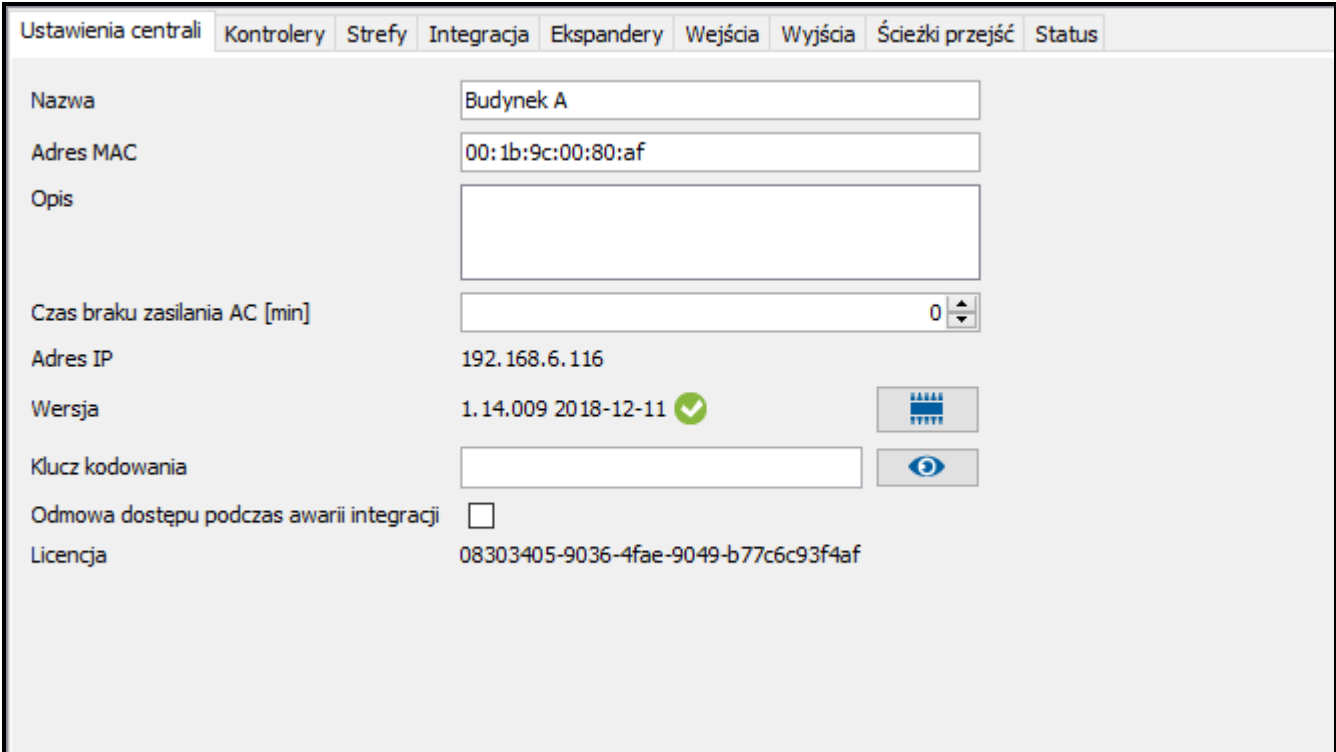
2. Przy pomocy przycisku  dodaj centralę. Zostanie ona wyświetlona na liście obiektów i central jako przypisana do dodanego obiektu.
3. Zaznacz centralę.
4. Kliknij na zakładkę „Ustawienia centrali”. Skonfiguruj ustawienia centrali, za wyjątkiem adresu MAC (patrz: rys. 11) i je zapisz.
5. Po podłączeniu centrali do sieci Ethernet i nawiązaniu przez nią komunikacji z ACCO Server, kliknij na symbol menu rozwijanego w polu „Adres MAC”. Wyświetlona zostanie lista adresów MAC central nieprzypisanych do obiektów.
6. Wybierz z listy adres MAC właściwej centrali.
7. Gdy wyświetli się pytanie, czy powiązać ze sobą urządzenia, kliknij „Tak”.


#### 4.2.3.3 Programowanie centrali

Kliknij na wybraną centralę na liście obiektów i central, żeby ją zaprogramować. Parametry wyświetlone zostaną w zakładce „Ustawienia centrali”.

#### Ustawienia centrali

**Nazwa** – indywidualna nazwa centrali (do 45 znaków). Domyślnie, jako nazwa używany jest adres MAC centrali.



Ustawienia centrali	Kontrolery	Strefy	Integracja	Ekspandery	Wejścia	Wyjścia	Ścieżki przejść	Status
Nazwa	Budynek A							
Adres MAC	00:1b:9c:00:80:af							
Opis								
Czas braku zasilania AC [min]	0							
Adres IP	192.168.6.116							
Wersja	1.14.009 2018-12-11 							
Klucz kodowania								
Odmowa dostępu podczas awarii integracji	<input type="checkbox"/>							
Licencja	08303405-9036-4fae-9049-b77c6c93f4af							

Rys. 11. Zakładka „Ustawienia centrali”.


**Adres MAC** – unikatowy numer identyfikacyjny karty sieciowej Ethernet (MAC) centrali. Jeżeli w polu wyświetlane jest polecenie „Powiąż z urządzeniem...”, możesz kliknąć na pole i wybrać adres MAC z listy.

**Opis** – w polu można dodatkowo opisać centralę.

**Czas braku zasilania AC [min]** – czas, przez który centrala musi być pozbawiona zasilania AC, aby zgłoszona została awaria. Opóźnienie zgłaszania awarii zapobiega informowaniu o krótkotrwałych zanikach zasilania nie mających wpływu na normalną pracę centrali. Maksymalnie zaprogramować można 60 minut.

**Adres IP** – adres IP centrali.

**Wersja** – wersja oprogramowania centrali (numer wersji i data kompilacji). Obok mogą wyświetlać się ikony informujące o wersji:

 – aktualna (biały symbol na zielonym tle),

 – do aktualizacji (biały wykrzykownik na pomarańczowym tle).

Ikona wyświetlana w przypadku centrali ACCO-NT w wersji oprogramowania 1.10.016 z dnia 09.02.2016 lub nowszej.



– kliknij na przycisk, jeżeli chcesz zaktualizować wersję oprogramowania centrali (patrz: rozdział „Zdalna aktualizacja oprogramowania centrali”).

**Klucz kodowania** – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne) określających klucz, jakim kodowane będą dane przesyłane pomiędzy serwerem ACCO Server a centralą. **Musi być zgodny z kluczem zdefiniowanym w centrali przy pomocy programu ACCO-NT Conf.** Serwer nawiąże połączenie tylko z urządzeniem, które będzie się posługiwało właściwym kluczem.



– kliknij na przycisk, żeby sprawdzić wpisaną wartość.

**Odmowa dostępu podczas awarii integracji** – jeżeli zaznaczysz opcję, w przypadku braku komunikacji z centralą alarmową, uzyskanie dostępu do zintegrowanej strefy systemu kontroli dostępu nie będzie możliwe do czasu przywrócenia poprawnej komunikacji. Jeżeli odznaczysz opcję, w przypadku braku komunikacji z centralą alarmową, dostęp do zintegrowanej strefy systemu kontroli dostępu będzie można uzyskać na takich samych zasadach, jakie obowiązują bez integracji systemów. Opcja dotyczy wszystkich central alarmowych przypisanych do danej centrali ACCO-NT (patrz: rozdział „Integracja”).



*Jeżeli opcja „Odmowa dostępu podczas awarii integracji” jest wyłączona i utracona zostanie łączność między ACCO NET a system alarmowym, strefa systemu ACCO NET mająca status „Czuwa”, przyjmie status „Strefa zablokowana”. Dzięki temu będzie można uzyskać dostęp do poszczególnych przejść systemu ACCO NET. W momencie, gdy użytkownik uzyska dostęp do tej strefy, strefa przyjmie status „Strefa kontrolowana”. Po powrocie komunikacji między systemami, strefa znowu przyjmie status „Czuwa”.*

**Licencja** – numer licencji przypisanej do centrali lub komunikat informujący o stanie licencji.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.





– kliknij, żeby zatwierdzić wprowadzone zmiany.

#### 4.2.3.4 Zdalna aktualizacja oprogramowania centrali

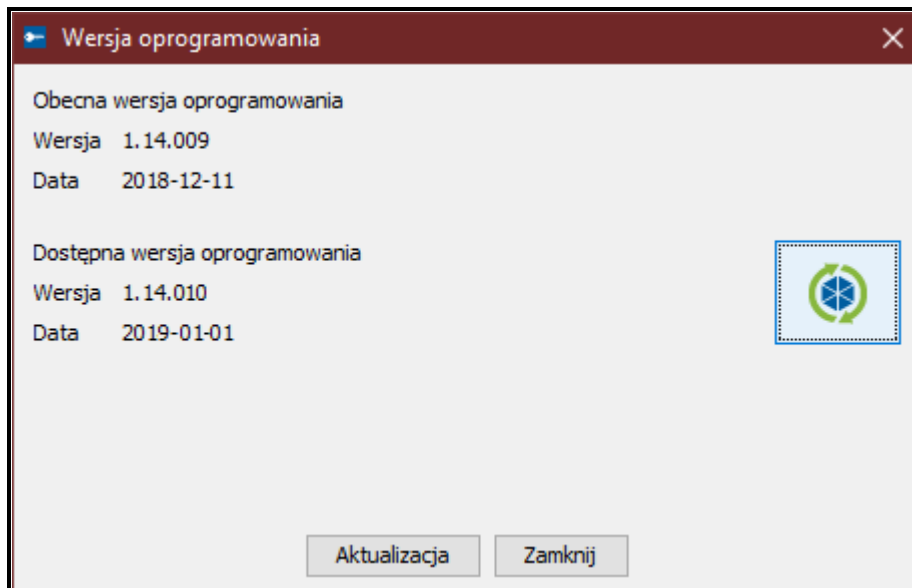


*Zdalną aktualizację oprogramowania można przeprowadzić w centrali ACCO-NT w wersji oprogramowania 1.10.016 z dnia 09.02.2016 i nowszej.*

*Po zaktualizowaniu oprogramowania centrali ACCO-NT zaleca się aktualizację oprogramowania wszystkich modułów kontroli dostępu podłączonych do tej centrali (patrz: rozdział „Zdalna aktualizacja oprogramowania kontrolera”).*


1. Jeżeli w polu „Wersja”, przy aktualnej wersji oprogramowania centrali, wyświetla się ikona , kliknij na przycisk .
2. W oknie, które się otworzy, wyświetlą się dane aktualnej wersji oprogramowania urządzenia, a także informacje dotyczące nowej dostępnej wersji (patrz: rys. 12).
3. Kliknij na przycisk „Aktualizacja”.

4. Rozpocznie się proces aktualizacji oprogramowania centrali.
5. Gdy aktualizacja zostanie przeprowadzona, wyświetli się odpowiedni komunikat.
6. Kliknij na przycisk „OK” i zamknij okno „Wersja oprogramowania”.







Rys. 12. Okno umożliwiające aktualizację oprogramowania centrali.

#### 4.2.3.5 Usunięcie centrali

1. Na liście obiektów i central zaznacz centralę, która ma zostać usunięta.
2. Kliknij wskaźnikiem myszki na przycisk .
3. Gdy wyświetli się pytanie, czy usunąć centralę, kliknij „Tak”. Jeżeli usuwana centrala była przypisana do obiektu, zostanie przeniesiona do kategorii central nieprzypisanych. Jeżeli usuwana centrala nie była przypisana do obiektu (znajdowała się na liście central nieprzypisanych), zostanie usunięta z systemu.
4. Zapisz wprowadzone zmiany.

#### 4.2.4 Kontrolery


##### Opis przycisków

-  - kliknij, żeby dodać moduł.
-  - kliknij, żeby z listy modułów usunąć zaznaczony wcześniej moduł (patrz: rozdział „Usunięcie kontrolera”).
-  - kliknij, żeby uruchomić procedurę identyfikacji modułów podłączonych do centrali. Po jej zakończeniu wyświetli się okno „Podsumowanie” z informacjami dotyczącymi zidentyfikowanych kontrolerów (patrz: rozdział „Identyfikacja kontrolerów podłączonych do systemu”). Przycisk dostępny tylko wtedy, gdy centrala, do której zostały podłączone kontrolery, ma status „Centrala OK” (status wyświetla się w nawiasie obok nazwy centrali na liście obiektów i central), a wprowadzone zmiany zostały zapisane.
-  - kliknij, żeby uruchomić procedurę aktualizacji oprogramowania zaznaczonego modułu / zaznaczonych modułów. Przycisk dostępny, gdy nie ma zmian do zapisania (patrz: rozdział „Zdalna aktualizacja oprogramowania kontrolera”).

Pod przyciskami wyświetlana jest liczba kontrolerów. Po najechaniu kursorem na liczbę wyświetli się informacja o liczbie kontrolerów podłączonych do pierwszej i drugiej magistrali RS-485 wybranej centrali ACCO-NT.

#### 4.2.4.1 Identyfikacja kontrolerów podłączonych do systemu

Każdy moduł musi zostać zidentyfikowany, aby centrala ACCO-NT mogła nawiązać z nim komunikację. Pozwoli to na odczytanie i zapisanie jego danych.

1. Na liście obiektów i central zaznacz centralę, do której są podłączone moduły.
2. Przejdź do zakładki „Kontrolery” i kliknij na przycisk .
3. W oknie, które się otworzy, wyświetlane będą informacje dotyczące postępu identyfikacji (możesz przerwać procedurę klikając na przycisk „Pobierz wyniki”).
4. Wyświetlone zostanie okno „Podsumowanie” (patrz: rozdział „Okno „Podsumowanie”). Nowe kontrolery będą miały status „Nowy”.
5. Kliknij na przycisk „Zatwierdź”.
6. Wyświetlone zostanie okno z pytaniem, czy zapisać konfigurację. Kliknij „Tak”.





*Funkcję identyfikacji należy uruchamiać za każdym razem, gdy do którejkolwiek z magistral zostanie podłączone nowe urządzenie lub zostanie zmieniony adres w urządzeniu podłączonym do którejkolwiek z magistral.*

*Odłączenie zidentyfikowanego urządzenia od magistrali komunikacyjnej spowoduje:*

- wygenerowanie zdarzenia informującego o awarii centrali, o treści „Początek awarii. Brak kontrolera. Indeks urządzenia...”,
- zmianę koloru nazwy kontrolera na czerwony na liście kontrolerów (patrz: rozdział „Tabela z listą kontrolerów”).

*Użytkownicy mogą uzyskać dostęp do strefy od razu po zarejestrowaniu kontrolera nadzorującego przejście należące do strefy.*

#### 4.2.4.2 Dodanie kontrolera przed podłączeniem go do systemu

1. Na liście obiektów i central zaznacz centralę, do której chcesz dodać kontroler.
2. Kliknij na przycisk .
3. W oknie, które zostanie wyświetlone, wybierz adres modułu i kliknij „Dodaj”.
4. Skonfiguruj ustawienia modułu i je zapisz.
5. Po podłączeniu kontrolera do centrali (podłączonej do sieci Ethernet), kliknij na przycisk .
6. W oknie, które się otworzy, wyświetlane będą informacje dotyczące postępu identyfikacji (możesz przerwać procedurę klikając na przycisk „Pobierz wyniki”).
7. Wyświetlone zostanie okno „Podsumowanie” (patrz: rozdział „Okno „Podsumowanie”). Kontroler będzie miał status „Zmieniony”.
8. Kliknij na przycisk „Zatwierdź”.
9. Wyświetlone zostanie okno z pytaniem, czy zapisać konfigurację. Kliknij „Tak”.

#### 4.2.4.3 Okno „Podsumowanie”

**Liczba zidentyfikowanych kontrolerów** – liczba wyszukanych i zidentyfikowanych kontrolerów.

**Adres** – adres ustawiony w kontrolerze.

**Nazwa modułu** – nazwa kontrolera.

**Status** – w polu mogą wyświetlać się następujące informacje:

**Niezmieniony** – moduł, którego dane są zgodne z danymi w programie.

**Nowy** – moduł, który został dodany do systemu.

**Zmieniony** – moduł, którego dane nie są zgodne z danymi w programie.

**Brak komunikacji** – moduł, który był wcześniej obecny w systemie, a z którym, podczas bieżącej procedury identyfikacji, centrala nie nawiązała komunikacji.

**Wersja** – wersja oprogramowania kontrolera (numer wersji i data kompilacji).

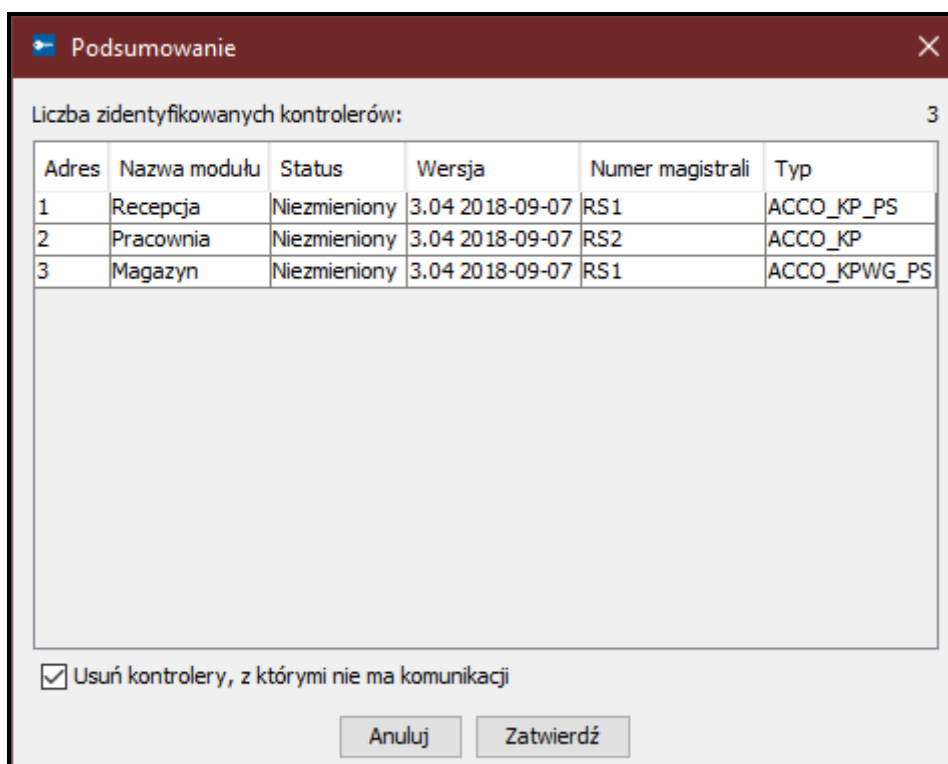
**Numer magistrali** – numer magistrali RS-485, do której podłączony jest zidentyfikowany kontroler.

**Typ** – rodzaj kontrolera.

**Usuń kontrolery, z którymi nie ma komunikacji** – jeżeli opcja jest włączona, kontrolery, z którymi nie udało się nawiązać komunikacji, zostaną usunięte po kliknięciu na przycisk „Zatwierdź”. Jeżeli opcja jest wyłączona, po kliknięciu na przycisk „Zatwierdź”, żaden z kontrolerów nie zostanie usunięty.

**Anuluj** – kliknij, żeby anulować procedurę identyfikacji.

**Zatwierdź** – kliknij, żeby zatwierdzić dane odczytane podczas identyfikacji.



Rys. 13. Okno „Podsumowanie” wyświetlane po zakończeniu procedury identyfikacji kontrolerów.

#### 4.2.4.4 Tabela z listą kontrolerów

**Adres** – adres kontrolera.





**Nazwa** – indywidualna nazwa kontrolera (do 32 znaków). Nazwy kontrolerów mogą być prezentowane w następujących kolorach:

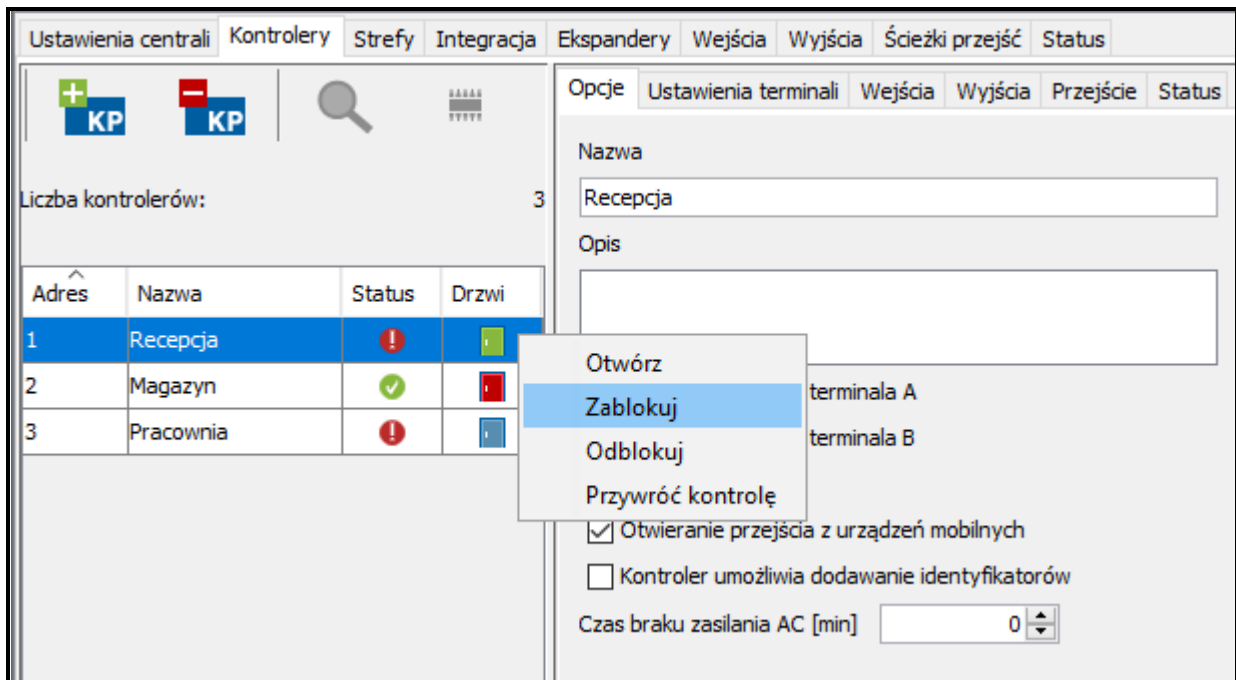
**szary** – kontroler dodany, ale jeszcze niezapisany;

**czerwony** – kontroler zapisany; brak komunikacji z kontrolerem;

**czarny** – kontroler zapisany; komunikacja poprawna.










**Status** – informacje o statusie kontrolera. Poszczególne ikony symbolizują następujący stan:

-  – alarm / awaria (biały wykrzyknik na czerwonym tle),
-  – pamięć alarmu / awarii (biały wykrzyknik na szarym tle),
-  – wszystko OK (biały symbol na zielonym tle),
-  – brak komunikacji z centralą (biały znak zapytania na szarym tle).
- Po kliknięciu na ikonę wyświetlona zostanie zakładka „Status”.



