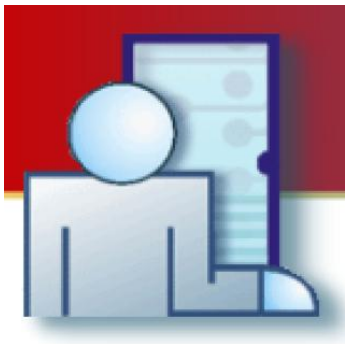


INSTRUKCJA DO PROGRAMU PR MASTER

Wersja PRM 4.5.26

Rev. P

Spis treści

I. WPROWADZENIE

PR Master to program do obsługi systemu kontroli dostępu RACS 4 (**Roger Access Control System**) zbudowanego na bazie produkowanych przez firmę Roger kontrolerów serii PRxx2 oraz PRxx1, czytników serii PRT, interfejsów komunikacyjnych serii UT i RCI oraz central CPR32-SE i CPR32-NET.

Program PR Master jest aplikacją systemów operacyjnych 32-bitowych od Windows XP wzwyż oraz 64-bitowych od Windows Vista wzwyż.

W programie PR Master od wersji 4.5.4 wzwyż wprowadzono licencjonowanie. Do integracji z centralami alarmowymi serii INTEGRA (SATEL) i z zamkami bezprzewodowymi systemu APERIO (ASSA ABLOY) wymagany jest klucz licencyjny, który jest obsługiwany przez program PR Master ale jest oddzielnie generowany dla każdej centrali CPR32-NET w systemie. Wbudowany (darmowy) klucz licencyjny programu PR Master pozwala realizować wszystkie opisane w instrukcji funkcje systemu kontroli dostępu a jedyne jego ograniczenia to:

- obsługa maksymalnie dwóch stref alarmowych centrali INTEGRA (SATEL) przez każdą centralę CPR32-NET
- obsługa maksymalnie dwóch zamków systemu APERIO (ASSA ABLOY) przez każdą centralę CPR32-NET

Maksymalna możliwa ilość stref alarmowych INTEGRY obsługiwanych w systemie to 32 a maksymalna możliwa ilość zamków w ramach pojedynczej centrali CPR32-NET to 16.

Dodatkowo licencjonowaniu mogą podlegać niektóre wersje językowe programu PR Master z wyłączeniem wersji polskiej i angielskiej.

Program jest wykorzystywany przez:

- **instalatorów** — którzy przeprowadzają wstępną konfigurację systemu i przygotowują go do pracy;
- **użytkowników końcowych (właścicieli)** — którzy zajmują się bieżącą eksploatacją systemu, tworzeniem raportów, wykonywaniem kopii zapasowych, zarządzaniem użytkownikami, doraźnym tworzeniem stref APB, obszarów obecności itp.

Podział ten jest zgodny z cyklem życia systemu kontroli dostępu. Najpierw firma instaluje system kontroli dostępu, montuje wszystkie urządzenia, wstępnie konfiguruje system, a następnie przekazuje go użytkownikowi końcowemu, który od tej pory jest odpowiedzialny za jego bieżącą eksploatację.

Aplikacja PR Master powinna zostać zainstalowana przez instalatora — przedstawiciela firmy wdrażającej system KD — po fizycznym zamontowaniu wszystkich elementów systemu (kontrolerów, central, terminali i interfejsów) i zestawieniu wszystkich połączeń. Następnie powinna być przekazana do eksploatacji finalnemu użytkownikowi systemu, który będzie z niej korzystał na co dzień.

Celem niniejszej instrukcji jest zaprezentowanie możliwości aplikacji PR Master z podziałem na zadania wykonywane przez instalatora oraz użytkowników końcowych. Oczywiście podział ten ma charakter umowny. Może się zdarzyć, że po awarii, wymianie komputera, utracie kopii zapasowej lub wystąpieniu innych zdarzeń tego rodzaju, użytkownik końcowy pokusi się o samodzielne skonfigurowanie systemu. Wtedy najlepiej sięgnąć do rozdziału 1. „Przygotowanie systemu do pracy” i wykonać wszystkie omówione tam czynności. Specyficznym przypadkiem przygotowywania systemu do pracy jest aktualizacja programu PR Master ze starszej do nowszej wersji. W takiej sytuacji konieczne jest zadbanie o zachowanie danych z wersji poprzedniej.

W ramach systemu RACS 4 możliwe jest dodatkowo stosowanie programu Remote Monitor na różnych stanowiskach komputerowych. Program Remote Monitor łącząc się przez sieć z programem PR Master umożliwia np. dodawanie użytkowników do systemu RACS 4. Dzięki zastosowaniu Remote Monitora możliwe jest więc uzyskanie z pewnymi ograniczeniami wielostanowiskowego funkcjonowania systemu RACS 4.

Instrukcję podzielono na 5 rozdziałów.

W **rozdziale 1.** „Przygotowanie systemu do pracy" omówiono proces instalacji systemu oraz jego wstępną konfigurację.

W **rozdziale 2.** „Eksploatacja systemu" omówiono typowe zadania wykonywane podczas korzystania z systemu, a zatem definiowanie użytkowników i grup, harmonogramów, stref alarmowych, monitorowanie zdarzeń, tworzenie raportów itp.

W **rozdziale 3.** „Opis funkcji systemu" zamieszczono syntetyczne zestawienie wszystkich menu i poleceń systemu, opis okien dialogowych oraz alternatywnych sposobów wywoływania poszczególnych funkcji.

W **rozdziale 4.** „Monitorowanie" opisano tryb monitorowania systemu PR Master.

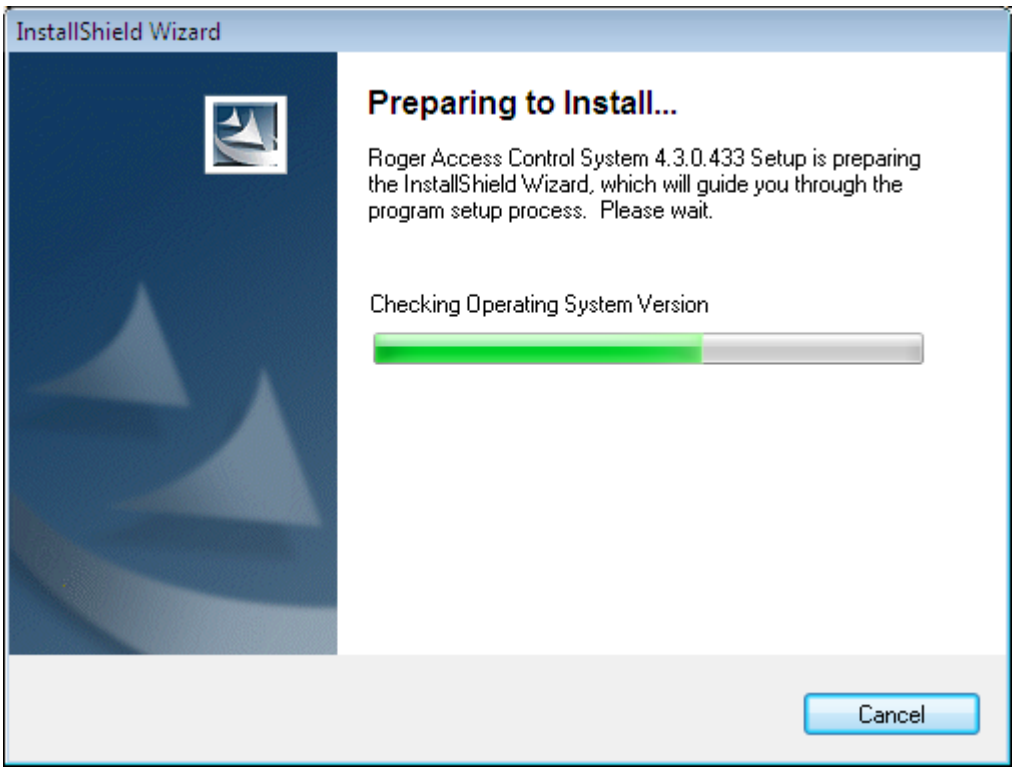
W **rozdziale 5.** „Oprogramowanie Remote Monitor" opisano oprogramowanie dodatkowe systemu RACS 4.