Rys. 14. Lista kontrolerów w zakładce „Kontrolery”.

**Drzwi** – informacje o stanie przejścia i drzwi nadzorowanych przez kontroler. Poszczególne ikony symbolizują następujący stan:

-  – przejście zablokowane (czerwone drzwi zamknięte),
-  – przejście zablokowane i otwarte drzwi (czerwone drzwi uchylone),
-  – przejście zablokowane z powodu alarmu (czerwony dzwonek i czerwone drzwi zamknięte),
-  – przejście zablokowane z powodu alarmu i otwarte drzwi (czerwony dzwonek i czerwone drzwi uchylone),
-  – przejście kontrolowane i zamknięte drzwi (zielone drzwi zamknięte),
-  – przejście kontrolowane i otwarte drzwi (zielone drzwi uchylone),
-  – przejście odblokowane (niebieskie drzwi zamknięte),
-  – przejście odblokowane i otwarte drzwi (niebieskie drzwi uchylone),
-  – przejście odblokowane z powodu pożaru (czerwony płomień i niebieskie drzwi zamknięte),
-  – przejście odblokowane z powodu pożaru i otwarte drzwi (czerwony płomień i niebieskie drzwi uchylone).

Po zaznaczeniu wybranego kontrolera na liście i kliknięciu na nim prawym przyciskiem myszki, wyświetli się rozwijane menu:

**Otwórz** – po wybraniu funkcji nastąpi otwarcie przejścia nadzorowanego przez wybrany kontroler na czas zaprogramowany w polu „Czas na wejście” w zakładce „Przejście”.

**Zablokuj** – po wybraniu funkcji nastąpi trwałe zamknięcie przejścia. Przejście pozostanie zamknięte do czasu zmiany jego stanu przez użytkownika posiadającego uprawnienie „Przełączanie” (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Odblokuj** – po wybraniu funkcji nastąpi trwałe otwarcie przejścia. Przejście pozostanie otwarte do czasu zmiany jego stanu przez użytkownika posiadającego uprawnienie „Przełączanie” (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Przywróć kontrolę** – po wybraniu funkcji zostanie przywrócona kontrola przejścia.

#### 4.2.4.5 Programowanie kontrolera

Kliknij na wybrany moduł na liście kontrolerów, żeby go zaprogramować. Parametry modułu wyświetlone zostaną w zakładkach w oknie obok.

#### Zakładka „Opcje”

The screenshot displays the 'Opcje' (Options) configuration window for a controller. At the top, there are navigation tabs: 'Ustawienia centrali', 'Kontrolery', 'Strefy', 'Integracja', 'Ekspandery', 'Wejścia', 'Wyjścia', 'Ścieżki przejść', and 'Status'. Below these, there are two 'KP' buttons (one green with a plus, one red with a minus) and a search icon. A label 'Liczba kontrolerów:' is followed by the number '3'. A table lists the controllers:

Adres	Nazwa	Status	Drzwi
1	Recepcja	!	🟢
2	Magazyn	✓	🔴
3	Pracownia	!	🔵

The right side of the window shows the configuration for the selected controller 'Recepcja'. It includes a 'Nazwa' field with the value 'Recepcja' and an empty 'Opis' field. Below these are several checkboxes: 'Kontroluj obecność terminala A' (checked), 'Kontroluj obecność terminala B' (checked), 'Anti-Skaner' (unchecked), and 'Otwieranie przejścia z urządzeń mobilnych' (checked). There is also an unchecked checkbox for 'Kontroler umożliwia dodawanie identyfikatorów'. At the bottom, there is a dropdown menu for 'Czas braku zasilania AC [min]' set to '0'.

Rys. 15. Zakładka „Opcje”.

**Nazwa** – indywidualna nazwa kontrolera (do 32 znaków).

**Opis** – w polu możesz dodatkowo opisać kontroler.

**Kontroluj obecność terminala A / B** – po włączeniu opcji moduł sprawdza obecność manipulatorów LCD, klawiatur oraz czytników kart zbliżeniowych pracujących w charakterze terminala A lub B. W pierwszej kolejności sprawdzana jest obecność manipulatorów LCD i klawiatur, a dopiero potem obecność czytników kart zbliżeniowych. Jeżeli opcja jest wyłączona, moduł w żaden sposób nie zgłosi braku terminala (nie zostanie wygenerowany alarm, nie zostanie zapisane zdarzenie i nie zostanie wyzwolone wyjście „Brak obecności terminala”).



Moduł nie ma możliwości sprawdzania obecności czytników pastylek DALLAS. W przypadku podłączenia tego typu czytnika zaleca się nie włączać opcji „Kontroluj obecność terminala A / B”.



**Anti-Skaner** – po włączeniu opcji, 5 prób uzyskania dostępu na podstawie nieznannej karty, nieznannej pastylki lub kodu w ciągu 3 minut spowoduje blokadę terminali na około 5 minut.

**Otwieranie przejścia z urządzeń mobilnych** – po włączeniu opcji przejście może być otwierane przez użytkownika przy pomocy urządzeń mobilnych.

**Kontroler umożliwia dodawanie identyfikatorów** – po włączeniu opcji, kontroler zostanie wyświetlony podczas dodawania użytkownikowi karty / sprawdzania karty użytkownika w aplikacji ACCO Web. Jeżeli opcja będzie wyłączona, kontroler nie będzie widoczny (nie dotyczy to modułów, do których podłączone są czytniki obsługujące formaty DALLAS, EM Marin oraz Wiegand 40/42/56 – są one zawsze widoczne).



*Karta dodana przy pomocy czytnika obsługującego dany typ formatu Wiegand, będzie odczytywana tylko przez terminale obsługujące ten typ formatu oraz terminale odczytujące krótsze liczby bitów numerów kart. Przykładowo: jeżeli karta zostanie dodana przy pomocy czytnika obsługującego format Wiegand 34, to karta będzie odczytywana przez terminale obsługujące formaty Wiegand 34/32/26. Dlatego zaleca się dodawać karty na terminalach odczytujących najdłuższe liczby bitów numerów kart. Karta dodana w ten sposób będzie obsługiwana na wszystkich czytnikach w systemie, również tych, które odczytują krótsze liczby bitów numerów kart.*

**Czas braku zasilania AC [min]** – funkcja dotyczy modułów ACCO-KP-PS i ACCO-KPWG-PS. Pozwala zdefiniować czas, przez który moduł może być pozbawiony zasilania AC. Po upływie tego czasu zostanie zgłoszona awaria. Czas programowany jest w minutach i może wynosić maksymalnie 255 minut. Wpisanie wartości 0 oznacza, że awaria zasilania AC nie będzie zgłaszana.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



– kliknij, żeby zatwierdzić wprowadzone zmiany.

## **Zakładka „Ustawienia terminali”**

### **Zakładka „Terminal A / B”**

**Format transmisji terminala A / B** – funkcja pozwala określić format transmisji danych przez terminale obsługiwane przez kontroler.



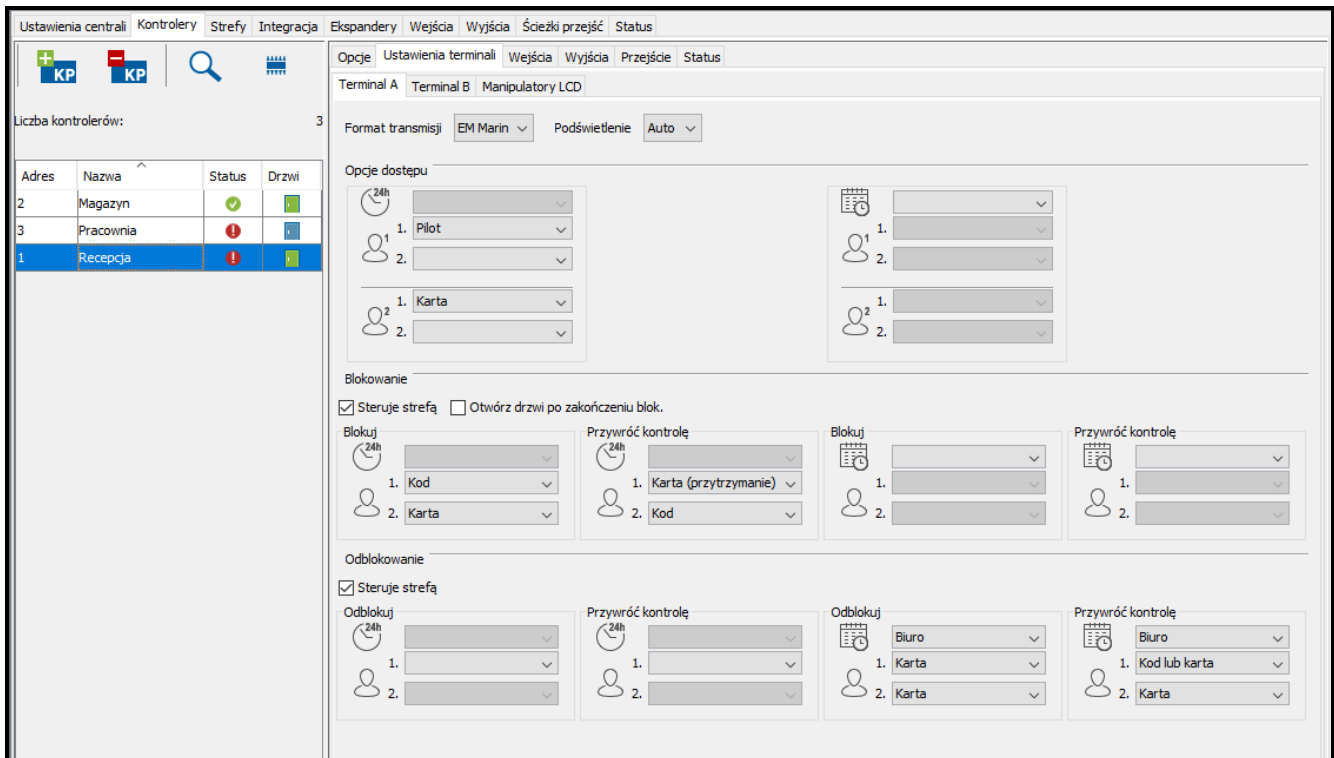
*W przypadku, gdy zostanie wybrany format WIEGAND, przytrzymanie karty przed czytnikiem przez około 3 sekundy nie spowoduje:*

- otwarcia przejścia zamkniętego z powodu alarmu (typ reakcji wejścia kontrolera: „Alarm – zablokowanie przejścia”),
- zablokowania / odblokowania strefy (włączona jest opcja „Steruje strefą” i nie są obsługiwane inne identyfikatory oprócz kart),
- otwarcia wszystkich przejść w strefie zamkniętych z powodu alarmu (typ reakcji wejścia centrali ACCO-NT: „Alarmowe zablokowanie strefy”),
- załączenia czuwania w zintegrowanej strefie systemu alarmowego (włączona jest opcja „Steruje strefą” i nie są obsługiwane inne identyfikatory oprócz kart),
- wyłączenia czuwania w zintegrowanej strefie systemu alarmowego (włączona jest opcja „Steruje strefą” i nie są obsługiwane inne identyfikatory oprócz kart).

**Podświetlenie terminala A / B** – funkcja określająca zasady podświetlania klawiszy oraz wyświetlacza w podłączonych do modułu manipulatorach LCD lub klawiaturach. Dostępne są następujące możliwości:

- podświetlenie wyłączone;

- podświetlenie automatyczne włączane po naciśnięciu dowolnego klawisza lub zbliżeniu karty;
- podświetlenie stałe.



Rys. 16. Zakładka „Terminal A”.

## Opcje dostępu



Jeżeli użytkownik ma mieć dostęp do danej strefy, w aplikacji ACCO Web musi mieć włączoną opcję „Uprawniony do dostępu” oraz przypisany odpowiedni kalendarz dostępu (→„Użytkownicy” →„Lista” →[nazwa użytkownika] →zakładka „Strefy”).

Jeżeli dostęp ma być udzielany na podstawie dwóch identyfikatorów:

- po użyciu 1. identyfikatora, urządzenia pracujące w charakterze terminali poinformują o konieczności użycia 2. identyfikatora (manipulator LCD poprzez komunikat na wyświetlaczu, klawiatury oraz czytniki kart zbliżeniowych poprzez dodatkową sygnalizację dźwiękową – 3 krótkie dźwięki),
- użytkownik ma na wprowadzenie 2. identyfikatora 30 sekund.

Konfiguracja opcji dostępu opisana w niniejszym rozdziale jest możliwa w przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej. W przypadku centrali z niższą wersją oprogramowania, dotychczasowy typ identyfikatora określający sposób dostępu zostanie przypisany pierwszemu użytkownikowi dla terminala A według następujących zasad:

- karta = 1. identyfikator: karta, 2. identyfikator: niezdefiniowany,
- kod = 1. identyfikator: kod, 2. identyfikator : niezdefiniowany,
- karta i kod = 1. identyfikator: kod lub karta, 2. identyfikator: kod lub karta,
- karta lub kod = 1. identyfikator: kod lub karta, 2. identyfikator: niezdefiniowany.

Ustawienia konfiguracyjne dla terminala B będą niedostępne.

W przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej, po aktualizacji systemu ACCO NET do wersji 1.6, dotychczasowe ustawienia opcji dostępu zostaną przypisane pierwszemu użytkownikowi jako obowiązujące przez całą dobę dla obu terminali danego kontrolera i odwzorowane w sposób opisany wyżej.

Dostęp można uzyskiwać lub potwierdzać przy pomocy:

- kodu,
- karty,
- pilota,
- kodu lub karty,
- karty lub pilota,
- kodu lub pilota,
- kodu, karty lub pilota.



### **– zasady dostępu obowiązujące przez całą dobę**



Jeżeli nie zdefiniujesz zasad dostępu obowiązujących przez całą dobę, dostęp będzie udzielany użytkownikom na zasadach obowiązujących w czasie określonym przez wybrany kalendarz dostępu.



– zasady dostępu użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik uzyska dostęp przy pomocy pierwszego identyfikatora).



– zasady potwierdzania dostępu przez drugiego użytkownika (zdefiniuj, jeżeli uzyskanie dostępu ma być uzależnione od drugiego użytkownika):

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, do potwierdzenia dostępu wystarczy pierwszy identyfikator).



Użytkownik potwierdzający dostęp musi mieć w aplikacji ACCO Web włączoną opcję „Potwierdzenie” (→„Użytkownicy” →„Lista” →[nazwa użytkownika] →zakładka „Strefy”).



### **– zasady dostępu obowiązujące w czasie określonym przez kalendarz dostępu**



Jeżeli nie zdefiniujesz zasad dostępu obowiązujących w czasie określonym przez kalendarz dostępu, dostęp będzie udzielany na zasadach obowiązujących przez całą dobę.



– kliknij na pole, jeśli w czasie określonym przez kalendarz dostępu dostęp ma być przydzielany użytkownikom według innych zasad niż przez całą dobę. Wyświetlona zostanie lista utworzonych w aplikacji ACCO Web kalendarzy dostępu. Kliknij na jeden z nich.



– zasady dostępu użytkownika:

1. – pierwszy identyfikator,

2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik uzyska dostęp przy pomocy pierwszego identyfikatora).



- zasady potwierdzania dostępu przez drugiego użytkownika (zdefiniuj, jeżeli uzyskanie dostępu, ma być uzależnione od drugiego użytkownika):

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, do potwierdzenia dostępu wystarczy pierwszy identyfikator).



*Użytkownik potwierdzający dostęp musi mieć w aplikacji ACCO Web włączoną opcję „Potwierdzenie” (→„Użytkownicy” →„Lista” →[nazwa użytkownika] →zakładka „Strefy”).*

## **Opcje sterowania – Blokowanie**



*Funkcje sterowania są poprawnie realizowane tylko wtedy, gdy jedno z wejść modułu kontroluje stan drzwi (zaprogramowane jest jako „Czujnik otwarcia drzwi”).*

*Jeżeli użytkownik ma sterować strefą, musi mieć dostęp do danej strefy oraz uprawnienie do przełączania jej stanu (włączone opcje „Uprawniony do dostępu” i „Przełączanie” w aplikacji ACCO Web (→„Użytkownicy” →„Lista” →[nazwa użytkownika] →zakładka „Strefy”)) oraz przypisany kalendarz dostępu.*

*Jeżeli sterowanie strefą ma się odbywać przy pomocy dwóch identyfikatorów:*

- po użyciu 1. identyfikatora, urządzenia pracujące w charakterze terminali poinformują o konieczności użycia 2. identyfikatora (manipulator LCD poprzez komunikat na wyświetlaczu, klawiatury oraz czytniki kart zbliżeniowych poprzez dodatkową sygnalizację dźwiękową – 3 krótkie dźwięki),
- użytkownik ma na wprowadzenie 2. identyfikatora 30 sekund.

*Należy zdefiniować identyfikatory służące zarówno do blokowania strefy, jak i przywracania jej kontroli.*

*Jeżeli:*

- pierwsze identyfikatory służące do blokowania strefy są takie same jak pierwsze identyfikatory służące do odblokowania strefy i /lub
- pierwsze identyfikatory służące do przywracania kontroli w zablokowanej strefie są takie same jak pierwsze identyfikatory służące do przywracania kontroli w odblokowanej strefie,

*od stanu drzwi zależy, jak zmieni się stan strefy. Jeśli drzwi są zamknięte, po użyciu identyfikatora strefa zostanie zablokowana lub przywrócona zostanie kontrola w zablokowanej strefie. Jeżeli drzwi są otwarte, po użyciu identyfikatora strefa zostanie odblokowana lub przywrócona zostanie kontrola w odblokowanej strefie.*

*Konfiguracja opcji blokowania opisana w niniejszym rozdziale jest możliwa w przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej. W przypadku centrali z niższą wersją oprogramowania, blokowanie przejść i stref oraz przywracanie ich kontroli będzie możliwe na takich zasadach, jakie obowiązywały w poprzedniej wersji systemu.*

*W przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej, po aktualizacji systemu ACCO NET do wersji 1.6, dotychczasowe ustawienia opcji sterowania strefami zostaną odwzorowane w nowym systemie. Jeżeli opcja „Zablokuj strefę po przytrzymaniu karty” była dotychczas włączona, po aktualizacji systemu, dla*

wszystkich terminali pełniących funkcję wejścia w tej strefie zostanie włączona opcja „Steruje strefą”.

Strefę można blokować lub przywracać w niej kontrolę przy pomocy:

- kodu,
- karty,
- karty (przytrzymanie),
- kodu lub karty,
- karty (zbliżenie lub przytrzymanie),
- kodu lub karty (przytrzymanie),
- kodu lub karty (zbliżenie lub przytrzymanie).

**Steruje strefą** – po włączeniu opcji, możesz blokować strefę i przywracać w niej kontrolę przy pomocy terminala pełniącego funkcję wejścia do tej strefy. W przypadku integracji zablokowanie strefy systemu kontroli dostępu przy użyciu terminala wejściowego będzie skutkowało załączeniem czuwania w zintegrowanej strefie systemu alarmowego.

**Otwórz drzwi po zakończeniu blok.** – jeżeli opcja jest włączona i użytkownik przywróci kontrolę przejścia lub strefy (przy włączonej opcji „Steruje strefą”), uzyska dostęp do przejścia.



– **zasady blokowania strefy obowiązujące przez całą dobę**



Jeżeli nie zdefiniujesz zasad dotyczących blokowania strefy obowiązujących przez całą dobę, strefy będzie można blokować na zasadach obowiązujących w czasie określonym przez wybrany kalendarz dostępu.



– zasady blokowania strefy przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik zablokuje strefę przy pomocy pierwszego identyfikatora).



– **zasady przywracania kontroli w zablokowanej strefie obowiązujące przez całą dobę**



Jeżeli nie zdefiniujesz zasad dotyczących przywracania kontroli w zablokowanej strefie obowiązujących przez całą dobę, kontrolę w strefie będzie można przywracać na zasadach obowiązujących w czasie określonym przez wybrany kalendarz dostępu.



– zasady przywracania kontroli w zablokowanej strefie przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik przywróci kontrolę w zablokowanej strefie przy pomocy pierwszego identyfikatora).



– **zasady blokowania strefy w czasie określonym przez kalendarz dostępu**



Jeżeli nie zdefiniujesz zasad dotyczących blokowania stref obowiązujących w czasie określonym przez kalendarz dostępu, blokowanie stref będzie możliwe na zasadach obowiązujących przez całą dobę.



– kliknij na pole, jeśli w czasie określonym przez kalendarz dostępu strefa ma być blokowana na innych zasadach niż przez całą dobę. Wyświetlona zostanie lista utworzonych w aplikacji ACCO Web kalendarzy dostępu. Kliknij na jeden z nich.



– zasady blokowania strefy przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik zablokuje strefę przy pomocy pierwszego identyfikatora).



– **zasady przywracania kontroli w zablokowanej strefie w czasie określonym przez kalendarz dostępu**



*Jeżeli nie zdefiniujesz zasad dotyczących przywracania kontroli w zablokowanej strefie obowiązujących w czasie określonym przez wybrany kalendarz dostępu, kontrolę w strefie będzie można przywracać na zasadach obowiązujących przez całą dobę.*



– kliknij na pole, jeśli w czasie określonym przez kalendarz dostępu przywracanie kontroli w zablokowanej strefie ma się odbywać na innych zasadach niż przez całą dobę. Wyświetlona zostanie lista utworzonych w aplikacji ACCO Web kalendarzy dostępu. Kliknij na jeden z nich.



– zasady przywracania kontroli w zablokowanej strefie przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik, przywróci kontrolę w zablokowanej strefie przy pomocy pierwszego identyfikatora).