Uzupełnieniem niniejszej instrukcji są instrukcje instalacyjne poszczególnych kontrolerów oraz instrukcje **Opis funkcjonalny kontrolerów serii PRxx2** i **Opis funkcjonalny kontrolerów serii PRxx1**. Wszystkie dostępne integracje systemu RACS 4 zostały opisane w dedykowanych instrukcjach.

ROZDZIAŁ 1.
PRZYGOTOWANIE SYSTEMU DO PRACY

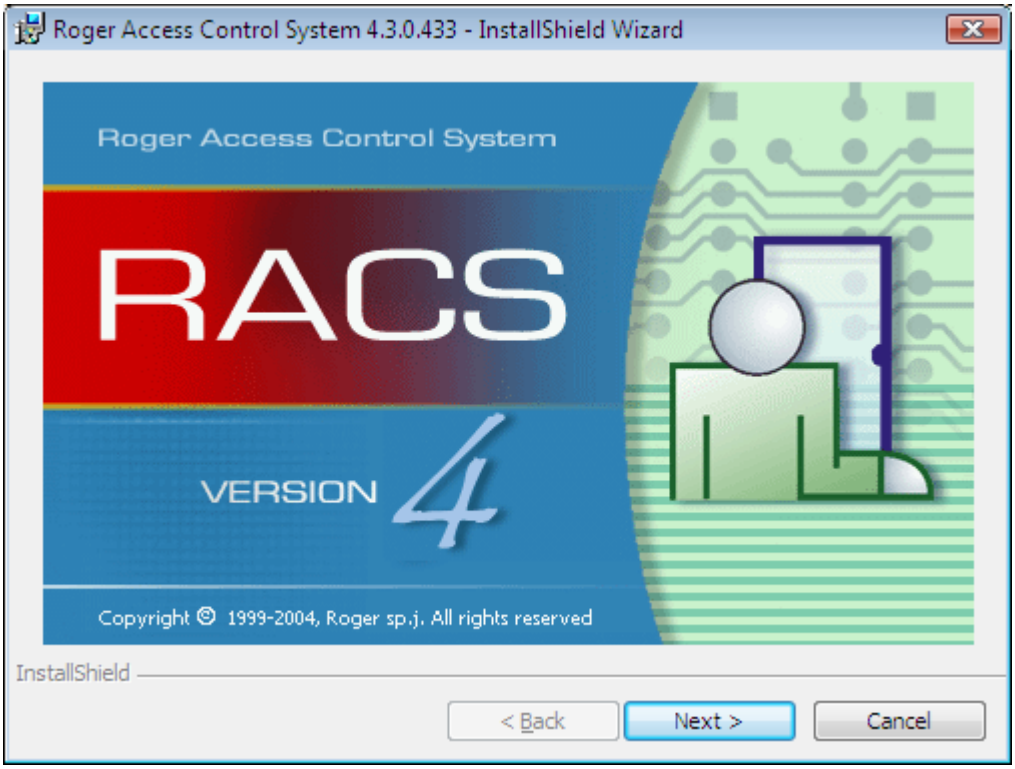
1.1. INSTALACJA PROGRAMU PR MASTER

Aby zainstalować program PR Master, należy pobrać archiwum z programem instalacyjnym z witryny internetowej firmy Roger (**http://www.roger.pl/**). Archiwum znajduje się w pliku o nazwie postaci **PRMaster 4.x.x.xxxx setup.exe**. Po pobraniu pliku, należy go uruchomić, co spowoduje wyświetlenie okna przygotowania instalacji (rysunek 1.1).



Rysunek 1.1. *Przygotowanie instalacji*

Następnie wyświetli się ekran początkowy kreatora instalacji systemu RACS 4 (rysunek 1.2).