## **Opcje sterowania – Odblokowanie**



*Funkcje sterowania są poprawnie realizowane tylko wtedy, gdy jedno z wejść modułu kontroluje stan drzwi (zaprogramowane jest jako „Czujnik otwarcia drzwi”).*

*Jeżeli użytkownik ma sterować strefą, musi mieć dostęp do danej strefy oraz uprawnienie do przełączania jej stanu (włączone opcje „Uprawniony do dostępu” i „Przełączanie” w aplikacji ACCO Web (→„Użytkownicy” →„Lista” →[nazwa użytkownika] →zakładka „Strefy”)) oraz przypisany kalendarz dostępu.*

*Jeżeli sterowanie strefą ma się odbywać przy pomocy dwóch identyfikatorów:*

- po użyciu 1. identyfikatora, urządzenia pracujące w charakterze terminali poinformują o konieczności użycia 2. identyfikatora (manipulator LCD poprzez komunikat na wyświetlaczu, klawiatury oraz czytniki kart zbliżeniowych poprzez dodatkową sygnalizację dźwiękową – 3 krótkie dźwięki),
- użytkownik ma na wprowadzenie 2. identyfikatora 30 sekund.

*Należy zdefiniować identyfikatory służące zarówno do odblokowania strefy, jak i przywracania jej kontroli.*

*Jeżeli:*

- pierwsze identyfikatory służące do odblokowania strefy są takie same jak pierwsze identyfikatory służące do blokowania strefy i /lub
- pierwsze identyfikatory służące do przywracania kontroli w odblokowanej strefie są takie same jak pierwsze identyfikatory służące do przywracania kontroli w zablokowanej strefie,

*od stanu drzwi zależy, jak zmieni się stan strefy. Jeżeli drzwi są otwarte, po użyciu identyfikatora, strefa zostanie odblokowana lub przywrócona zostanie kontrola w odblokowanej strefie. Jeśli drzwi są zamknięte, po użyciu identyfikatora, strefa zostanie zablokowana lub przywrócona zostanie kontrola w zablokowanej strefie.*

*Konfiguracja opcji odblokowania opisana w niniejszym rozdziale jest możliwa w przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej. W przypadku centrali z niższą wersją oprogramowania, odblokowanie przejść i stref oraz przywracanie ich kontroli będzie możliwe na takich zasadach, jakie obowiązywały w poprzedniej wersji systemu.*

*W przypadku centrali ACCO-NT w wersji oprogramowania 1.14.xxx lub nowszej, po aktualizacji systemu ACCO NET do wersji 1.6, dotychczasowe ustawienia opcji sterowania strefami zostanie odwzorowana w nowym systemie. Jeżeli opcja „Zablokuj strefę po przytrzymaniu karty” była dotychczas włączona, po aktualizacji systemu, dla wszystkich terminali pełniących funkcję wejścia w tej strefie zostanie włączona opcja „Steruje strefą”.*

Strefę można odblokowywać lub przywracać w niej kontrolę przy pomocy:

- kodu,
- karty,
- karty (przytrzymanie),
- kodu lub karty,
- karty (zbliżenie lub przytrzymanie),
- kodu lub karty (przytrzymanie),
- kodu lub karty (zbliżenie lub przytrzymanie).

**Steruje strefą** – po włączeniu opcji, możesz odblokowywać strefę i przywracać w niej kontrolę przy pomocy terminala pełniącego funkcję wejścia do tej strefy.



### **– zasady odblokowania strefy obowiązujące przez całą dobę**



*Jeżeli nie zdefiniujesz zasad dotyczących odblokowania strefy obowiązujących przez całą dobę, strefy będzie można odblokować na zasadach obowiązujących w czasie określonym przez wybrany kalendarz dostępu.*



– zasady odblokowania strefy przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik odblokuje strefę przy pomocy pierwszego identyfikatora).



### **– zasady przywracania kontroli w odblokowanej strefie obowiązujące przez całą dobę**



*Jeżeli nie zdefiniujesz zasad dotyczących przywracania kontroli w odblokowanej strefie obowiązujących przez całą dobę, kontrolę w strefie będzie można przywracać na zasadach obowiązujących w czasie określonym przez wybrany kalendarz dostępu.*



– zasady przywracania kontroli w odblokowanej strefie przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik przywróci kontrolę w odblokowanej strefie przy pomocy pierwszego identyfikatora).



– **zasady odblokowania strefy w czasie określonym przez kalendarz dostępu**



Jeżeli nie zdefiniujesz zasad dotyczących odblokowania stref obowiązujących w czasie określonym przez kalendarz dostępu, strefę będzie można odblokować na zasadach obowiązujących przez całą dobę.



– kliknij na pole, jeśli w czasie określonym przez kalendarz dostępu strefa ma być odblokowywana na innych zasadach niż przez całą dobę. Wyświetlona zostanie lista utworzonych w aplikacji ACCO Web kalendarzy dostępu. Kliknij na jeden z nich.



– zasady odblokowania strefy przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik, odblokuje strefę przy pomocy pierwszego identyfikatora).



– **zasady przywracania kontroli w odblokowanej strefie w czasie określonym przez kalendarz dostępu**



Jeżeli nie zdefiniujesz zasad dotyczących przywracania kontroli w odblokowanej strefie obowiązujących w czasie określonym przez wybrany kalendarz dostępu, kontrolę w strefie będzie można przywracać na zasadach obowiązujących przez całą dobę.



– kliknij na pole, jeśli w czasie określonym przez kalendarz dostępu, przywracanie kontroli w odblokowanej strefie ma się odbywać na innych zasadach niż przez całą dobę. Wyświetlona zostanie lista utworzonych w aplikacji ACCO Web kalendarzy dostępu. Kliknij na jeden z nich.



– zasady przywracania kontroli w odblokowanej strefie przez użytkownika:

1. – pierwszy identyfikator,
2. – drugi identyfikator (jeżeli go nie wybierzesz, użytkownik, przywróci kontrolę w odblokowanej strefie przy pomocy pierwszego identyfikatora).

## **Przykłady**

### **Przykład definiowania opcji dostępu**

Wybrany kalendarz dostępu uprawnia użytkowników do dostępu od godziny 8:00 do 16:00. W tym czasie użytkownik uzyska dostęp przy pomocy dwóch identyfikatorów: 1. – kodu i 2. – karty. Drugi użytkownik potwierdzi dostęp również przy pomocy dwóch identyfikatorów: 1. – pilota i 2. – kodu lub karty. W pozostałych godzinach (do 8:00 i od 16:00, kiedy nie obowiązuje wybrany kalendarz) użytkownik uzyska dostęp przy pomocy dwóch identyfikatorów: 1. – karty i 2. – karty, a drugi użytkownik potwierdzi dostęp również przy pomocy dwóch identyfikatorów: 1. – kodu i 2. – karty lub pilota.

W godzinach między 8:00 a 16:00 użytkownik uzyska dostęp, jeżeli:

- wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”, po czym przyłoży do czytnika kartę,
- użytkownik uprawniony do potwierdzania użyje pilota, po czym wprowadzi kod i zatwierdzi go przyciskiem # lub „OK” lub przyłoży do czytnika kartę.

Natomiast w godzinach od 16:00 do 8:00, użytkownik uzyska dostęp jeśli:

- przyłoży do czytnika kolejno karty,



- użytkownik uprawniony do potwierdzania wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”, po czym przyłoży do czytnika kartę lub użyje pilota.

### **Przykład definiowania opcji blokowania strefy i przywracania kontroli w zablokowanej strefie**

Wybrany kalendarz dostępu uprawnia użytkowników do sterowania strefą w godzinach między 6:00 a 18:00. W tym czasie użytkownik zablokuje strefę przy pomocy dwóch identyfikatorów: 1. – kodu i 2. – karty, a przywróci kontrolę w zablokowanej strefie przy pomocy: 1. – karty i 2. – kodu lub karty. W pozostałych godzinach (do 6:00 i od 18:00, kiedy nie obowiązuje wybrany kalendarz) zablokuje strefę przy pomocy dwóch identyfikatorów: 1. – karty (przytrzymanie) i 2. – kodu, a przywróci kontrolę w zablokowanej strefie przy pomocy: 1. – karty.

W godzinach między 6:00 a 18:00 użytkownik zablokuje strefę, jeżeli wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”, po czym przyłoży do czytnika kartę. Kontrolę w zablokowanej strefie przywróci, jeśli przyłoży do czytnika kartę, po czym wprowadzi kod i zatwierdzi go przyciskiem # lub „OK” lub przyłoży do czytnika kartę.

Natomiast w godzinach od 18:00 do 6:00, użytkownik zablokuje strefę, jeżeli przez około 3 sekundy przytrzyma przy czytniku kartę, po czym wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”. Kontrolę w zablokowanej strefie przywróci, jeśli przyłoży do czytnika kartę.

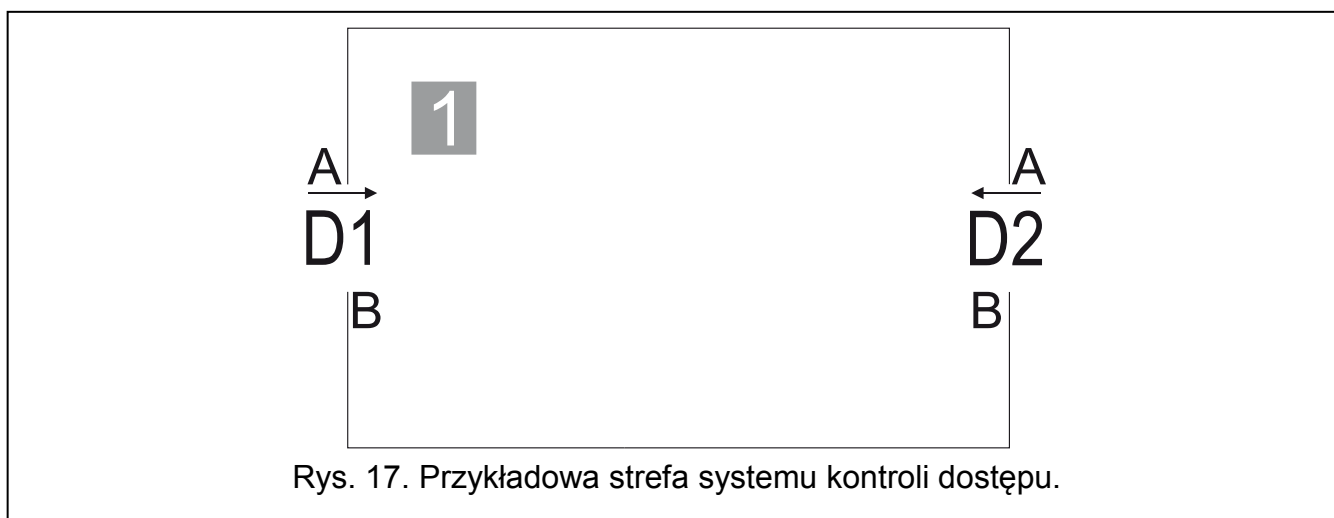
### **Przykład definiowania opcji odblokowania strefy i przywracania kontroli w odblokowanej strefie**

Wybrany kalendarz dostępu uprawnia użytkowników do sterowania strefą w godzinach między 10:00 a 14:00. W tym czasie użytkownik odblokuje strefę przy pomocy jednego identyfikatora: 1. – karty, a przywróci kontrolę w odblokowanej strefie przy pomocy: 1. – kodu. W pozostałych godzinach (do 10:00 i od 14:00, kiedy nie obowiązuje wybrany kalendarz) odblokuje strefę przy pomocy jednego identyfikatora: 1. – kodu, a przywróci kontrolę w odblokowanej strefie przy pomocy: 1. – karty (przytrzymanie).

W godzinach między 10:00 a 14:00 użytkownik odblokuje strefę, jeżeli przyłoży do czytnika kartę. Kontrolę w odblokowanej strefie przywróci, jeśli wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”.

Natomiast w godzinach od 14:00 do 10:00, użytkownik odblokuje strefę, jeżeli wprowadzi kod i zatwierdzi go przyciskiem # lub „OK”. Kontrolę w odblokowanej strefie przywróci, jeśli przez około 3 sekundy przytrzyma przy czytniku kartę.

### **Przykład sterowania strefą z dwoma przejściami**



Rys. 17. Przykładowa strefa systemu kontroli dostępu.

Objaśnienia do rysunku 17:

1 (numer na szarym tle) – strefa systemu kontroli dostępu.

D1 – kontroler przypisany do strefy 1. Terminal A to wejście do strefy 1, natomiast terminal B to wyjście ze strefy 1.

D2 – kontroler przypisany do strefy 1. Terminal A to wejście do strefy 1, natomiast terminal B to wyjście ze strefy 1.

### BLOKOWANIE STREFY

Gdy chcesz zablokować strefę 1:

- jeżeli w strefie jest terminal wejściowy, dla którego włączona jest opcja „Steruje strefą”, użyj tego terminala.

**i** Jeżeli zablokujesz w ten sposób strefę kontroli dostępu zintegrowaną ze strefą systemu alarmowego, załączysz czuwanie w strefie systemu alarmowego.

- jeżeli w strefie nie ma terminala wejściowego, dla którego włączona jest opcja „Steruje strefą”, zablokuj wszystkie przejścia.

### ODBLOKOWANIE STREFY

Gdy chcesz odblokować strefę 1:

- jeżeli w strefie jest terminal wejściowy, dla którego włączona jest opcja „Steruje strefą”, użyj tego terminala.
- jeżeli w strefie nie ma terminala wejściowego, dla którego włączona jest opcja „Steruje strefą”, odblokuj wszystkie przejścia.

**i** Gdy strefa jest zintegrowana ze strefą systemu alarmowego i załączone jest w niej czuwanie, przy pomocy terminali nie można odblokować ani strefy, ani przejść.

### PRZYWRÓCENIE KONTROLI W STREFIE

Gdy chcesz przywrócić kontrolę w zablokowanej lub odblokowanej strefie 1:

- jeżeli w strefie jest terminal wejściowy, dla którego włączona jest opcja „Steruje strefą”, użyj tego terminala.
- jeżeli w strefie nie ma terminala wejściowego, dla którego włączona jest opcja „Steruje strefą”, przywróć kontrolę wszystkim przejściom.

### Zakładka „Manipulatory LCD”

Adres	Nazwa	Status	Drzwi
1	Recepcja	!	🚪
2	Magazyn	✓	🚪
3	Pracownia	!	🚪

Rys. 18. Zakładka „Manipulatory LCD”.

**Przejście służbowe** – gdy opcja zostanie włączona, po przyznaniu dostępu wyświetli się komunikat „Przejście służbowe”. Jeżeli wejście / wyjście ma charakter służbowy, użytkownik powinien nacisnąć klawisz ▲. Dopóki go nie naciśnie albo nie otworzy przejścia, komunikat będzie widoczny na wyświetlaczu manipulatora. W szczegółach zdarzenia zostanie wówczas dopisana odpowiednia informacja. Jest ona przydatna, jeśli rejestrowane przez moduł przejścia użytkowników mają być pomocne dla określania czasu ich pracy.



*Funkcja nie jest realizowana, jeżeli nie jest kontrolowany stan drzwi lub drzwi są otwarte.*

**Pokaż nazwę użytkownika na manipulatorze** – po włączeniu opcji na wyświetlaczu manipulatora LCD, przy pomocy którego otwarte zostało przejście, wyświetlana będzie nazwa użytkownika, który otworzył przejście.

**Pokaż nazwę użytkownika na obu manipulatorach** – po włączeniu opcji na wyświetlaczach obu manipulatorów LCD, podłączonych do kontrolera, wyświetlana będzie nazwa użytkownika, który otworzył to przejście. Włączenie opcji włącza jednocześnie opcję „Pokaż nazwę użytkownika na manipulatorze”.

**Format czasu na LCD** – funkcja pozwala na wybór sposobu wyświetlania czasu i daty na wyświetlaczu manipulatora.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



– kliknij, żeby zatwierdzić wprowadzone zmiany.

## **Zakładka „Wejścia”**

**Numer** – numer wejścia kontrolera.

**Typ reakcji:**

**Czujnik otwarcia drzwi** – kontrola stanu drzwi.



*Kontrola stanu drzwi, czyli podłączenie czujnika do wejścia zaprogramowanego jako „Czujnik otwarcia drzwi”, jest niezbędna, aby poprawnie realizować wszystkie funkcje kontroli dostępu.*

**Przycisk otwarcia** – otwarcie przejścia.

**Odblokowanie przejścia** – trwałe otwarcie przejścia. Przejście pozostanie otwarte tak długo, jak długo wejście będzie aktywne (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Zablokowanie przejścia** – trwałe zamknięcie przejścia. Przejście pozostanie zamknięte tak długo, jak długo wejście będzie aktywne (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Czujnik śluzy** – kontrola stanu pozostałych drzwi tworzących śluzę. W konfiguracji śluzy mogą być otwarte tylko 1 drzwi.

**Pożar – odblokowanie przejścia** – trwałe otwarcie przejścia na wypadek pożaru. Przejście pozostanie otwarte do czasu, gdy wejście wróci do stanu normalnego. Przejście może przełączyć użytkownik posiadający uprawnienie „Przełączanie”.

**Alarm – zablokowanie przejścia** – trwałe zamknięcie przejścia na wypadek alarmu. Przejście pozostanie zamknięte do czasu zmiany jego stanu przy pomocy kodu lub dłuższego przytrzymania karty przez użytkownika posiadającego uprawnienie „Przełączanie”. Czas, przez który wejście będzie aktywne, nie ma wpływu na czas zablokowania przejścia.

**Sygnal dzwonka** – uruchomienie wyjścia typu „Sygnal dzwonka”.

**Informacja 1÷4** – generowanie zaprogramowanego wcześniej zdarzenia. Jego treść możesz zdefiniować w tabeli poniżej.



*Zdarzenia zaprogramowane dla typu reakcji „Informacja 1÷4” nie są globalne. Należy je zdefiniować dla każdego kontrolera oddzielnie.*

Ustawienia centrali				Kontrolery	Strefy	Integracja	Ekspandery	Wejścia	Wyjścia	Ścieżki przejść	Status	
Liczba kontrolerów:				3								
Adres	Nazwa	Status	Drzwi									
1	Recepcja	!	🔒									
2	Pracownia	✓	🔒									
3	Magazyn	!	🔒									
Opcje				Ustawienia terminali	Wejścia	Wyjścia	Przejście	Status				
Numer	Typ reakcji	Typ	Czułość [ms]									
1	Czujnik otwarcia drzwi	NO	50									
2	Przycisk otwarcia	NO	50									
3	Odblokowanie przejścia	NO	50									
4	dzwonek	NO	50									
5	obchód wartownika	NO	50									
Typ reakcji	Treść											
Informacja 1	dzwonek											
Informacja 2	obchód wartownika											
Informacja 3												
Informacja 4												

Rys. 19. Zakładka „Wejścia”.

**Typ** – możesz wybrać:

**NO** – wejście obsługuje urządzenie posiadające wyjście typu NO (normalnie otwarte),

**NC** – wejście obsługuje urządzenie posiadające wyjście typu NC (normalnie zamknięte).

**Czułość [ms]** – czas, przez który stan wejścia musi być zmieniony, aby zostało to zarejestrowane. Czas ten można programować w zakresie od 10 ms do 2,55 s.

### Zakładka „Wyjścia”

**Status drzwi** – informuje o aktualnym stanie drzwi. Uaktywnia się wraz z otwarciem drzwi i pozostaje aktywne do czasu ich zamknięcia. Wyjście skonfigurowane jako „Status drzwi” nie może realizować innych funkcji.

**Otwarcie drzwi** – uruchamia się na zaprogramowany czas po otwarciu drzwi. Dla wyjścia skonfigurowanego jako „Otwarcie drzwi” można dodatkowo włączyć tylko funkcję „Sygnał dzwonka”.

**Sygnał dzwonka** – uruchamia się na zaprogramowany czas po podaniu sygnału na wejście zaprogramowane jako „Sygnał dzwonka”. Dla wyjścia skonfigurowanego jako „Sygnał dzwonka” można dodatkowo włączyć tylko funkcję „Otwarcie drzwi”.

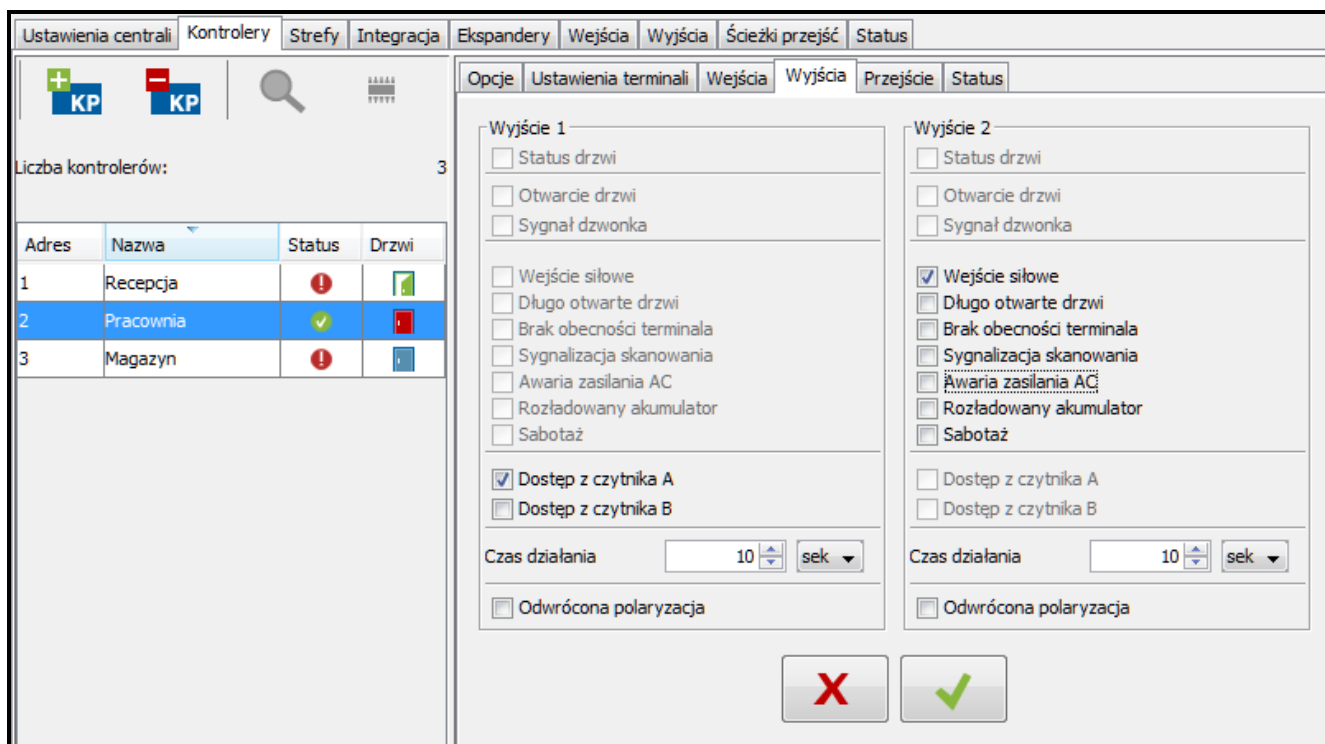
**Wejście siłowe** – uruchamia się na zaprogramowany czas po otwarciu drzwi bez udzielenia dostępu (przejście jest zamknięte).