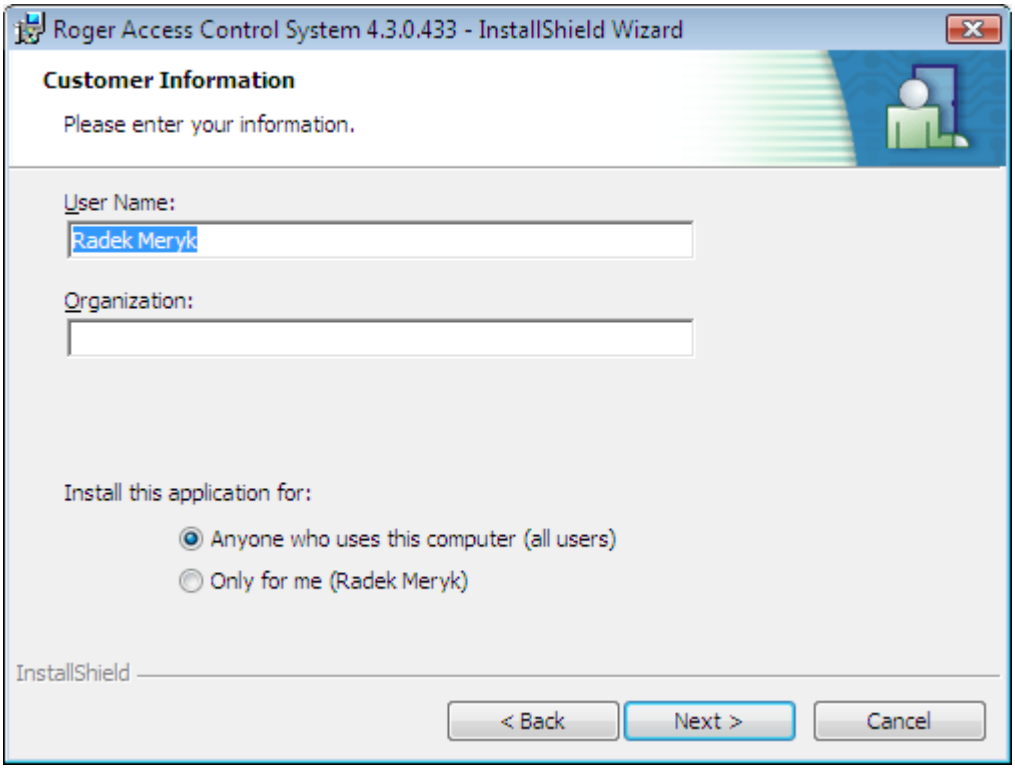


Rysunek 1.2. *Kreator instalacji systemu RACS 4 — krok 1*

W tym oknie klikamy **Next**. Wyświetli się kolejne okno kreatora — ekran powitalny z informacją o prawach autorskich. W tym oknie także należy kliknąć **Next**.

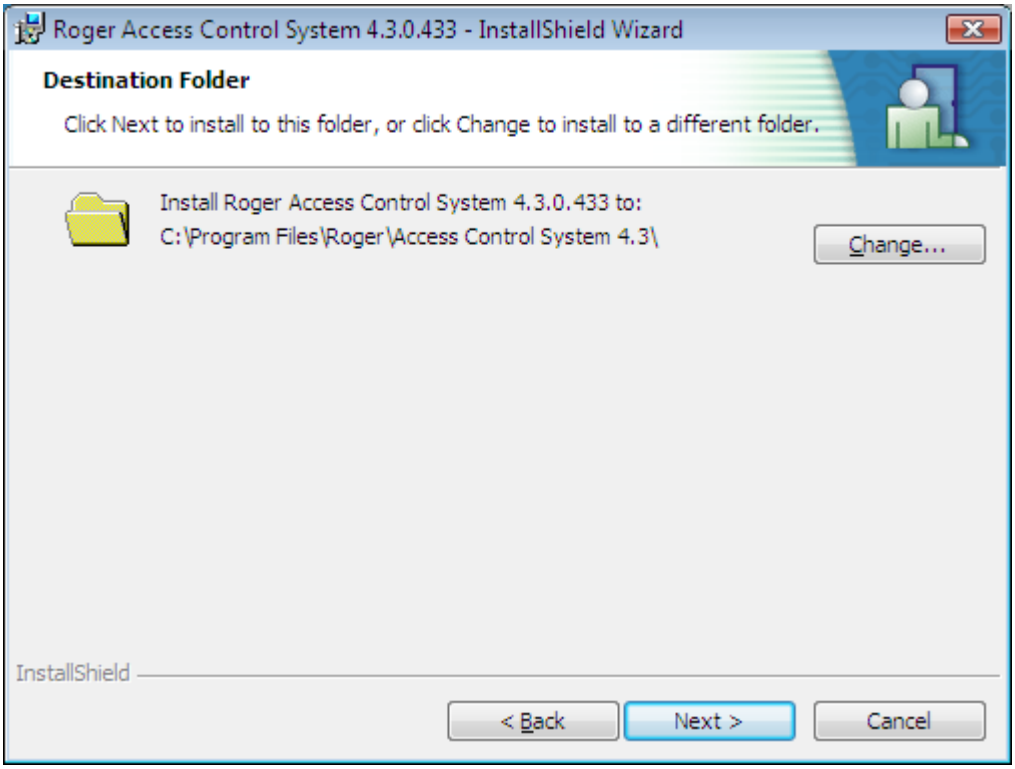
Kolejne okno kreatora to ekran z warunkami licencji. Należy zapoznać się z nią i zaznaczyć opcję **I accept the terms in the license agreement**. Bez zaznaczenia tej opcji przycisk **Next** będzie nieaktywny i nie można będzie kontynuować instalacji. Po zapoznaniu się z warunkami licencji można kliknąć Next i przejść do dalszych działań instalacyjnych.Kolejne okno kreatora zawiera plik **README**. Należy się z nim uważnie zapoznać i kliknąć **Next**.

Wyświetli się następne okno kreatora (rysunek 1.3), w którym należy podać imię i nazwisko użytkownika (pole **User Name**) oraz jego firmę (pole **Organization**). Tak, jak dla większości aplikacji Windows można również wskazać, czy aplikacja ma być zainstalowana tylko dla bieżącego użytkownika (opcja **Only for me**), czy też dla wszystkich użytkowników komputera (**Anyone who uses this computer (all users)**).



Rysunek 1.3. *Kreator instalacji systemu RACS 4 — dane użytkownika*

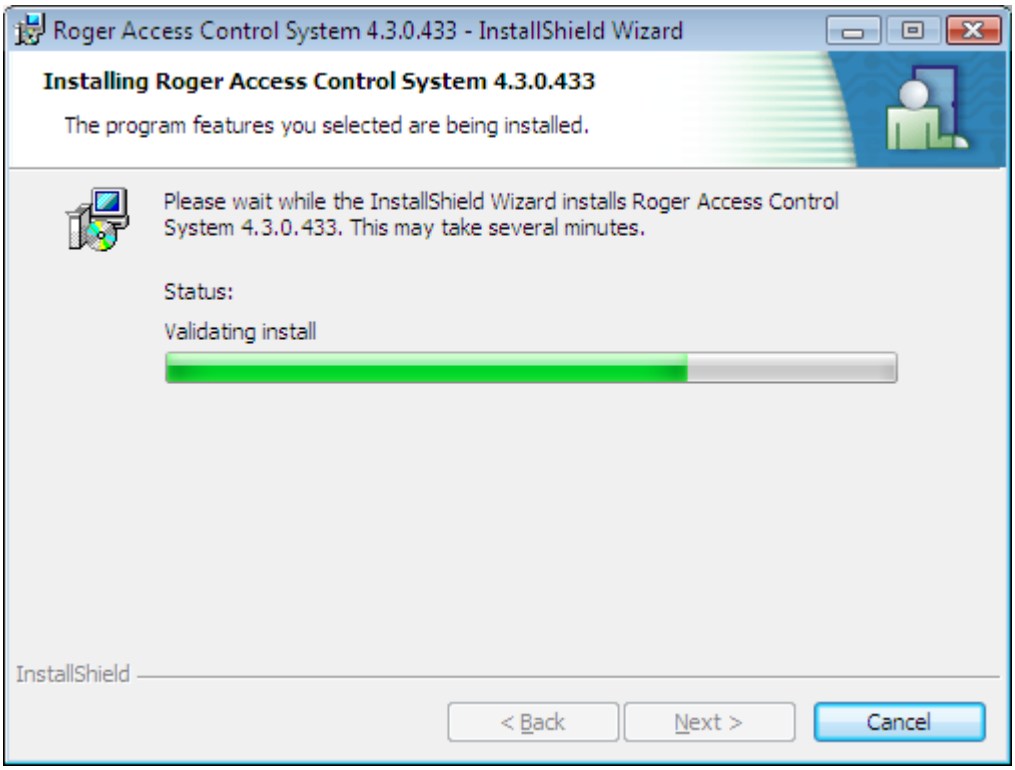
Po wprowadzeniu tych danych klikamy **Next**. Wyświetli się okno wyboru folderu instalacji (rysunek 1.4).