**Długo otwarte drzwi** – uruchamia się na zaprogramowany czas, jeżeli drzwi pozostają otwarte po upływie „Maksymalnego czasu otwarcia drzwi”.

**Brak obecności terminala** – uruchamia się na zaprogramowany czas, jeżeli w czasie testu stwierdzono brak terminala (manipulatora LCD, klawiatury lub czytnika kart zbliżeniowych). Moduł kontroluje obecność terminali tylko wówczas, gdy włączone są odpowiednie opcje („Kontroluj obecność terminala A / B”).

**Sygnalizacja skanowania** – uruchamia się na zaprogramowany czas, jeżeli miało miejsce 5 prób odczytu niezarejestrowanej karty zbliżeniowej, niezarejestrowanej pastylki lub wpisania nieznanego kodu. Wyjście jest uaktywniane niezależnie od tego, czy włączona jest opcja „Anty-Skaner”.

**Awaria zasilania AC** – uaktywnia się, jeżeli od utraty zasilania AC przez moduł ACCO-KP-PS / ACCO-KPWG-PS upłynął czas zaprogramowany jako „Czas braku zasilania AC”, a zasilanie nie zostało przywrócone. Wyjście pozostaje aktywne do czasu przywrócenia zasilania AC.



Rys. 20. Zakładka „Wyjścia”.

**Rozładowany akumulator** – uaktywnia się, jeżeli napięcie akumulatora podłączonego do modułu ACCO-KP-PS / ACCO-KPWG-PS spadnie poniżej 11 V na czas dłuższy niż 12 minut (3 testy akumulatora). Wyjście pozostaje aktywne do chwili, gdy napięcie akumulatora wzrośnie powyżej 11 V na czas dłuższy niż 12 minut (3 testy akumulatora).



Aby wyjście mogło poprawnie realizować funkcje typu „Status drzwi”, „Otwarcie drzwi”, „Wejście siłowe” i „Długo otwarte drzwi”, jedno z wejść kontrolera musi kontrolować stan drzwi („Czujnik otwarcia drzwi”).

**Sabotaż** – uaktywnia się, jeżeli zostanie naruszone wejście ITMP. Funkcja niedostępna, jeżeli włączona jest jedna z funkcji: „Status drzwi”, „Otwarcie drzwi”, „Sygnał dzwonka” lub „Dostęp z czytnika A / B”.

**Dostęp z czytnika A / B** – uaktywnia się, jeżeli uprawniony do tego użytkownik uzyska dostęp do przejścia przy pomocy czytnika A / B.

**Czas działania** – jeżeli wyjście ma być włączone na czas, to należy go zdefiniować. Po jego upływie, wyjście się wyłączy. Można zaprogramować wartości w zakresie 1-120 sekund albo 1-120 minut.

**Odwrócona polaryzacja** – jeżeli opcja jest włączona, odwrócona jest logika działania wyjścia tzn. w stanie aktywnym wyjście jest odcinane od masy.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



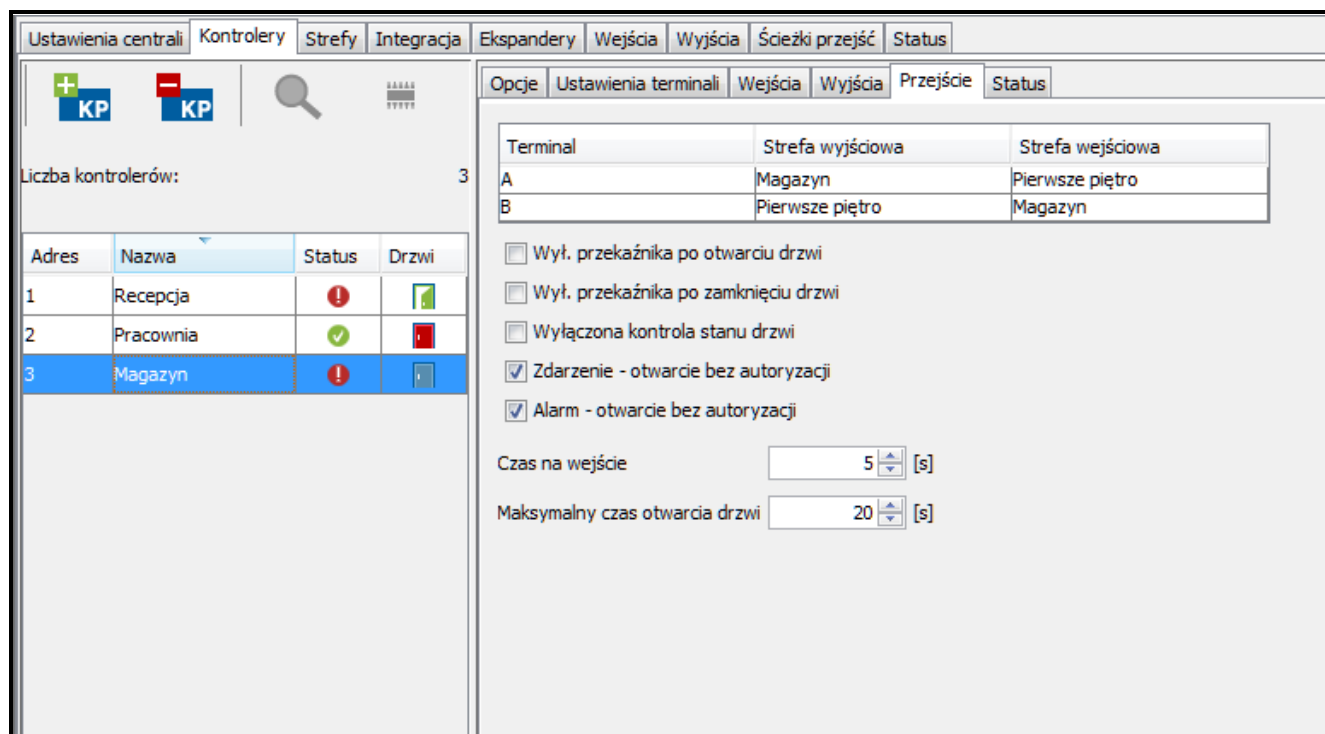
– kliknij, żeby zatwierdzić wprowadzone zmiany.

### **Zakładka „Przejście”**

**Terminale** – w formie tabeli wyświetlane są informacje mówiące o tym, jaka strefa wyjściowa / wejściowa została przypisana do terminala A / B modułu.

**Wył. przekaźnika po otwarciu drzwi** – jeśli opcja jest włączona, przekaźnik sterujący pracą urządzenia aktywującego przejście wyłączy się po otwarciu drzwi.

**Wył. przekaźnika po zamknięciu drzwi** – jeśli opcja jest włączona, przekaźnik sterujący pracą urządzenia aktywującego przejście wyłączy się po zamknięciu otwartych drzwi.



Rys. 21. Zakładka „Przejście” dla wybranego kontrolera.



Jeżeli żadna z opcji określających moment wyłączenia przekaźnika nie zostanie włączona, przekaźnik zostanie wyłączony po upływie „Czasu na wejście”.

W następujących przypadkach przekaźnik jest wyłączany po upływie „Czasu na wejście”, pomimo włączenia jednej z opcji określających moment wyłączenia przekaźnika:

- żadne z wejść nie informuje o stanie drzwi (nie został zainstalowany czujnik kontrolujący stan drzwi),
- włączona została opcja „Wyłączona kontrola stanu drzwi”,
- użytkownik uzyskał dostęp, ale nie otworzył drzwi.

**Wyłączona kontrola stanu drzwi** – włączenie tej opcji jest zalecane, jeśli do modułu nie docierają informacje o stanie drzwi (czujnik kontrolujący stan uległ awarii lub z jakiegoś powodu nie został podłączony). Zapobiega to generowaniu niewłaściwych zdarzeń. Gdy opcja jest włączona:

- uzyskanie dostępu traktowane jest jako równoznaczne otwarciu drzwi (zostanie wygenerowane zdarzenie informujące o przejściu bez kontroli stanu drzwi),
- część zdarzeń nie jest generowana (np. zdarzenia informujące o siłowym otwarciu drzwi, o długo otwartych drzwiach itd.),
- nie działa opcja „Przejście służbowe”.



Opcję „Wyłączona kontrola stanu drzwi” należy włączać w sytuacjach wyjątkowych, ponieważ poważnie ogranicza ona funkcjonalność kontroli dostępu.

**Zdarzenie – otwarcie bez autoryzacji** – jeżeli opcja jest włączona, w przypadku otwarcia drzwi bez autoryzacji zostanie wygenerowane zdarzenie o treści „Wejście siłowe”.

**Alarm – otwarcie bez autoryzacji** – jeżeli opcja jest włączona, w przypadku otwarcia drzwi bez autoryzacji zostanie wygenerowany alarm oraz zdarzenie o treści „Wejście siłowe”.

**Czas na wejście** – czas, na który przełącznik jest włączany po uzyskaniu dostępu, umożliwiając otwarcie drzwi. Może być programowany w zakresie od 1 do 60 sekund.

**Maksymalny czas otwarcia drzwi** – czas, przez który drzwi mogą pozostawać otwarte po wyłączeniu przełącznika. Jeśli drzwi pozostaną otwarte ponad przewidziany czas, zostanie wygenerowane odpowiednie zdarzenie. Ponadto uaktywni się wyjście zaprogramowane jako „Długo otwarte drzwi”. Czas może być programowany w zakresie od 1 do 60 sekund.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



– kliknij, żeby zatwierdzić wprowadzone zmiany.

## Zakładka „Status”



*W przypadku, gdy pomiędzy centralą a kontrolerem nie będzie komunikacji, wyświetli się informacja o braku komunikacji pomiędzy urządzeniami, a także data i godzina ostatniej transmisji odebranej przez centralę od kontrolera.*

**Stan przejścia** – aktualny stan przejścia:

- Przejście kontrolowane,
- Przejście zablokowane,
- Przejście odblokowane,
- Nieznany (brak komunikacji z kontrolerem).

**Zasilanie** – aktualna wartość napięcia zasilania kontrolera.

**Wersja oprogramowania** – wersja oprogramowania kontrolera (numer wersji i data kompilacji).

**Jakość komunikacji** – aktualny procentowy stosunek liczby wysłanych danych (z centrali do modułu) do liczby odebranych danych (z modułu do centrali).

Rys. 22. Zakładka „Status”.

**Typ modułu** – rodzaj kontrolera.

**Alarmy** – przy pomocy ikon prezentowane są statusy: „Sabotaż modułu”, „Sabotaż terminala A / B”, „Próba skanowania”, „Wejście siłowe” i „Długo otwarte drzwi”.

**Awarye** – przy pomocy ikon prezentowane są statusy: „Awaria zegara” i „Brak obecności terminala A / B”.

**Awarye zasilania** – przy pomocy ikon prezentowane są statusy: „Brak akumulatora”, „Rożładowany akumulator” i „Brak zasilania AC”.

**Wyjątkowe sytuacje** – przy pomocy ikon prezentowane są statusy: „Pożar” i „Alarm”.

Poszczególne ikony symbolizują następujący stan:



– brak alarmu / awarii (szare tło).



– alarm / awaria (biały wykrzyknik na czerwonym tle).



– potwierdzony alarm / awaria (biały wykrzyknik na czerwonym tle i biały symbol na zielonym tle).



– pamięć alarmu / awarii (biały wykrzyknik na szarym tle).



– pamięć potwierdzonego alarmu / awarii (biały wykrzyknik na szarym tle i biały symbol na zielonym tle).



– brak informacji o stanie (biały znak zapytania na szarym tle).



*Istnieje możliwość potwierdzania awarii, alarmów oraz wyjątkowych sytuacji. Jeśli chcesz potwierdzić awarię / alarm, kliknij na znajdujący się przy niej przycisk.*

**Przełącznik i drzwi** – przy pomocy ikon prezentowane są statusy: „Przełącznik aktywny” i „Otwarte drzwi”.

**Stan wejść, wyjść** – przy pomocy ikon prezentowany jest stan wejść i wyjść.

Poszczególne ikony oznaczają:



– przełącznik aktywny / otwarte drzwi / aktywne wejście / aktywne wyjście (zielone tło z niebieską obwódką).




– przełącznik nieaktywny / zamknięte drzwi / nieaktywne wejście / nieaktywne wyjście (szare tło).



– stan nieznan (biały znak zapytania na szarym tle).

#### 4.2.4.6 Zdalna aktualizacja oprogramowania kontrolera

1. Jeżeli chcesz zaktualizować oprogramowanie modułu / modułów kontroli dostępu, zaznacz wybrany moduł lub moduły w tabeli z listą kontrolerów.

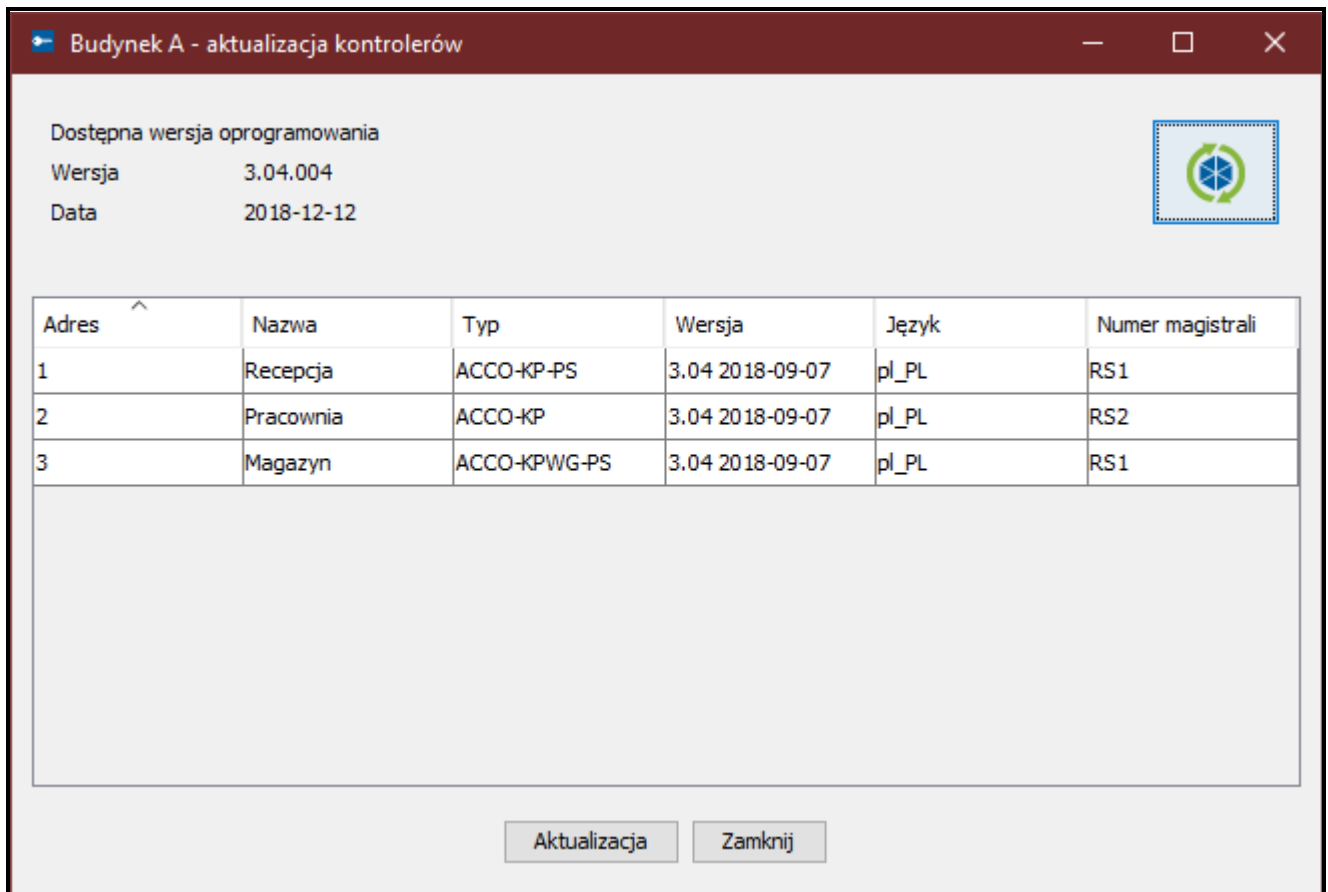
2. Kliknij na przycisk .

3. W oknie, które się otworzy, wyświetlone zostaną dane aktualnej wersji oprogramowania wszystkich zaznaczonych urządzeń, a także informacje dotyczące nowej dostępnej wersji (patrz: rys. 23).

4. Kliknij na przycisk „Aktualizacja”.

5. Otworzy się okno z informacjami dotyczącymi kontrolerów, których oprogramowanie zostanie zaktualizowane. Kliknij na przycisk „OK”.





Rys. 23. Okno umożliwiające aktualizację oprogramowania kontrolerów.

#### 6. Rozpocznie się proces aktualizacji oprogramowania.



*Podczas zdalnej aktualizacji oprogramowania modułu kontroli dostępu, pozostałe moduły podłączone do centrali pracują w trybie autonomicznym (opis zamieszczono w instrukcji do centrali kontroli dostępu ACCO-NT).*


*W przypadku jakichkolwiek problemów wyświetlony zostanie informujący o tym komunikat. Konieczne będzie ponowne uruchomienie aktualizacji.*

#### 7. Gdy aktualizacja zostanie zakończona, wyświetli się odpowiedni komunikat. Kliknij na „OK”, a następnie na „Zamknij”.

#### 4.2.4.7 Usunięcie kontrolera

1. Jeżeli chcesz usunąć pojedynczy kontroler, zaznacz kursorem wybrany kontroler w tabeli z listą kontrolerów.
2. Jeśli chcesz usunąć za jednym razem kilka kontrolerów, zaznacz kursorem jeden z kontrolerów i trzymając wciśnięty klawisz Ctrl wybierz kolejne zaznaczając je lewym przyciskiem myszki.
3. W przypadku, gdy chcesz usunąć wszystkie kontrolery jednocześnie, zaznacz kursorem jeden z kontrolerów i naciśnij jednocześnie klawisze Ctrl+A.



4. Kliknij wskaźnikiem myszki na przycisk .
5. Gdy wyświetli się pytanie, czy usunąć kontroler, kliknij „Tak”.
6. Zapisz wprowadzone zmiany.

## 4.2.5 Strefy

Strefa to wydzielony obszar w chronionym obiekcie. Podział na strefy ułatwia Administratorowi zarządzanie systemem kontroli dostępu.

### Opis przycisków



- kliknij, żeby dodać strefę.



- kliknij, żeby usunąć zaznaczoną wcześniej strefę (patrz: rozdział „Usunięcie strefy”).

Pod przyciskami wyświetlana jest liczba stref.

### 4.2.5.1 Utworzenie strefy

1. Zaznacz centralę na liście obiektów i central.

2. Kliknij na przycisk . Nowa strefa pojawi się w tabeli.

### 4.2.5.2 Tabela z listą stref

Lp. – numer porządkowy strefy.

**Strefa** – indywidualna nazwa strefy (do 32 znaków). Nazwy stref mogą być prezentowane w następujących kolorach:

**szary** – strefa, do której nie przypisano kontrolerów;

**czarny** – strefa z przypisanymi kontrolerami.

**Status** – informacja dotycząca aktualnego stanu strefy:

**Odczytywanie stanu,**

**Strefa kontrolowana,**

**Strefa odblokowana,**

**Strefa zablokowana,**

**Czuwa,**

**Czas na wejście** (czas, o jaki może zostać opóźniony alarm z wejścia centrali alarmowej, podczas którego można wyłączyć czuwanie w zintegrowanej strefie przed wywołaniem alarmu),

**Czas na wyjście < 10 s** (czas – wartość mniejsza niż 10 sekund, odliczany od momentu rozpoczęcia procedury załączenia czuwania w zintegrowanej strefie, pozwalający na opuszczenie chronionego obszaru bez wywołania alarmu),

**Czas na wyjście > 10 s** (czas – wartość większa niż 10 sekund, odliczany od momentu rozpoczęcia procedury załączenia czuwania w zintegrowanej strefie, pozwalający na opuszczenie chronionego obszaru bez wywołania alarmu),

**Mieszany** (przejścia nadzorowane przez kontrolery przypisane do strefy znajdują się w różnych stanach),

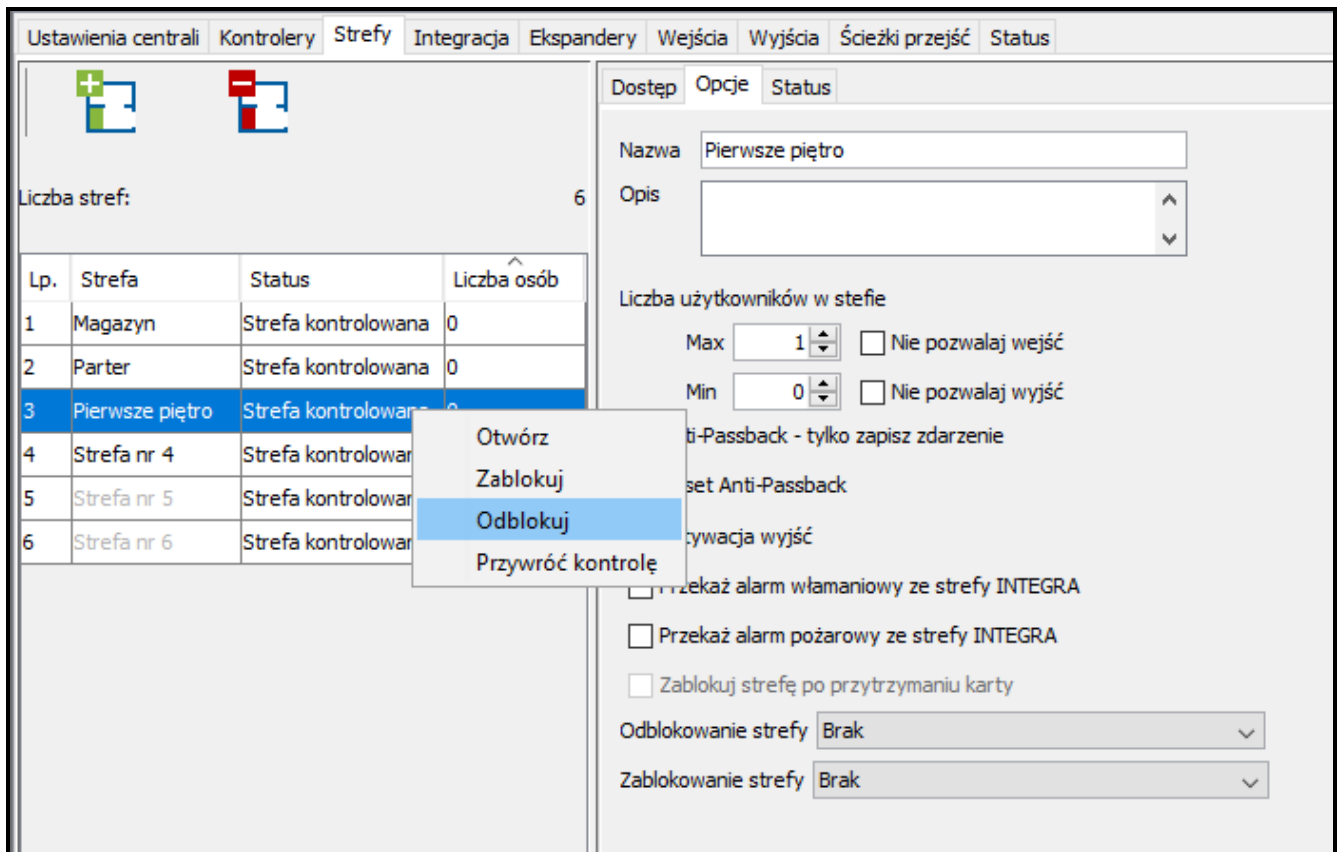
**Alarm w strefie,**

**Pożar w strefie,**

**Nieznany** (przed zapisaniem utworzonej strefy),

**Niedostępny** (nieodpowiednia wersja oprogramowania centrali ACCO-NT).

**Liczba osób** – liczba osób aktualnie przebywających w strefie.



Rys. 24. Lista stref w zakładce „Strefy”.

Po zaznaczeniu strefy na liście i kliknięciu na niej prawym przyciskiem myszki, wyświetli się rozwijane menu:

**Otwórz** – po wybraniu funkcji nastąpi otwarcie przejść nadzorowanych przez wszystkie kontrolery przypisane do wybranej strefy.

**Zablokuj** – po wybraniu funkcji nastąpi trwałe zamknięcie wszystkich przejść.

**Odblokuj** – po wybraniu funkcji nastąpi trwałe otwarcie wszystkich przejść.



*W przypadku, gdy dany moduł zostanie przypisany do kilku stref, zablokowanie lub odblokowanie jednej ze stref spowoduje – odpowiednio – zablokowanie lub odblokowanie modułu w pozostałych strefach, do których został przypisany.*

**Przywróć kontrolę** – po wybraniu funkcji zostanie przywrócona kontrola wszystkich przejść.

#### 4.2.5.3 Programowanie stref

Kliknij na wybraną strefę na liście stref, żeby ją zaprogramować. Parametry strefy wyświetlone zostaną w zakładkach „Dostęp” oraz „Opcje”.

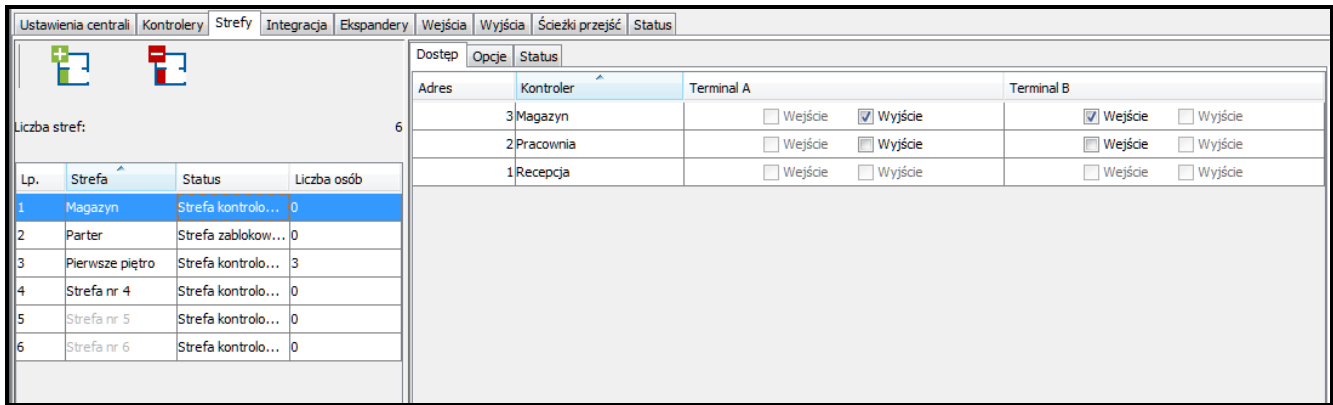
##### Parametry stref

##### **Zakładka „Dostęp”**

**Adres** – adres kontrolera.

**Kontroler** – nazwa kontrolera.

**Terminal A / B** – wskaź, który terminal (A lub B) w danym module będzie pełnił funkcję wejścia do strefy, a który wyjścia ze strefy.



Rys. 25. Zakładka „Dostęp”.

## Zakładka „Opcje”

**Nazwa** – indywidualna nazwa strefy (do 32 znaków).

**Opis** – w polu możesz dodatkowo opisać strefę.

### Liczba użytkowników w strefie

**Max** – pole pozwala określić maksymalną liczbę użytkowników, którzy jednocześnie mogą przebywać w strefie. Możesz zaprogramować wartości w zakresie od 1 do 8000. Liczbę można edytować klikając wskaźnikiem myszki na pole (można wpisać wartość przy pomocy klawiatury lub wybrać ją przy pomocy strzałek). W przypadku, gdy wartość minimalnej liczby osób w strefie będzie większa od maksymalnej, to wartość maksymalnej liczby osób w strefie automatycznie zostanie zwiększona o 1 od wartości minimalnej liczby osób w strefie.

**Nie pozwalaj wejść** – jeżeli opcja jest włączona, do strefy nie można uzyskać dostępu, gdy przebywa w niej maksymalna liczba użytkowników.



*Włączenie opcji „Nie pozwalaj wejść” dla strefy nie wpływa na sposób działania wyjścia o typie reakcji „Wskaźnik maks. liczby użytkowników” powiązanego z tą strefą.*

**Min** – pole pozwala określić minimalną liczbę użytkowników, którzy powinni przebywać w strefie. Możesz zaprogramować wartości w zakresie od 0 do 7999. Liczbę można edytować klikając wskaźnikiem myszki na pole (można wpisać wartość przy pomocy klawiatury lub wybrać ją przy pomocy strzałek). W przypadku, gdy wartość maksymalnej liczby osób w strefie będzie mniejsza od minimalnej, to wartość minimalnej liczby osób w strefie automatycznie zostanie zmniejszona o 1 od wartości maksymalnej liczby osób w strefie.

**Nie pozwalaj wyjść** – jeżeli opcja jest włączona, do strefy nie można uzyskać dostępu, gdy przebywa w niej minimalna liczba użytkowników.



*Włączenie opcji „Nie pozwalaj wyjść” dla strefy nie wpływa na sposób działania wyjścia o typie reakcji „Wskaźnik min. liczby użytkowników” powiązanego z tą strefą.*

**Anti-Passback – tylko zapisz zdarzenie** – po włączeniu opcji działanie funkcji Anti-Passback będzie ograniczone do rejestracji w pamięci zdarzeń przypadków wielokrotnego przejścia użytkownika w tym samym kierunku.

**Reset Anti-Passback** – po zaznaczeniu opcji stanie się aktywne pole „O godzinie [hh:mm]”, w którym można zdefiniować godzinę zresetowania funkcji „Anti-Passback”. Użytkownicy, których wyjście ze strefy nie zostało zarejestrowane, będą mogli po zaprogramowanej godzinie uzyskać dostęp do strefy.

**Aktywacja wyjść** – jeżeli opcja jest włączona, strefa może sterować wyjściami typu „Aktywacja dostępem”.

Ustawienia centrali Kontrolery Strefy Integracja Ekspandery Wejścia Wyjścia Ścieżki przejść Status

Dostęp Opcje Status

Nazwa: Magazyn

Opis:

Liczba użytkowników w strefie

Max: 1  Nie pozwalaj wejść

Min: 0  Nie pozwalaj wyjść

Anti-Passback - tylko zapisz zdarzenie

Reset Anti-Passback

O godzinie [hh:mm]: 00:30

Aktywacja wyjść

Przekaż alarm włamaniowy ze strefy INTEGRA

Przekaż alarm pożarowy ze strefy INTEGRA

Zablokuj strefę po przytrzymaniu karty

Odblokowanie strefy: Wg czasu

Początek [hh:mm]: 06:00

Koniec [hh:mm]: 18:00

Zablokowanie strefy: Wg kalendarza

Kalendarz: Ochrona Noc

Liczba stref: 6

Lp.	Strefa	Status	Liczba osób
1	Magazyn	Strefa kontrolowana	0
2	Parter	Strefa kontrolowana	0
3	Pierwsze piętro	Strefa kontrolowana	0
4	Strefa nr 4	Strefa kontrolowana	0
5	Strefa nr 5	Strefa kontrolowana	0
6	Strefa nr 6	Strefa kontrolowana	0

Rys. 26. Zakładka „Opcje”.

**Przekaż alarm włamaniowy ze strefy INTEGRA** – zaznacz opcję, jeśli alarm włamaniowy wygenerowany w zintegrowanej strefie systemu alarmowego, ma w strefie systemu ACCO NET trwale zamknąć przejścia na wypadek alarmu. Opcja dotyczy integracji systemu ACCO NET z systemem alarmowym (patrz: rozdział „Integracja”).

**Przekaż alarm pożarowy ze strefy INTEGRA** – zaznacz opcję, jeśli alarm pożarowy wygenerowany w zintegrowanej strefie systemu alarmowego, ma w strefie systemu ACCO NET trwale otworzyć przejścia na wypadek pożaru. Opcja dotyczy integracji systemu ACCO NET z systemem alarmowym (patrz: rozdział „Integracja”).

**Odblokowanie strefy** – można wybrać, czy strefa ma zostać odblokowana zgodnie ze zdefiniowanym czasem (określonym w polach „Początek [hh:mm]” oraz „Koniec [hh:mm]”), czy kalendarzem dostępu (kalendarz wybiera się z rozwijalnej listy w polu „Kalendarz”, jeśli został jakiś utworzony w aplikacji ACCO Web).

**Zablokowanie strefy** – można wybrać, czy strefa ma zostać zablokowana zgodnie ze zdefiniowanym czasem (określonym w polach „Początek [hh:mm]” oraz „Koniec [hh:mm]”), czy kalendarzem dostępu (kalendarz wybiera się z rozwijalnej listy w polu „Kalendarz”, jeśli został jakiś utworzony w aplikacji ACCO Web).

Po wprowadzeniu jakiegokolwiek zmiany wyświetlą się przyciski:



– kliknij, żeby anulować wprowadzone zmiany.



– kliknij, żeby zatwierdzić wprowadzone zmiany.

## Zakładka „Status”

W tabeli wyświetlają się aktualne stany kontrolerów przypisanych do strefy.

**Adres** – adres kontrolera.

**Nazwa** – indywidualna nazwa kontrolera.

**Status** – informacje o statusie kontrolera. Ikony symbolizujące stan urządzenia zostały opisane w rozdziale „Tabela z listą kontrolerów”.

**Drzwi** – informacje o stanie przejścia i drzwi nadzorowanych przez kontroler. Ikony symbolizujące stan przejścia i drzwi zostały opisane w rozdziale „Tabela z listą kontrolerów”.

Lp.	Strefa	Status	Liczba osób
1	Magazyn	Strefa kontrolo...	0
2	Parter	Strefa zablokow...	0
3	Pierwsze piętro	Strefa kontrolo...	3
4	Strefa nr 4	Strefa kontrolo...	0
5	Strefa nr 5	Strefa kontrolo...	0
6	Strefa nr 6	Strefa kontrolo...	0

Adres	Nazwa	Status	Drzwi
3	Magazyn	✓	✗
1	Recepcja	⚠	✓

Rys. 27. Zakładka „Status”.

### 4.2.5.4 Usunięcie strefy

1. Jeżeli chcesz usunąć pojedynczą strefę, zaznacz kursorem wybraną strefę w tabeli z listą stref.
2. Jeśli chcesz usunąć za jednym razem kilka stref, zaznacz kursorem jedną ze stref i trzymając wciśnięty klawisz Ctrl wybierz kolejne zaznaczając je lewym przyciskiem myszki.
3. W przypadku, gdy chcesz usunąć wszystkie strefy jednocześnie, zaznacz kursorem jedną ze stref i naciśnij jednocześnie klawisze Ctrl+A.

4. Kliknij wskaźnikiem myszki na przycisk .

5. Zapisz wprowadzone zmiany.



*Nie można usunąć strefy, do której zostały przypisane kontrolery.*

### 4.2.6 Integracja

Integracja systemu ACCO NET z systemami alarmowymi opartymi na centralach INTEGRA lub INTEGRA Plus (wersja oprogramowania 1.17 lub nowsza) jest realizowana przez sieć Ethernet. Do centrali alarmowej musi być podłączony moduł ETHM-1 Plus (wersja oprogramowania 2.03 lub nowsza) lub ETHM-1 (wersja oprogramowania 1.07 lub nowsza). Komunikacja odbywa się za pośrednictwem kanału komunikacyjnego GUARDX.



*ACCO NET używa do komunikacji z centralą alarmową tego samego portu co np. GUARDX, INTEGRA CONTROL lub INTEGRUM. Jeżeli system ACCO NET jest połączony z centralą alarmową, nie można nawiązać połączenia z centralą z innych programów za pośrednictwem tego samego modułu ethernetowego.*

Za połączenie oraz wymianę danych między systemami odpowiedzialny jest ACCO Serwer. Integracja umożliwia równoczesne sterowanie strefami systemu kontroli dostępu i strefami systemu alarmowego. W jednej centrali ACCO-NT można utworzyć 255 stref. Jedna centrala alarmowa umożliwia utworzenie maksymalnie 32 stref. Do jednej strefy systemu alarmowego może być przypisana jedna strefa systemu ACCO NET. Zintegrować można wszystkie lub tylko część stref, reszta stref systemu ACCO NET może być niezależna.

#### 4.2.6.1 Konfigurowanie systemu alarmowego

Informacje na temat konfigurowania centrali alarmowej i modułu ethernetowego znajdziesz w instrukcjach do tych urządzeń.

#### Ustawienia centrali alarmowej

W centrali alarmowej należy:

- zaprogramować identyfikator komunikacji między systemami „Identyfikator ACCO” (program DLOADX → „Komunikacja” → „Konfiguracja komunikacji”).



*Identyfikatory komunikacji w centrali oraz programach DLOADX i ACCO Soft (zakładka „Integracja” → wybrany system alarmowy → zakładka „Konfiguracja” → pole „Identyfikator ACCO”) muszą być identyczne.*

Poniżej zostały opisane przypadki, w których mogą zaistnieć pewne ograniczenia przy załączaniu czuwania w centrali alarmowej. Jeżeli:

- włączona jest opcja „Grade 2 / 3”:
  - w systemie alarmowym: czuwanie można załączyć tylko zgodnie z wymaganiami normy EN 50131 – odpowiednio dla Grade 2 / 3; w aplikacji ACCO Web będą widoczne dodatkowe informacje w zdarzeniach,
  - w systemie kontroli dostępu: strefę można zablokować zawsze,
- zdefiniowany jest czas dla opcji „Blokada na obchód wartownika” oraz użytkownik typu „Wartownik” posłużył się hasłem / identyfikatorem:
  - w systemie alarmowym: w strefie, w której jest załączone czuwanie, uruchamia się blokada czasowa strefy na zaprogramowany czas; w aplikacji ACCO Web będą widoczne dodatkowe informacje w zdarzeniach,
  - w systemie kontroli dostępu: strefa ma status „Czuwa”,
- użytkownik typu „Włącza blokadę czasową stref” posłużył się hasłem / identyfikatorem:
  - w systemie alarmowym: w strefie, w której jest załączone czuwanie, uruchamia się blokada czasowa strefy na czas zaprogramowany indywidualnie dla tego użytkownika; w aplikacji ACCO Web będą widoczne dodatkowe informacje w zdarzeniach,
  - w systemie kontroli dostępu: strefa ma status „Czuwa”,
- zdefiniowany jest typ strefy „Z blokadą na czas”, włączona jest opcja „Domyślny czas blokady”, zdefiniowany jest czas w polu „Domyślny czas blokady stref”:
  - w systemie alarmowym: po załączeniu czuwania, strefa jest blokowana na czas określony przez instalatora,
  - w systemie kontroli dostępu: strefę można zablokować; strefa centrali alarmowej jest blokowana automatycznie na czas określony przez instalatora, co widoczne jest tylko w programie DLOADX.
- zdefiniowany jest typ strefy „Z blokadą na czas”:
  - w systemie alarmowym: po załączeniu czuwania, strefa jest blokowana na czas podany przez użytkownika,
  - w systemie kontroli dostępu: strefę można zablokować; strefa centrali alarmowej nie jest blokowana czasowo,



*W systemie alarmowym w czasie blokady czuwanie może wyłączyć tylko użytkownik posiadający uprawnienie „Dostęp do stref zablokowanych czasowo”. W systemie kontroli dostępu użytkownik może przywrócić kontrolę w strefie przy pomocy terminala wejściowego, dla którego włączono opcję „Steruje strefą” tylko wtedy, gdy:*

- posiada uprawnienie „Przełączanie”,
- ma dostęp do danej strefy, zgodnie z przypisanym mu kalendarzem dostępu.

- zaprogramowane są globalne opcje dotyczące czuwania:
  - w systemie alarmowym: czuwanie można załączyć, jeżeli są spełnione warunki włączonej opcji / włączonych opcji – w zależności od stanu wejść, wyjść, istniejących awarii w systemie alarmowym,
  - w systemie kontroli dostępu: strefę można zablokować zawsze.

### **Ustawienia modułu ethernetowego (ETHM-1, ETHM-1 Plus)**

W module ethernetowym należy:

- włączyć opcje „GUARDX” i „GSM”, żeby możliwe było uzyskanie połączenia z systemem ACCO NET przez sieć TCP/IP;
- zaprogramować numer portu TCP, który będzie używany do komunikacji z systemem ACCO NET, jeżeli ma być inny niż 7091 (pole „Port”);
- zaprogramować klucz (ciąg do 12 znaków alfanumerycznych – cyfry, litery i znaki specjalne), jakim szyfrowane będą dane podczas komunikacji z systemem ACCO NET (pole „Klucz GUARDX/Java”).

#### **Opis przycisków**



- kliknij, żeby dodać system alarmowy.



- kliknij, żeby usunąć zaznaczony wcześniej system alarmowy (patrz: rozdział „Usunięcie systemu alarmowego”).


Przy przyciskach wyświetlana jest liczba w postaci x/y, gdzie x to liczba systemów alarmowych zintegrowanych dla centrali ACCO-NT, a y to maksymalna liczba systemów alarmowych, którą może obsługiwać centrala ACCO-NT (patrz: rozdział „Licencje”).

Kolory oznaczają:

- czarny – maksymalna liczba obsługiwanych systemów alarmowych dla danej centrali ACCO-NT nie została jeszcze przekroczona,
- czerwony – maksymalna liczba systemów alarmowych dla danej centrali ACCO-NT została przekroczona.

#### **4.2.6.2 Dodanie systemu alarmowego**

1. Zaznacz centralę na liście obiektów i central.

2. Kliknij na przycisk . Nowy system alarmowy pojawi się w tabeli.

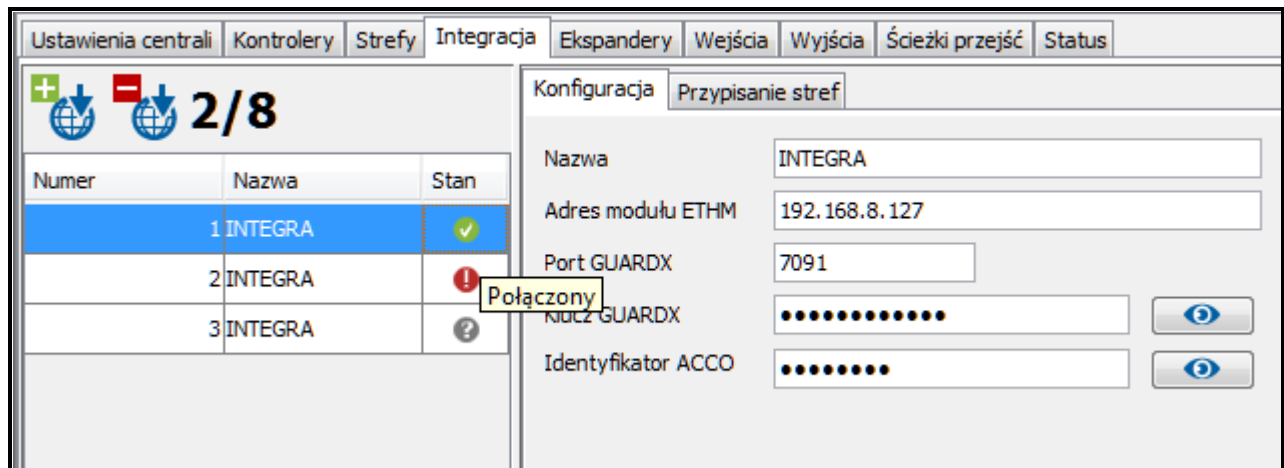
#### **4.2.6.3 Tabela z listą systemów alarmowych**

W tabeli prezentowana jest lista systemów alarmowych zintegrowanych z systemem ACCO NET.

**Numer** – numer porządkowy systemu alarmowego.

**Nazwa** – nazwa systemu alarmowego.





Rys. 28. Tabela z listą systemów w zakładce „Integracja”.

**Stan** – informacje o stanie komunikacji między systemami alarmowym a ACCO NET. Poszczególne ikony symbolizują:

- komunikacja nie działa poprawnie; po najechaniu kursorem na ikonę wyświetli się jego opis: „Zajęty”, „Brak połączenia”, „Niewłaściwy klucz GUARDX”, „Przekroczony limit central INTEGRA” lub „Niewłaściwa konfiguracja połączenia” (biały wykrzyknik na czerwonym tle),
- komunikacja między ACCO Server a modułem ethernetowym działa poprawnie; po najechaniu kursorem na ikonę wyświetli się „Połączony” (biały symbol na zielonym tle),
- dane nie zostały zapisane do bazy danych; po najechaniu kursorem na ikonę wyświetli się „Nieznany” (biały znak zapytania na szarym tle).

#### 4.2.6.4 Konfigurowanie ustawień dotyczących integracji

Kliknij na wybrany system alarmowy, żeby skonfigurować ustawienia dotyczące jego integracji z ACCO NET. Dane wyświetlone zostaną w zakładkach „Konfiguracja” oraz „Przypisanie stref”.

##### Zakładka „Konfiguracja”

**Nazwa** – nazwa systemu alarmowego w systemie ACCO NET.

**Adres modułu ETHM** – adres IP modułu ethernetowego podłączonego do centrali INTEGRA).

**Port GUARDX** – numer portu TCP używanego do komunikacji między ACCO NET a centralą alarmową.

**Klucz GUARDX** – ciąg do 12 znaków alfanumerycznych (cyfry, litery i znaki specjalne), który służy do szyfrowania danych podczas komunikacji między systemem ACCO NET a centralą. Kliknij , żeby zobaczyć ciąg znaków.

**Identyfikator ACCO** – identyfikator na potrzeby integracji systemu ACCO NET z centralą alarmową. Składa się z 8 cyfr. Kliknij , żeby zobaczyć ciąg znaków.

Po wprowadzeniu jakiegokolwiek zmiany wyświetlone zostaną przyciski:

- kliknij, żeby anulować wprowadzone zmiany.
- kliknij, żeby zatwierdzić wprowadzone zmiany.

Rys. 29. Zakładka „Konfiguracja”.

### **Zakładka „Przypisanie stref”**

**Pokaż wszystkie** – zaznacz opcję, jeśli w tabeli ze strefami mają być wyświetlane wszystkie strefy systemu alarmowego. Ich liczba zależy od typu centrali. Jeśli opcja jest wyłączona, w tabeli widoczne są tylko strefy utworzone w danym systemie, odczytane z pamięci centrali, automatycznie po nawiązaniu komunikacji pomiędzy systemami.

**Nr** – numer porządkowy.

**Strefa – INTEGRA** – nazwa strefy w systemie alarmowym.

**Strefa – ACCO** – nazwa strefy w systemie kontroli dostępu, która jest zintegrowana ze strefą systemu alarmowego.

#### **4.2.6.5 Przypisanie stref**


1. W kolumnie „Strefa – ACCO” kliknij prawym klawiszem myszki na pole odpowiadające strefie systemu alarmowego.
2. Gdy wyświetli się lista dostępnych stref systemu ACCO NET, kliknij na strefę, którą chcesz przypisać. Nazwa wybranej strefy wyświetli się w polu.
3. W ten sam sposób przypisz inne strefy systemu ACCO NET.
4. Zapisz wprowadzone zmiany.

Nr	Strefa - INTEGRA	Strefa - ACCO
1	Zewnętrzna	Magazyn
2	Wewnętrzna	Parter
3	Produkcja 1	Drugie piętro
4	Produkcja 2	
5	Produkcja 3	
6	Strefa 6	

Rys. 30. Zakładka „Przypisanie stref”.

#### **4.2.6.6 Usunięcie systemu alarmowego**

1. Zaznacz wybrany system w tabeli z listą systemów.

2. Kliknij na przycisk .

3. Zapisz wprowadzone zmiany.

## 4.2.7 Ekspandery

Ustawienia centrali			Kontrolery	Strefy	Integracja	Ekspandery	Wejścia	Wyjścia	Ścieżki przejść	Status
Adres	Typ	Nazwa								
0	INT-O	korytarz na parterze								
1	INT-PP	piwnica								
2	INT-RX-S	brama								
3	INT-ORS	magazyn								
4	---									
5	---									
6	---									
7	---									
8	---									
9	---									
10	---									
11	---									
12	---									
13	---									
14	---									
15	---									
16	---									
17	---									
18	---									
19	---									
20	---									

Nr	Typ reakcji	Nazwa	Typ	Czułość [ms]	Aktywacja kalendarzem	Aktywne
17	Zablokowanie strefy	Wejście 17	Brak	320	Ochrona Noc	<input checked="" type="checkbox"/>
18	Odblokowanie strefy	Wejście 18	Brak	320		<input checked="" type="checkbox"/>
19	Otwarcie przejścia	Wejście 19	Brak	320	Ochrona Noc	<input checked="" type="checkbox"/>
20	Otwarcie przejścia	Wejście 20	Brak	320		<input checked="" type="checkbox"/>
21	Alarmowe zablokowanie przejścia	Wejście 21	Brak	320		<input checked="" type="checkbox"/>
22	Sabotaż	Wejście 22	Brak	320	Ochrona Noc	<input checked="" type="checkbox"/>
23	Niewykorzystane					<input type="checkbox"/>
24	Niewykorzystane					<input type="checkbox"/>

Typ wyjścia	Nazwa	Tryb działania	Czas działania	w min/sek	Polaryzacja	Negacja	Aktywne	
17	Wskaźnik odblokowania przejść	Wyjście 17	Wskaźnik	10	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
18	Wskaźnik alarmowego zablokowania przejść	Wyjście 18	Wskaźnik	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
19	Wskaźnik pożarowego odblokowania przejść	Wyjście 19	Wskaźnik	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
20	Wskaźnik kontroli przejść	Wyjście 20	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
21	Według kalendarza	Wyjście 21	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Niewykorzystane						<input type="checkbox"/>	<input type="checkbox"/>
23	Pilot	Wyjście 23	Przełączanie	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Status czuwania	Wyjście 24	Włączanie na czas (ignorowanie zdarzeń)	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Rys. 31. Zakładka „Ekspandery”.

### 4.2.7.1 Dodanie ekspandera

Dopiero po dodaniu ekspandera zgodnie z poniższą procedurą będzie on obsługiwany w systemie.

1. Kliknij na adres, który odpowiada adresowi ustawionemu w ekspanderze.
2. Kliknij prawym klawiszem myszki w kolumnie „Typ”. Wyświetlona zostanie lista typów ekspanderów.
3. Wybierz właściwy typ ekspandera.
4. W kolumnie „Nazwa” wprowadź nazwę ekspandera.
5. Zapisz wprowadzone zmiany.

### 4.2.7.2 Ustawienia ekspandera

**Adres** – adres ekspandera.

**Typ** – typ ekspandera. Do wyboru: INT-O, INT-E, INT-PP, INT-RX-S, INT-ORS oraz INT-IORS.

**Nazwa** – indywidualna nazwa ekspandera.

Po zaznaczeniu wybranego ekspandera, w przypadku ekspanderów wejść / wyjść / wejść i wyjść, obok listy ekspanderów wyświetli się jedna lub dwie tabele zawierające informacje dotyczące wejść / wyjść w zaznaczonym ekspanderze (opis wejść – patrz. str. 50; opis wyjść – patrz. str. 52).

### 4.2.7.3 Usunięcie ekspandera

1. W tabeli z listą ekspanderów wybierz moduł, który ma zostać usunięty.
2. W kolumnie „Typ”, po kliknięciu prawym klawiszem myszki, wybierz puste pole.
3. Zapisz wprowadzone zmiany.

## 4.2.8 Wejścia

System kontroli dostępu obsługuje wejścia:

- **przewodowe** – na płycie elektroniki centrali oraz w ekspanderach.
- **wirtualne** – wejścia, które nie istnieją fizycznie, ale które mogą zostać zaprogramowane jako „Według wyjścia”.

### 4.2.8.1 Numeracja wejść w systemie

Wejścia otrzymują numery w następujący sposób:

- wejścia przewodowe na płycie elektroniki centrali mają numery od 1 do 8.
- numery wejść w ekspanderach są uzależnione od adresu ekspandera w systemie (dla poszczególnych adresów ekspanderów numery wejść są zarezerwowane – np. dla ekspandera o adresie 0 wejścia będą miały numery od 9 do 16, dla ekspandera o adresie 1 wejścia będą miały numery od 17 do 24 itd.).

### 4.2.8.2 Programowanie wejść

Kliknij na zakładkę „Wejścia”. Zaznacz wejście, żeby je zaprogramować.

#### Przypisanie wejścia do strefy

1. Zaprogramuj dla wejścia któryś z typów reakcji: „Zablokowanie strefy”, „Odblokowanie strefy”, „Alarmowe zablokowanie strefy” lub „Pożarowe odblokowanie strefy”.
2. Po prawej stronie okna w części „Opcje reakcji” przypisz wejście do wybranej strefy albo do wszystkich stref.

#### Przypisanie wejścia do kontrolera

1. Zaprogramuj dla wejścia któryś z typów reakcji: „Otwarcie przejścia”, „Zablokowanie przejścia”, „Odblokowanie przejścia”, „Alarmowe zablokowanie przejścia” lub „Pożarowe odblokowanie przejścia”.
2. W oknie, które się wyświetli, wybierz kontroler, do którego chcesz przypisać wejście, i kliknij „OK”.

Nr	Typ reakcji	Nazwa	Typ	Czułość [ms]	Aktywacja kalendarzem	Aktywne
1	Bez reakcji	Wejście 1	Brak	320		<input checked="" type="checkbox"/>
2	Zablokowanie strefy	Wejście 2	NO	320	+576	<input checked="" type="checkbox"/>
3	Odblokowanie strefy	Wejście 3	NO	320		<input checked="" type="checkbox"/>
4	Alarmowe zablokowanie strefy	Wejście 4	NO	320		<input checked="" type="checkbox"/>
5	Pożarowe odblokowanie strefy	Wejście 5	NO	320		<input checked="" type="checkbox"/>
6	Otwarcie przejścia	Wejście 6	NO	320		<input checked="" type="checkbox"/>
7	Zablokowanie przejścia	Wejście 7	NO	320		<input checked="" type="checkbox"/>
8	Odblokowanie przejścia	Wejście 8	NO	320		<input checked="" type="checkbox"/>
9	Alarmowe zablokowanie przejścia	Wejście 9	NO	320		<input checked="" type="checkbox"/>
10	Pożarowe odblokowanie przejścia	Wejście 10	NO	320		<input checked="" type="checkbox"/>
11	Otwarcie przejścia	Wejście 11	NC	320		<input checked="" type="checkbox"/>
12	Zablokowanie strefy	Wejście 12	NO	320		<input checked="" type="checkbox"/>
13	Odblokowanie strefy	Wejście 13	NO	320		<input checked="" type="checkbox"/>
14	Zablokowanie przejścia	Wejście 14	NO	320		<input checked="" type="checkbox"/>
15	Odblokowanie przejścia	Wejście 15	NO	320		<input checked="" type="checkbox"/>
16	Otwarcie przejścia	Wejście 16	NO	320		<input checked="" type="checkbox"/>
17	Zablokowanie strefy	Wejście 17	NO	320	Ochrona Noc	<input checked="" type="checkbox"/>
18	Odblokowanie strefy	Wejście 18	NO	320		<input checked="" type="checkbox"/>
19	Otwarcie przejścia	Wejście 19	NO	320	Ochrona Noc	<input checked="" type="checkbox"/>
20	Otwarcie przejścia	Wejście 20	NO	320		<input checked="" type="checkbox"/>
21	Alarmowe zablokowanie przejścia	Wejście 21	NO	320		<input checked="" type="checkbox"/>
22	Sabotaż	Wejście 22	Według wyjścia	320	Ochrona Noc	<input checked="" type="checkbox"/>
23	Niewykorzystane					<input type="checkbox"/>
24	Niewykorzystane					<input type="checkbox"/>
25	Niewykorzystane					<input type="checkbox"/>

Moduł: piwnica  
 Typ modułu: INT-PP  
 Adres modułu: 1  
 Numer wejścia: 5  
 Typ

Opcje reakcji  
 Kontroler: 3, Magazyn

Rys. 32. Zakładka „Wejścia”.

### Parametry wejść

#### Tabela z listą wejść

**Nr** – numer porządkowy wejścia w systemie.

**Typ reakcji** (patrz: rozdział „Typy reakcji wejść”).

**Nazwa** – indywidualna nazwa wejścia (do 32 znaków).

**Typ linii** – możesz zaprogramować:

**Brak** – brak podłączonego urządzenia,

**NO** – obsługuje urządzenie posiadające wyjście typu NO (normalnie otwarte),

**NC** – obsługuje urządzenie posiadające wyjście typu NC (normalnie zamknięte),

**Według wyjścia** – stan zależy od stanu wybranego wyjścia (nie obsługuje żadnych podłączonych urządzeń).

**Czułość [ms]** – czas, przez który stan wejścia musi być zmieniony, aby zostało to zarejestrowane. Czas ten można programować w zakresie od 20 ms do 5,1 s.

**Aktywacja kalendarzem** – jeżeli opcja jest włączona, wejście jest obsługiwane tylko w czasie określonym przez kalendarz dostępu. Kalendarz możesz wybrać po kliknięciu prawym klawiszem myszki na pole. Kalendarze dostępu można utworzyć w aplikacji ACCO Web.

**Aktywne** – gdy opcja jest włączona, wejście jest obsługiwane. Opcja dostępna, gdy dla wejścia wybrany został typ reakcji.

### Informacje o wejściu

Po zaznaczeniu wejścia na liście, obok tabeli, wyświetlą się:

- nazwa, typ i adres modułu oraz numer wejścia w module,
- parametry definiowane dla danego typu linii lub reakcji:
  - numer wyjścia (typ linii „Według wyjścia”),
  - kontroler (typ reakcji „Otwarcie przejścia”, „Zablokowanie / Odblokowanie przejścia”, „Alarmowe zablokowanie przejścia” lub „Pożarowe odblokowanie przejścia”),
  - strefa – jedna lub wszystkie (typ reakcji: „Zablokowanie / Odblokowanie strefy”, „Alarmowe zablokowanie strefy” lub „Pożarowe odblokowanie strefy”).

### Typy reakcji wejść

Typ reakcji możesz wybrać po kliknięciu prawym klawiszem myszki na pole.

#### Niewykorzystane wejście

**Bez reakcji** – wejście wykorzystywane do złożonych operacji logicznych na wyjściach. Aktywne wejście nie wywoła bezpośrednio żadnej reakcji.

**Zablokowanie strefy** – aktywne wejście zablokuje przejścia nadzorowane przez wszystkie kontrolery przypisane do wybranej strefy. Przejścia pozostaną zablokowane tak długo, jak długo wejście będzie aktywne (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Odblokowanie strefy** – aktywne wejście odblokuje przejścia nadzorowane przez wszystkie kontrolery przypisane do wybranej strefy. Przejścia pozostaną odblokowane tak długo, jak długo wejście będzie aktywne (chyba że pojawi się zdarzenie, które w inny sposób zmieni stan przejścia).

**Alarmowe zablokowanie strefy** – trwałe zamknięcie wszystkich przejść w strefie z powodu alarmu. Przejścia pozostaną zablokowane do czasu zmiany ich stanu przy pomocy kodu lub dłuższego przytrzymania karty przez użytkownika posiadającego uprawnienie „Przełączanie”.

**Pożarowe odblokowanie strefy** – trwałe otwarcie wszystkich przejść w strefie z powodu pożaru. Przejścia pozostaną otwarte do czasu, gdy wszystkie wejścia kontrolera lub centrali ACCO-NT wrócą do stanu normalnego. Przejścia może przełączyć użytkownik posiadający uprawnienie „Przełączanie”.

**Otwarcie przejścia** – aktywne wejście otworzy przejście nadzorowane przez wybrany kontroler na czas zaprogramowany w polu „Czas na wejście” (w zakładce „Przejście” po

zaznaczeniu odpowiedniego kontrolera na liście). Kontroler należy wskazać w oknie, które wyświetli się po wybraniu tego typu reakcji dla wejścia.

**Zablokowanie przejścia** – aktywne wejście zablokuje przejście nadzorowane przez wybrany kontroler. Kontroler należy wskazać w oknie, które wyświetli się po wybraniu tego typu reakcji dla wejścia. Przejście pozostanie zablokowane do czasu zmiany jego stanu przez użytkownika posiadającego uprawnienie „Przełączanie” lub przy użyciu odpowiednich funkcji w programie ACCO Soft lub aplikacji ACCO Web.

**Odblokowanie przejścia** – aktywne wejście odblokuje przejście nadzorowane przez wybrany kontroler. Kontroler należy wskazać w oknie, które wyświetli się po wybraniu tego typu reakcji dla wejścia. Przejście pozostanie odblokowane do czasu zmiany jego stanu przez użytkownika posiadającego uprawnienie „Przełączanie” lub przy użyciu odpowiednich funkcji w programie ACCO Soft lub aplikacji ACCO Web.

**Alarmowe zablokowanie przejścia** – trwałe zamknięcie z powodu alarmu przejścia nadzorowanego przez wybrany kontroler. Kontroler należy wskazać w oknie, które wyświetli się po wybraniu tego typu reakcji dla wejścia. Przejście pozostanie zamknięte do czasu zmiany jego stanu przez użytkownika posiadającego uprawnienie „Przełączanie”.

**Pożarowe odblokowanie przejścia** – trwałe otwarcie z powodu pożaru przejścia nadzorowanego przez wybrany kontroler. Kontroler należy wskazać w oknie, które wyświetli się po wybraniu tego typu reakcji dla wejścia. Przejście pozostanie otwarte do czasu, gdy wejście kontrolera wróci do stanu normalnego. Przejście może przełączyć użytkownik posiadający uprawnienie „Przełączanie”.

**Sabotaż** – aktywowanie wejścia wywoła:

- awarię centrali ACCO-NT, o której odpowiednia ikona poinformuje w zakładce „Status”;
- alarm sabotażowy na wyjściu skonfigurowanym jako „Alarm sabotażowy z centrali”.

#### 4.2.9 Wyjścia

System kontroli dostępu obsługuje wyjścia:

- **przewodowe** – na płycie elektroniki centrali oraz w ekspanderach.
- **wirtualne** – wyjścia, które nie istnieją fizycznie, ale które mogą być wykorzystywane np. do realizacji funkcji logicznych.

##### 4.2.9.1 Numeracja wyjść w systemie

Wyjścia otrzymują numery w następujący sposób:

- wyjścia przewodowe na płycie elektroniki centrali mają numery od 1 do 8.
- numery wyjść w ekspanderach są uzależnione od adresu ekspandera w systemie (dla poszczególnych adresów ekspanderów numery wyjść są zarezerwowane – np. dla ekspandera o adresie 0 wyjścia będą miały numery od 9 do 16, dla ekspandera o adresie 1 wyjścia będą miały numery od 17 do 24 itd.).

##### 4.2.9.2 Programowanie wyjść

Kliknij na zakładkę „Wyjścia”. Zaznacz wyjście, żeby je zaprogramować.

#### Parametry wyjść

##### Tabela z listą wyjść

**Nr** – numer wyjścia w systemie.

**Typ wyjścia** (patrz: rozdział „Typy wyjść”).

**Nazwa** – indywidualna nazwa wyjścia (do 32 znaków).

**Tryb działania** – wybierz tryb działania wyjścia:

**Włączanie na czas (zdarzenie przedłuża)** – wyjście będzie włączane na czas zdefiniowany w polu „Czas działania”. Gdy wyjście jest aktywne, ponowne jego wyzwolenie skutkuje odliczaniem czasu działania od nowa.

**Włączanie na czas (zdarzenie wyłącza)** – wyjście będzie włączane na czas zdefiniowany w polu „Czas działania”. Gdy wyjście jest aktywne, ponowne jego wyzwolenie skutkuje wyłączeniem wyjścia.

**Włączanie na czas (ignorowanie zdarzeń)** – wyjście będzie włączane na czas zdefiniowany w polu „Czas działania”. Gdy wyjście jest aktywne, ponowne jego wyzwolenie nie ma wpływu na stan wyjścia.

**Przełączanie** – wyzwolenie wyjścia skutkuje przełączeniem jego stanu na przeciwny (jeżeli było włączone, zostanie wyłączone; jeżeli było wyłączone, zostanie włączone).

**Wskaźnik** – wyjście będzie aktywne tak długo, jak będzie podawany sygnał sterujący.

**Czas działania** – czas, przez który wyjście jest aktywne. Można zaprogramować od 0 do 127 sekund lub minut. W przypadku, gdy zostanie zaprogramowana wartość 0, wyjście będzie aktywne, gdy podawany będzie sygnał sterujący.

**i** *Jeśli wyjście typu: „Iloczyn logiczny z wyjść”, „Suma logiczna z wyjść”, „Iloczyn logiczny z wejść” lub „Suma logiczna z wejść” będzie miało zaprogramowany czas działania, będzie ono aktywne, gdy podawany będzie sygnał sterujący i jeszcze przez zaprogramowany czas.*

**w min/sek** – wybierz, czy czas działania ma być liczony w sekundach czy minutach.

**Polaryzacja** – opcja określa sposób działania wyjścia. W przypadku odwróconej polaryzacji w stanie aktywnym:

- wyjście typu OC jest odcinane od masy,
- zacisk NO wyjścia przekaźnikowego jest rozwierany, a zacisk NC zwierany.

**Negacja** – jeżeli opcja jest włączona, stan fizyczny wyjścia jest odwrotny do stanu prezentowanego w systemie (włączone wyjście prezentowane jest jako nieaktywne, a wyłączone – jako aktywne).

**Aktywne** – gdy opcja jest włączona, wyjście jest obsługiwane. Opcja dostępna, gdy dla wyjścia wybrany został typ.

Nr	Typ wyjścia	Nazwa	Tryb działania	Czas działania	w min/sek	Polaryzacja	Negacja	Aktywne
4	Iloczyn logiczny z wyjść	Wyjście 4	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	Suma logiczna z wyjść	Wyjście 5	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Iloczyn logiczny z wejść	Wyjście 6	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	Suma logiczna z wejść	Wyjście 7	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Aktywacja dostępem	Wyjście 8	Przełączanie	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9	Wskaźnik zablokowania stref	Wyjście 9	Wskaźnik	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Wskaźnik odblokowania stref	Wyjście 10	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11	Wskaźnik alarmowego zablokowania stref	Wyjście 11	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
12	Wskaźnik pożarowego odblokowania stref	Wyjście 12	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
13	Wskaźnik kontroli stref	Wyjście 13	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
14	Wskaźnik maks. liczby użytkowników	Wyjście 14	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
15	Wskaźnik min. liczby użytkowników	Wyjście 15	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
16	Wskaźnik zablokowania przejść	Wyjście 16	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
17	Wskaźnik odblokowania przejść	Wyjście 17	Wskaźnik	10	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
18	Wskaźnik alarmowego zablokowania przejść	Wyjście 18	Wskaźnik	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
19	Wskaźnik pożarowego odblokowania przejść	Wyjście 19	Wskaźnik	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
20	Wskaźnik kontroli przejść	Wyjście 20	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
21	Według kalendarza	Wyjście 21	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Niewykorzystane						<input type="checkbox"/>	<input type="checkbox"/>
23	Pilot	Wyjście 23	Przełączanie	0	sek	Normalna	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Status czuwania	Wyjście 24	Włączanie na czas (ignorowanie zdarzeń)	20	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
25	Alarm WEJŚCIE SŁOWE	Wyjście 25	Włączanie na czas (zdarzenie wyłącza)	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
26	Alarm sabotażowy z centrali	Wyjście 26	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
27	Alarm sabotażowy z ekspanderów	Wyjście 27	Wskaźnik	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
28	Alarm sabotażowy z kontrolerów	Wyjście 28	Włączanie na czas (zdarzenie przedłuża)	0	sek	Normalna	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Rys. 33. Zakładka „Wyjścia”.

## Informacje o wyjściu

Po zaznaczeniu wyjścia na liście, obok tabeli, wyświetlą się:

- nazwa, typ i adres modułu oraz numer wyjścia w module,
- parametry definiowane dla danego typu:
  - numery wyjść (typ wyjścia „Iloczyn logiczny z wyjść” lub „Suma logiczna z wyjść”),
  - numery wejść (typ wyjścia „Iloczyn logiczny z wejść” lub „Suma logiczna z wejść”),
  - strefa – jedna lub wszystkie (typ wyjścia „Aktywacja dostępem”),
  - strefa – wybrane (typ wyjścia: „Status czuwania”, „Wskaźnik zablokowania / odblokowania stref”, „Wskaźnik alarmowego zablokowania stref”, „Wskaźnik pożarowego odblokowania stref”, „Wskaźnik kontroli stref”, „Wskaźnik maks. liczby użytkowników” lub „Wskaźnik min. liczby użytkowników”),
  - przejście – wybrane (typ wyjścia: „Wskaźnik zablokowania / odblokowania przejść”, „Wskaźnik alarmowego zablokowania przejść”, „Wskaźnik pożarowego odblokowania przejść”, „Wskaźnik kontroli przejść”, „Alarm WEJŚCIE SIŁOWE”, „Alarm sabotażowy z kontrolerów”, „Uzyskanie dostępu” lub „Odmowa dostępu”),
  - kalendarz dostępu (typ wyjścia „Według kalendarza”),
  - ekspander (typ wyjścia „Alarm sabotażowy z ekspanderów”).

## Typy wyjść

Typ wyjścia możesz wybrać po kliknięciu prawym klawiszem myszki na pole.

### Niewykorzystane

**Iloczyn logiczny z wyjść** – wyzwalane, gdy wszystkie wyjścia sterujące są aktywne.

**Suma logiczna z wyjść** – wyzwalane, gdy dowolne z wyjść sterujących jest aktywne.

**Iloczyn logiczny z wejść** – wyzwalane, gdy wszystkie wejścia sterujące są aktywne.

**Suma logiczna z wejść** – wyzwalane, gdy dowolne z wejść sterujących jest aktywne.

**Pilot** – wyzwalane po naciśnięciu przycisku pilota.

**Aktywacja dostępem** – wyzwalane po uzyskaniu przez użytkownika dostępu do wybranej strefy z włączoną opcją „Aktywacja wyjść”.



*Aktywacja wyjść typu „Aktywacja dostępem” (przypisanych użytkownikowi w aplikacji ACCO Web) nastąpi po uzyskaniu przez użytkownika dostępu do wybranej strefy.*

**Wskaźnik zablokowania stref** – wyzwalane, gdy dowolna z wybranych stref zostanie zablokowana.

**Wskaźnik odblokowania stref** – wyzwalane, gdy dowolna z wybranych stref zostanie odblokowana.

**Wskaźnik alarmowego zablokowania stref** – wyzwalane, gdy dowolne przejście w dowolnej z wybranych stref są trwale zamknięte z powodu alarmu.

**Wskaźnik pożarowego odblokowania stref** – wyzwalane, gdy dowolne przejście w dowolnej z wybranych stref są trwale otwarte z powodu pożaru.

**Wskaźnik zablokowania przejść** – wyzwalane, gdy dowolne z wybranych przejść zostanie zablokowane.

**Wskaźnik odblokowania przejść** – wyzwalane, gdy dowolne z wybranych przejść zostanie odblokowane.

**Wskaźnik alarmowego zablokowania przejść** – wyzwalane, gdy dowolne z wybranych przejść jest trwale zamknięte z powodu alarmu.

**Wskaźnik pożarowego odblokowania przejść** – wyzwalane, gdy dowolne z wybranych przejść jest trwale otwarte z powodu pożaru.



**Wskaźnik kontroli stref** – wyzwalane, gdy stan dowolnej z wybranych stref jest kontrolowany.

**Wskaźnik kontroli przejść** – wyzwalane, gdy stan dowolnego z wybranych przejść jest kontrolowany.

**Według kalendarza** – wyzwalane zgodnie z ramkami czasowymi wyznaczonymi przez wybrany kalendarz dostępu.

**Wskaźnik maks. liczby użytkowników** – wyzwalane, gdy w dowolnej z wybranych stref przebywa maksymalna liczba użytkowników.

**Wskaźnik min. liczby użytkowników** – wyzwalane, gdy w dowolnej z wybranych stref przebywa minimalna liczba użytkowników.

**Status czuwania** – wyzwalane, gdy w dowolnej z wybranych zintegrowanych stref zostanie załączone czuwanie.

**Alarm WEJŚCIE SIŁOWE** – wyzwalane, gdy z dowolnego z wybranych przejść zostanie wywołany alarm „Wejście siłowe”.

**Alarm sabotażowy z centrali** – wyzwalane podczas aktywacji wejścia zaprogramowanego jako „Sabotaż”. Zostanie wywołany alarm sabotażowy centrali ACCO-NT.

**Alarm sabotażowy z ekspanderów** – wyzwalane, gdy z dowolnego z wybranych ekspanderów zostanie wywołany alarm sabotażowy.

**Alarm sabotażowy z kontrolerów** – wyzwalane, gdy z dowolnego z wybranych kontrolerów zostanie wywołany alarm sabotażowy.

**Uzyskanie dostępu** – wyzwalane, gdy do dowolnego z wybranych przejść zostanie uzyskany dostęp.

**Odmowa dostępu** – wyzwalane, gdy do dowolnego z wybranych przejść nie zostanie uzyskany dostęp.

#### 4.2.10 Ścieżki przejść

Ścieżka przejścia to trasa, którą będzie musiał poruszać się użytkownik po obiekcie. Takie rozwiązanie może być wykorzystane np. przez serwis sprzątający.

##### Opis przycisków




- kliknij, żeby dodać ścieżkę.



- kliknij, żeby usunąć zaznaczoną wcześniej ścieżkę (patrz: rozdział „Usunięcie ścieżki przejścia”).

##### 4.2.10.1 Utworzenie ścieżki przejścia


1. Zaznacz centralę na liście obiektów i central.
2. Kliknij na przycisk . Nowa ścieżka przejścia pojawi się na liście.
3. Kliknij prawym klawiszem myszki na pole w kolumnie „Strefa” i wybierz jedną ze stref.
4. Określ minimalny czas przebywania użytkownika w danej strefie.
5. Jeśli chcesz przypisać do ścieżki kolejne strefy, powtórz czynności opisane w punktach 3 i 4.
6. Zapisz wprowadzone zmiany.

##### 4.2.10.2 Programowanie ścieżki przejścia

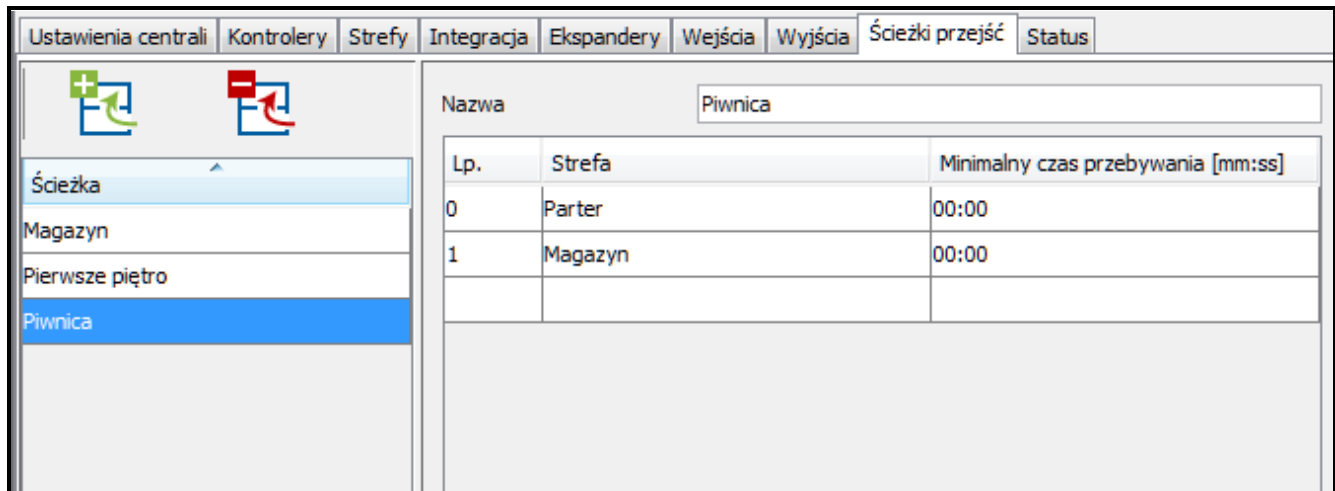
Kliknij na zakładkę „Ścieżki przejść”. Zaznacz ścieżkę przejścia, żeby ją zaprogramować.

**Nazwa** – indywidualna nazwa ścieżki (do 45 znaków).

Po wprowadzeniu nowej nazwy lub zmiany w dotychczasowej nazwie wyświetlą się przyciski:

 – kliknij, żeby anulować wprowadzone zmiany.

 – kliknij, żeby zatwierdzić wprowadzone zmiany.



Rys. 34. Zakładka „Ścieżki przejść”.

### **Tabela do definiowania ścieżki przejścia**

**Lp.** – liczba określająca kolejność stref tworzących trasę.

**Strefa** – nazwa strefy wchodzącej w skład ścieżki przejścia.

**Minimalny czas przebywania [mm:ss]** – minimalny czas przebywania użytkownika w danej strefie, po upływie którego będzie on mógł przejść do następnej strefy. Maksymalnie zaprogramować można 59 minut i 59 sekund.

Jeżeli w kolumnie „Strefa” jest wyświetlana nazwa strefy, po kliknięciu prawym klawiszem myszki na wiersz w tabeli, wyświetli się rozwijane menu:

**W górę** – przenosi zaznaczoną strefę o jedno pole wyżej.

**Usuń** – usuwa zaznaczoną strefę z listy.

**W dół** – przenosi zaznaczoną strefę o jedno pole niżej.

#### **4.2.10.3 Usunięcie ścieżki przejścia**

1. Jeżeli chcesz usunąć pojedynczą ścieżkę, zaznacz kursorem wybraną ścieżkę na liście ścieżek.
2. Jeśli chcesz usunąć za jednym razem kilka ścieżek, zaznacz kursorem jedną ze ścieżek i trzymając wciśnięty klawisz Ctrl wybierz kolejne zaznaczając je lewym przyciskiem myszki.
3. W przypadku, gdy chcesz usunąć wszystkie ścieżki, zaznacz kursorem jedną ze ścieżek i naciśnij jednocześnie klawisze Ctrl+A.

4. Kliknij wskaźnikiem myszki na przycisk .

5. Gdy wyświetli się pytanie, czy usunąć ścieżkę, kliknij „Tak”.

6. Zapisz wprowadzone zmiany.

#### **4.2.11 Status**

W zakładce „Status” wyświetlane są informacje dotyczące aktualnego stanu: centrali, zasilania, a także wejść i wyjść centrali oraz ekspanderów.



W przypadku, gdy pomiędzy ACCO Server a centralą nie będzie komunikacji, wyświetli się informacja o braku komunikacji, a także data i godzina ostatniej transmisji odebranej przez serwer od centrali.

Rys. 35. Zakładka „Status” dla systemu.



#### 4.2.11.1 Awarie centrali

W obszarze tym wyświetlane są ikony informujące o:

- awarii lub braku karty MicroSD,
- przeciążeniu wyjścia zasilającego AUX,
- przeciążeniu wyjścia zasilającego urządzenia podłączone do magistrali ekspanderów +EX,
- awarii zasilacza,
- braku zasilania AC,
- braku akumulatora,
- rozładowaniu akumulatora,
- sabotażu centrali.

Poszczególne ikony symbolizują następujący stan:

- – wszystko OK (szare tło),
- – awaria (biały wykrzyknik na czerwonym tle),
- – potwierdzona awaria (biały wykrzyknik na czerwonym tle i biały symbol na zielonym tle),
- – pamięć awarii (biały wykrzyknik na szarym tle),

-  – pamięć potwierdzonej awarii (biały wykrzyknik na szarym tle i biały symbol na zielonym tle),
-  – stan nieznan (biały znak zapytania na szarym tle).



*Jeśli chcesz potwierdzić awarię, kliknij na znajdujący się przy niej przycisk.*

#### 4.2.11.2 Stan zasilania centrali

W obszarze tym wyświetlane są informacje dotyczące stanu zasilania centrali.

#### 4.2.11.3 Zakładka „Wejścia”

W zakładce wyświetlane są informacje o stanie wejść. Kolory oznaczają:

- szary – nieaktywne wejście,
- zielony – aktywne wejście.

#### 4.2.11.4 Zakładka „Wyjścia”

W zakładce wyświetlane są informacje o stanie wyjść. Kolory oznaczają:

- szary – nieaktywne,
- zielony – aktywne.

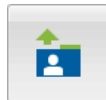
### 4.2.12 Import


Przycisk „Import” umożliwia importowanie danych dotyczących użytkowników i harmonogramów z plików z programu ACCO-SOFT-LT (z rozszerzeniem kkd) oraz z plików w formacie CSV.

#### 4.2.12.1 Import danych z pliku w formacie CSV



*Importowanie pakietu danych dotyczących kilkudziesięciu użytkowników może trwać nawet kilkanaście minut.*

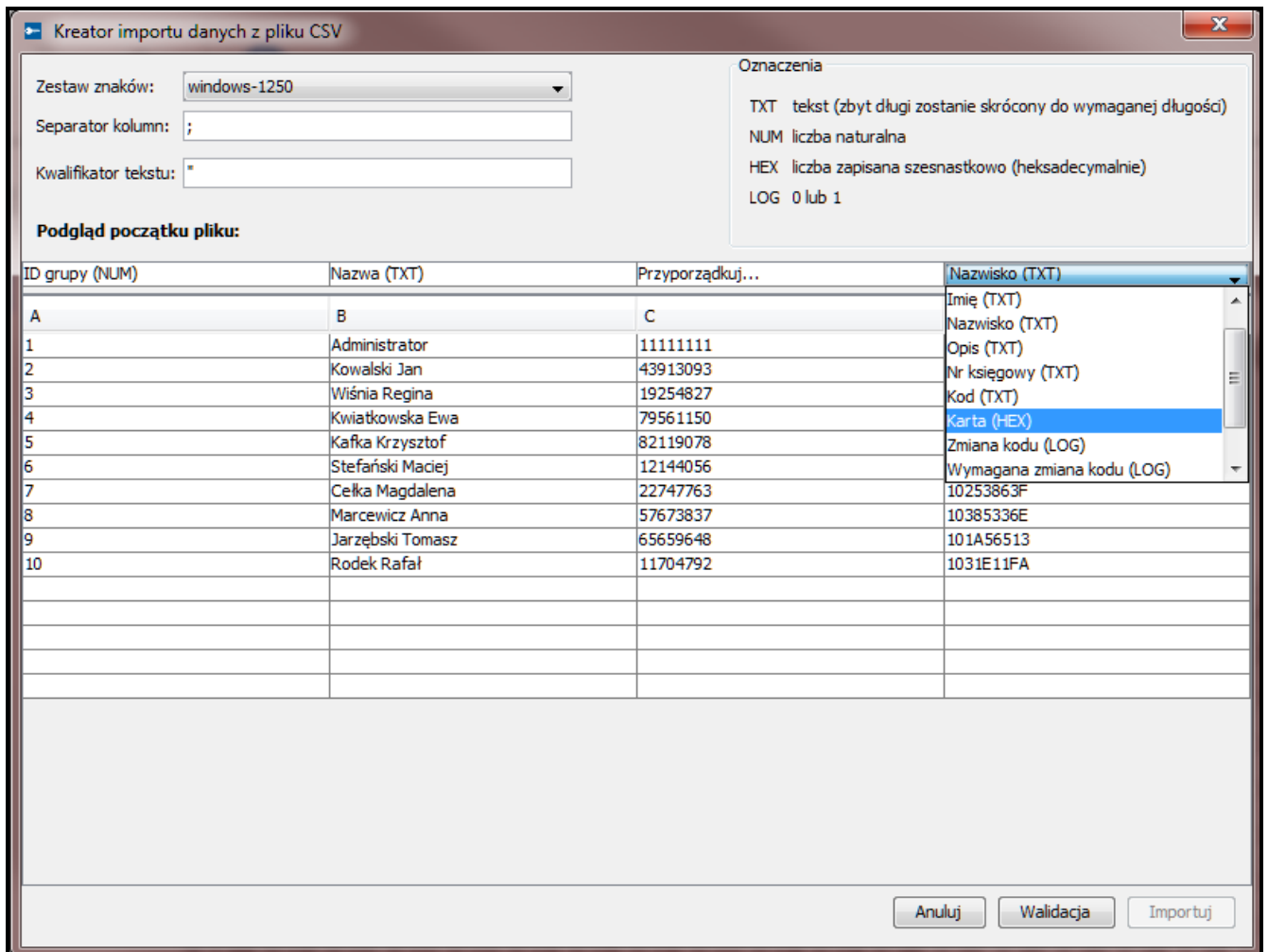


1. W głównym oknie kliknij na przycisk .
2. W menu, które się wyświetli, wybierz polecenie „Importuj z csv”.
3. Wskaż plik z danymi, które chcesz zaimportować.
4. W oknie, które się otworzy, określ sposób kodowania danych z importowanego pliku.
5. Dopasuj etykiety do poszczególnych kolumn z zaimportowanymi danymi. **Konieczne jest przyporządkowanie etykiety „Nazwa” do kolumny zawierającej zaimportowane nazwy użytkowników.**
6. Kliknij na przycisk „Walidacja”, żeby sprawdzić, czy wybrany plik zawiera poprawne dane.
7. Jeśli dane są poprawne, kliknij wskaźnikiem myszki na przycisk „Importuj”, żeby uruchomić procedurę importowania danych. Po jej zakończeniu wyświetli się komunikat, który o tym poinformuje.
8. Jeśli dane nie są poprawne, wybierz inny plik i powtórz czynności opisane w punktach 4 - 7.

**Zestaw znaków** – wybierz zestaw znaków pisarskich odpowiedni dla języka, który został zastosowany w importowanym pliku.

**Separator kolumn** – wpisz znak, który został zastosowany w importowanym pliku do podzielenia tekstu na kolumny.

**Kwalifikator tekstu** – wpisz znak, który został zastosowany w importowanym pliku do wyznaczania granic danych tekstowych.



Rys. 36. Okno do importowania danych z pliku w formacie CSV.

**Przyporządkuj...** – kliknij prawym klawiszem myszki na pole. Wyświetli się menu rozwijane z listą etykiet danych, które zostały zaimportowane z pliku. Dopasuj wybraną etykietę do zawartości kolumny klikając na nią wskaźnikiem myszki.


**Anuluj** – kliknij, żeby anulować wprowadzone zmiany.

**Walidacja** – kliknij, żeby sprawdzić poprawność danych w importowanym pliku. Po sprawdzeniu wyświetli się komunikat informujący o wynikach walidacji. Przycisk stanie się aktywny po przyporządkowaniu etykiety „Nazwa” do kolumny zawierającej zaimportowane nazwy użytkowników.

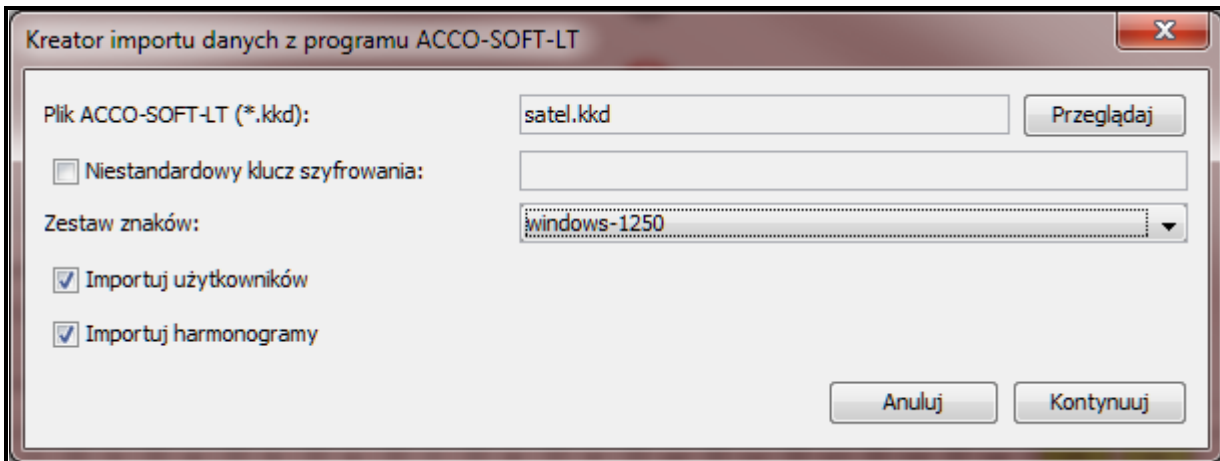
**Importuj** – kliknij, żeby uruchomić procedurę importowania danych. Przycisk stanie się aktywny po przeprowadzeniu walidacji danych w importowanym pliku.

#### 4.2.12.2 Import danych z pliku z rozszerzeniem kkd



1. W głównym oknie kliknij na przycisk .
2. W menu, które się wyświetli, wybierz polecenie „Importuj z ACCO-SOFT-LT”.
3. Wskaż plik z danymi, które chcesz zaimportować.
4. Jeśli w programie ACCO-SOFT-LT zdefiniowałeś swój klucz szyfrowania, zaznacz opcję „Niestandardowy klucz szyfrowania” i wpisz klucz w odpowiednie pole. Jeżeli nie definiowałeś klucza, nie zaznaczaj opcji.
5. Określ sposób kodowania danych.

6. Zdecyduj, które dane mają być importowane.
7. Kliknij wskaźnikiem myszki na przycisk „Kontynuuj”.
8. Otworzy się okno z informacjami dotyczącymi importowanych danych (patrz: rys. 38). Kliknij na przycisk „Importuj”, żeby uruchomić procedurę importowania danych. Po jej zakończeniu wyświetli się komunikat, który o tym poinformuje.



Rys. 37. Okno do importowania danych z programu ACCO-SOFT-LT.

**Plik ACCO-SOFT-LT (\*.kkd)** – nazwa pliku z danymi.

**Przełóżaj** – kliknij, żeby wskazać ścieżkę dostępu do wybranego pliku z danymi.

**Niestandardowy klucz szyfrowania** – zaznacz opcję, a w polu obok wpisz indywidualny klucz (hasło) kodowania danych pliku konfiguracyjnego, który został zastosowany w programie ACCO-SOFT-LT.

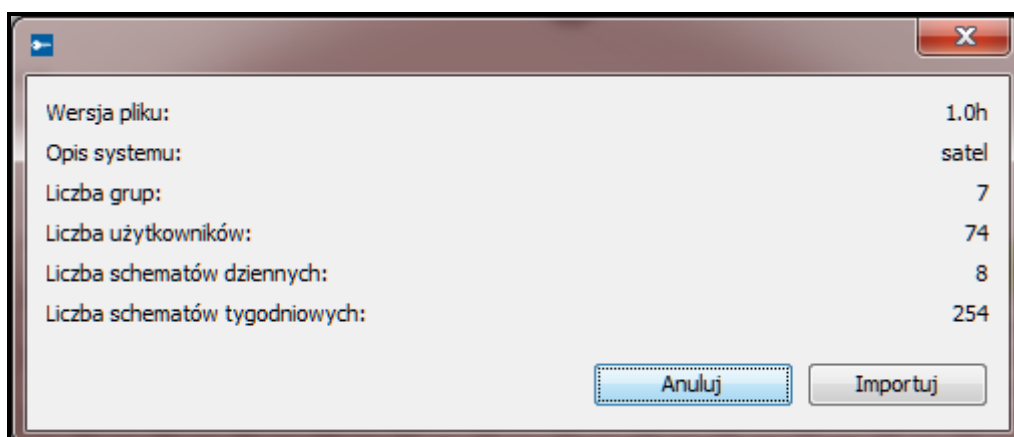
**Zestaw znaków** – wybierz zestaw znaków odpowiedni dla języka, który został zastosowany w importowanym pliku.

**Importuj użytkowników** – zaznacz opcję, jeśli chcesz importować dane dotyczące użytkowników.

**Importuj harmonogramy** – zaznacz opcję, jeśli chcesz importować dane dotyczące harmonogramów. Zimportowane dane wyświetlą się w aplikacji ACCO Web jako schematy dostępu – tygodniowe i dzienne.

**Anuluj** – kliknij, żeby anulować wprowadzone zmiany.

**Kontynuuj** – kliknij, żeby zatwierdzić wprowadzone dane. Otworzy się okno z informacjami dotyczącymi importowanych danych z programu ACCO-SOFT-LT (patrz: rys. 38).



Rys. 38. Okno z informacjami dotyczącymi importowanych danych z programu ACCO-SOFT-LT.

## 5. Załącznik 1 „Opis działania integracji systemów”

- Zablokowanie strefy w systemie kontroli dostępu skutkuje załączeniem czuwania w strefie systemu alarmowego.
- Przywrócenie kontroli w strefie systemu kontroli dostępu skutkuje wyłączeniem czuwania w strefie systemu alarmowego.
- Załączenie czuwania w strefie systemu alarmowego skutkuje zablokowaniem strefy systemu kontroli dostępu.
- Wyłączenie czuwania w strefie systemu alarmowego skutkuje przywróceniem kontroli w strefie systemu kontroli dostępu.



*W przypadku, gdy zostaną zmienione ustawienia kontrolerów, a załączone jest czuwanie, po zapisaniu nowych ustawień czuwanie zostanie automatycznie wyłączone.*

Możesz załączyć czuwanie w strefie systemu alarmowego:

- blokując strefę systemu kontroli dostępu przy pomocy programu ACCO Soft lub aplikacji ACCO Web,
- blokując przejście przy pomocy terminala wejściowego do tej strefy; dla tego terminala musi być włączona opcja „Steruje strefą”,
- blokując przejścia nadzorowane przez kontrolery należące do strefy kontroli dostępu (tylko przy odpowiedniej konfiguracji terminali podłączonych do kontrolerów).



*Strefę można zablokować tylko przy pomocy terminala wejściowego, dla którego włączono opcję „Steruje strefą”. Przy pomocy terminala wyjściowego można zablokować tylko przejście (zablokowanie wszystkich przejść w strefie skutkuje zablokowaniem strefy).*

*Jeżeli strefa jest zablokowana i przypisanych jest do niej kilka kontrolerów, próba uzyskania dostępu do przejścia przez użytkownika, który posiada uprawnienie „Przełączanie”, spowoduje zmianę stanu strefy na „Mieszany” i otwarcie tego przejścia.*

*Jeżeli odblokujesz strefę przy pomocy programu ACCO Soft lub aplikacji ACCO Web, wyłączysz czuwanie w strefie.*

*Jeżeli przejście w strefie, w której załączone jest czuwanie, zostanie odblokowane przy pomocy programu ACCO Soft lub aplikacji ACCO Web, czuwanie w strefie nadal będzie załączone.*

*W przypadku integracji, zmiana stanu strefy systemu alarmowego wpływa na stan strefy systemu kontroli dostępu. Przykładowo: obiekt został podzielony na dwie strefy. Do każdej z nich przypisano po dwa przejścia, z czego jedno jest wspólne. Obie strefy systemu kontroli dostępu są zintegrowane ze strefami systemu alarmowego (jak na rys. 39). W przypadku, gdy:*

- w strefie systemu alarmowego zostaje załączone czuwanie, wszystkie przejścia przypisane do zintegrowanej strefy systemu kontroli dostępu są blokowane,
- w strefie systemu alarmowego zostaje wyłączone czuwanie:
  - sprawdzany jest aktualny stan sąsiedniej strefy. Jeśli w sąsiedniej strefie jest załączone czuwanie, to wspólne przejście obu stref pozostanie nadal zablokowane.

- sprawdzany jest aktualny stan wspólnego dla obu stref przejścia. Jeśli jest odblokowane, to nadal pozostanie odblokowane.

*W pozostałych przypadkach kontrola przejścia zostanie przywrócona.*

Czuwanie w strefie systemu alarmowego możesz wyłączyć przywracając kontrolę w strefie systemu kontroli dostępu.


Alarmy, które zostały wywołane w systemie alarmowym mogą być przekazywane do systemu kontroli dostępu (patrz: opcje „Przełącz alarm włamaniowy ze strefy INTEGRA” i „Przełącz alarm pożarowy ze strefy INTEGRA”). Alarm wywołany w systemie alarmowym może być skasowany tylko w systemie alarmowym.

Alarmy, które zostały wywołane w systemie kontroli dostępu, nie są przekazywane do systemu alarmowego.

Szczegółowe informacje znajdziesz w załączniku „Obsługa zintegrowanych stref”.

## 6. Załącznik 2 „Obsługa zintegrowanych stref”

W celu załączenia czuwania możesz zablokować strefę systemu kontroli dostępu:

- przy pomocy czytnika pełniącego funkcję terminala wejściowego, podłączonego do jednego z kontrolerów w strefie; dla tego terminala musi być włączona opcja „Steruje strefą”,
- z programu ACCO Soft – w zakładce „Strefy” najedź kursorem na wybraną strefę na liście stref, kliknij prawym klawiszem myszki i w rozwijanym menu, które się otworzy, wybierz funkcję „Zablokuj”,
- z aplikacji ACCO Web – w menu po lewej stronie kliknij na polecenie „Zarządzanie”, następnie na „Struktura”, przejdź do zakładki „Strefy”, zaznacz wybraną strefę na liście stref i kliknij na przycisk ,
- z aplikacji ACCO Web – w menu po lewej stronie kliknij na polecenie „Mapy”, otwórz odpowiednią mapę, najedź kursorem na obszar ilustrujący na mapie wybraną strefę, kliknij lewym przyciskiem myszki i wybierz funkcję „Zablokuj”,
- zgodnie z zaprogramowanym czasem lub przypisanym kalendarzem dostępu – w programie ACCO Soft w zakładce „Strefy” zaznacz wybraną strefę na liście stref, przejdź do zakładki „Opcje” i przy pomocy funkcji „Zablokowanie strefy” zdefiniuj czas lub przypisz kalendarz dostępu,
- przez aktywację wejścia centrali ACCO-NT – w programie ACCO Soft w zakładce „Wejścia” zaprogramuj wybrane wejście jako „Zablokowanie strefy”,



*Użytkownik może zablokować strefę tylko wtedy, gdy:*


- użyje terminala wejściowego, dla którego włączono opcję „Steruje strefą”,
- posiada uprawnienie „Przełączanie”,
- ma dostęp do danej strefy, zgodnie z przypisanym mu kalendarzem dostępu.

*Zdefiniowany czas oraz zaprogramowany kalendarz nie mają priorytetu. Oznacza to, że wystąpienie innych zdarzeń w module może zmienić stan strefy przed upływem przewidzianego czasu zablokowania.*

*Jeżeli dla danego terminala wybierzesz ten sam typ identyfikatora dla uzyskania dostępu oraz blokowania, po użyciu identyfikatora zostanie przyznany dostęp. Stan przejścia / strefy nie ulegnie zmianie.*



W celu wyłączenia czuwania możesz przywrócić kontrolę w strefie systemu kontroli dostępu:

- przy pomocy czytnika pełniącego funkcję terminala wejściowego, podłączonego do jednego z kontrolerów w strefie; dla tego terminala musi być włączona opcja „Steruje strefą”,
- z programu ACCO Soft – w zakładce „Strefy” najedź kursorem na wybraną strefę na liście stref, kliknij prawym klawiszem myszki i w rozwijanym menu, które się otworzy, wybierz funkcję „Przywróć kontrolę”,
- z aplikacji ACCO Web – w menu po lewej stronie kliknij na polecenie „Zarządzanie”, następnie na „Struktura”, przejdź do zakładki „Strefy”, zaznacz wybraną strefę na liście stref i kliknij na przycisk ,
- z aplikacji ACCO Web – w menu po lewej stronie kliknij na polecenie „Mapy”, otwórz odpowiednią mapę, najedź kursorem na obszar ilustrujący na mapie wybraną strefę, kliknij lewym przyciskiem myszki i wybierz funkcję „Przywróć kontrolę”,
- po powrocie naruszonego wejścia centrali ACCO-NT (zaprogramowanego jako „Zablokowanie strefy”) do stanu normalnego,



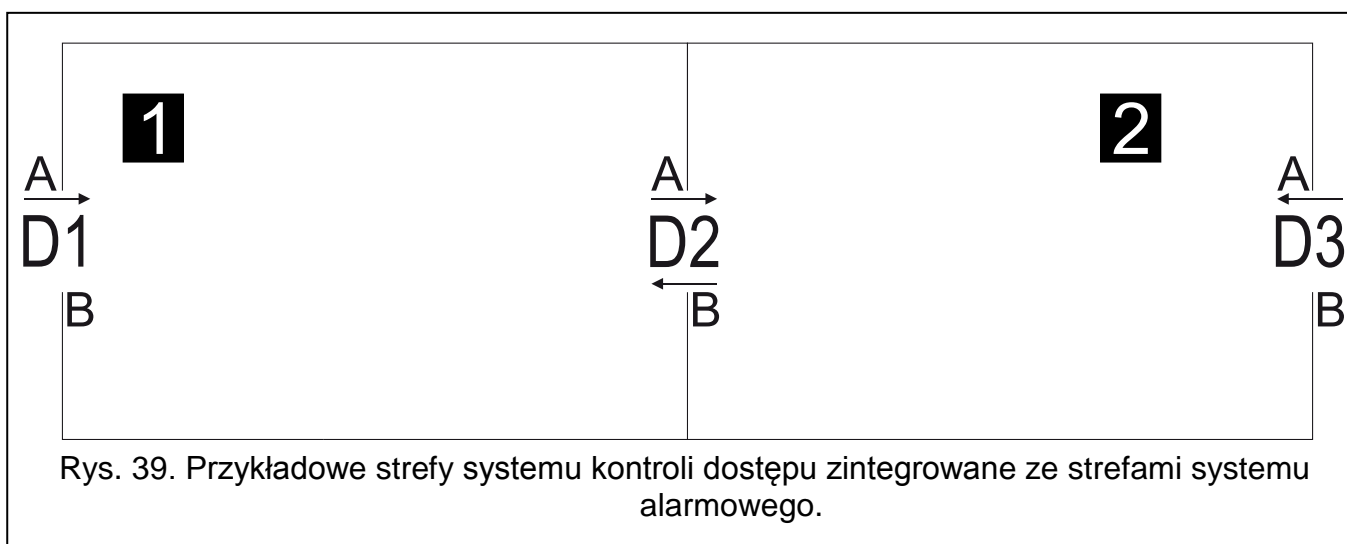
*Użytkownik może zablokować strefę tylko wtedy, gdy:*

- użyje terminala wejściowego, dla którego włączono opcję „Steruje strefą”,
- posiada uprawnienie „Przełączanie”,
- ma dostęp do danej strefy, zgodnie z przypisanym mu kalendarzem dostępu.

*Jeżeli dla danego terminala wybierzesz ten sam typ identyfikatora dla uzyskania dostępu oraz przywracania kontroli, po użyciu identyfikatora zostanie przyznany dostęp. Stan przejścia / strefy nie ulegnie zmianie.*

## 6.1 Przykłady

### 6.1.1 Przykład 1



Rys. 39. Przykładowe strefy systemu kontroli dostępu zintegrowane ze strefami systemu alarmowego.

Objaśnienia do rysunku 39:

**1 i 2** (numery na czarnym tle) – strefy zintegrowane ze strefami systemu alarmowego.

**D1** – kontroler przypisany do strefy 1. Terminal A to wejście do strefy 1, a terminal B to wyjście ze strefy 1.

**D2** – kontroler przypisany do stref 1 i 2. Terminal A to wejście do strefy 2 i wyjście ze strefy 1. Natomiast terminal B to wyjście ze strefy 2 i wejście do strefy 1.

**D3** – kontroler przypisany do strefy 2. Terminal A to wejście do strefy 2, a terminal B to wyjście ze strefy 2.

### **Załączenie czuwania**



*W celu załączenia czuwania w strefie systemu alarmowego, należy zablokować strefę systemu kontroli dostępu. Można to zrobić tylko przy pomocy terminala pełniącego funkcję wejścia do tej strefy. Dla tego terminala musi być włączona opcja „Steruje strefą”.*

#### **Obsługa strefy 1**

Gdy chcesz załączyć czuwanie w strefie 1, użyj terminala A przejścia D1 lub terminala B przejścia D2.

#### **Obsługa strefy 2**

Gdy chcesz załączyć czuwanie w strefie 2, użyj terminala A przejścia D2 lub terminala A przejścia D3.

### **Wyłączenie czuwania**



*W celu wyłączenia czuwania w strefie systemu alarmowego, należy przywrócić kontrolę w strefie systemu kontroli dostępu. Można to zrobić tylko przy pomocy terminala pełniącego funkcję wejścia do tej strefy. Dla tego terminala musi być włączona opcja „Steruje strefą”.*

#### **Obsługa strefy 1**

Gdy chcesz wyłączyć czuwanie w strefie 1, użyj terminala A przejścia D1 lub terminala B przejścia D2.

#### **Obsługa strefy 2**

Gdy chcesz wyłączyć czuwanie w strefie 2, użyj terminala A przejścia D2 lub terminala A przejścia D3.

## **6.2 Sygnalizacja blokowania przejścia / strefy przez urządzenia systemu kontroli dostępu**

---

W rozdziale opisana została dodatkowa sygnalizacja związana z integracją systemów.

### **6.2.1 Sygnalizacja optyczna**

#### **6.2.1.1 Priorytety stanów systemu ACCO NET**


W przypadku, gdy w systemie ACCO NET równocześnie występują różne zdarzenia, o których mogą informować diody LED w urządzeniach systemu kontroli dostępu, priorytet tych zdarzeń jest następujący (urządzenie informuje o zdarzeniu, które ma najwyższy priorytet):


1. Brak komunikacji pomiędzy centralą ACCO-NT a kontrolerem ACCO-KP.
2. Zablokowanie przejścia z powodu alarmu włamaniowego.
3. Zablokowanie przejścia.
4. Odblokowanie przejścia z powodu alarmu pożarowego.
5. Odblokowanie przejścia.
6. Błąd integracji (patrz: opis kolumny „Stan” w tabeli z listą systemów alarmowych w zakładce „Integracja”).

### 6.2.1.2 Manipulatory


Po zablokowaniu przejścia / strefy na wyświetlaczu manipulatora może zostać zaprezentowana nazwa użytkownika, który uruchomił tę funkcję.



Diody LED w manipulatorze informują o stanie przejścia / strefy w następujący sposób:

 (kolor czerwony) – dioda świeci, sygnalizując alarm, gdy wystąpił alarm włamaniowy lub pożarowy w centrali alarmowej. Alarm sygnalizowany jest przez 10 sekund (towarzyszy temu sygnalizacja dźwiękowa). Po upływie tego czasu, dioda zaczyna migać, sygnalizując pamięć alarmu. Po ustaniu przyczyny alarmu, sygnalizację pamięci alarmu w manipulatorze kasuje się przez potwierdzenie pamięci alarmu w programie ACCO Soft lub w aplikacji ACCO Web.

 (kolor żółty):



- dioda świeci – przejście / strefa jest zablokowane, w zintegrowanej strefie czuwanie jest załączone,
- dioda miga powoli – przejście zostało zablokowane z powodu alarmu włamaniowego w centrali alarmowej.

 (kolor zielony) – dioda miga powoli, gdy przejście zostało odblokowane z powodu alarmu pożarowego w centrali alarmowej.

 (kolor żółty) i  (kolor zielony):

- diody migają na przemian powoli – błąd integracji.
- diody migają na przemian szybko – brak komunikacji pomiędzy centralą ACCO-NT a kontrolerem ACCO-KP.

### 6.2.1.3 Klawiatura z czytnikiem kart zbliżeniowych

Informacje przekazywane przez klawiaturę przy pomocy diod LED ,  i  są identyczne, jak w przypadku manipulatora LCD.

### 6.2.1.4 Czytniki kart zbliżeniowych

Dwukolorowa dioda LED w czytnikach CZ-EMM i CZ-EMM2 sygnalizuje stan przejścia / strefy w następujący sposób:

- dioda miga powoli na zielono – przejście zostało odblokowane z powodu alarmu pożarowego w centrali alarmowej,
- dioda miga powoli na czerwono – przejście / strefa jest zablokowane, w zintegrowanej strefie czuwanie jest załączone lub przejście zostało zablokowane z powodu alarmu włamaniowego w centrali alarmowej,
- dioda miga powoli na przemian na zielono i czerwono – błąd integracji,
- dioda miga szybko na przemian na zielono i czerwono – brak komunikacji pomiędzy centralą ACCO-NT a kontrolerem ACCO-KP.

Diody LED w czytnikach CZ-EMM3 i CZ-EMM4 informują o stanie przejścia / strefy w następujący sposób:

- zielona dioda LED miga powoli – przejście zostało odblokowane z powodu alarmu pożarowego w centrali alarmowej,
- czerwona dioda LED miga powoli – przejście / strefa jest zablokowane, w zintegrowanej strefie czuwanie jest załączone lub przejście zostało zablokowane z powodu alarmu włamaniowego w centrali alarmowej,
- diody migają na przemian powoli – błąd integracji,
- diody migają na przemian szybko – brak komunikacji pomiędzy centralą ACCO-NT a kontrolerem ACCO-KP.

### 6.2.1.5 Czytnik pastylek DALLAS

Dwukolorowa dioda LED w czytniku sygnalizuje stan przejścia / strefy w następujący sposób:

- dioda miga powoli na zielono – przejście zostało odblokowane z powodu alarmu pożarowego w centrali alarmowej,
- dioda miga powoli na czerwono – przejście / strefa jest zablokowane, w zintegrowanej strefie czuwanie jest załączone lub przejście zostało zablokowane z powodu alarmu włamaniowego w centrali alarmowej,
- dioda miga powoli na przemian na zielono i czerwono – błąd integracji,
- dioda miga szybko na przemian na zielono i czerwono – brak komunikacji pomiędzy centralą ACCO-NT a kontrolerem ACCO-KP.

### 6.2.2 Sygnalizacja dźwiękowa

Urządzenia współpracujące z modułami ACCO-KP (manipulator, klawiatura z czytnikiem kart zbliżeniowych oraz czytniki kart zbliżeniowych) generują dźwięki o charakterze informacyjnym:

**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).

**Dźwięk ciągły** – alarm.

**2 krótkie dźwięki co sekundę** – odliczanie czasu na wejście lub powrót przejścia / strefy do trybu normalnego, czyli wyłączenie czuwania.

**1 krótki dźwięk, a następnie 2 krótkie dźwięki** – udzielenie dostępu, a następnie zablokowanie przejścia / strefy, czyli załączenie czuwania.