Rysunek 1.4. *Kreator instalacji systemu RACS 4 — wybór folderu instalacji*

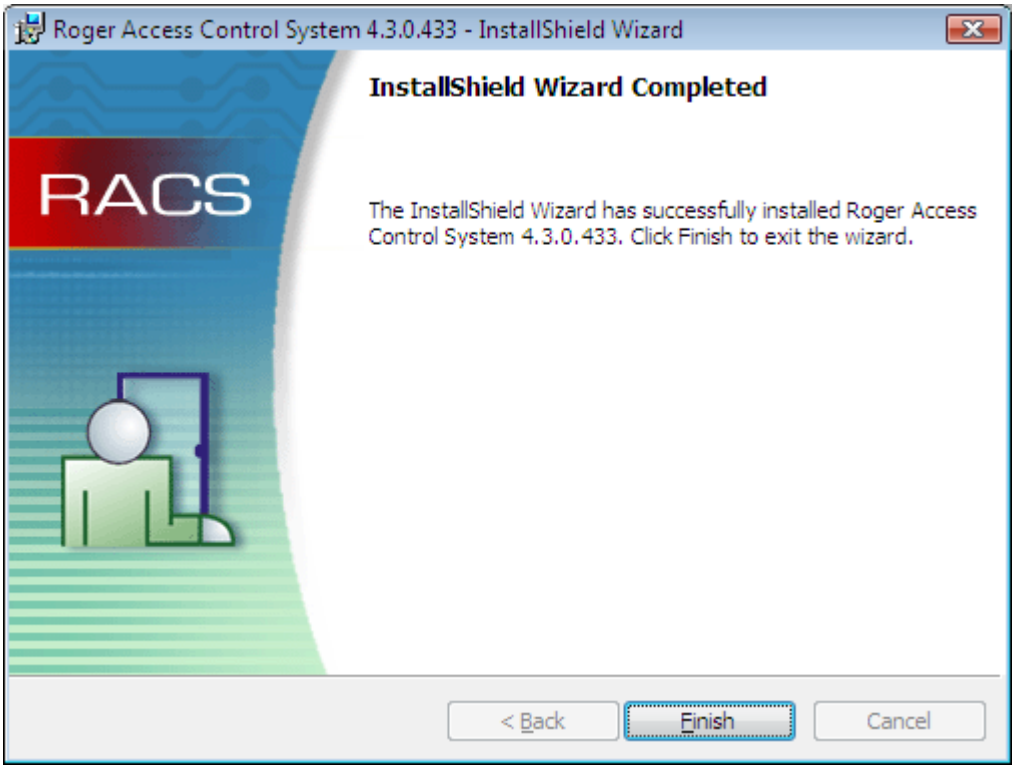
Domyślnie program PR Master instaluje się w katalogu **C:\Roger\Access Control System 4.5**. Aby zmienić tę lokalizację, można skorzystać z przycisku **Change**.

Po wprowadzeniu folderu instalacji klikamy przycisk **Next**. Rozpocznie się proces kopiowania plików, po którym system przeprowadzi weryfikację poprawności instalacji (rysunek 1.5)



Rysunek 1.5. *Kreator instalacji systemu RACS 4 — kopiowanie plików i weryfikacja instalacji*

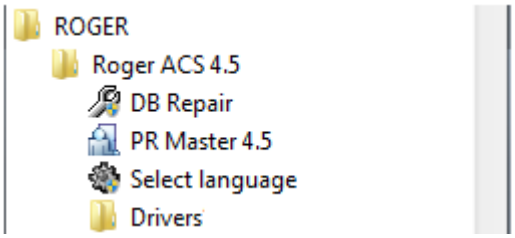
Po zakończeniu tego procesu, jeśli wszystko przebiegnie pomyślnie, wyświetli się okno z informacją o sukcesie instalacji (rysunek 1.6).



Rysunek 1.6. *Kreator instalacji systemu RACS 4 — instalacja zakończona sukcesem*

1.1.1. Zawartość grupy aplikacji Roger ACS 4.5

Zainstalowanie programu PR Master powoduje utworzenie grupy programów **Roger ACS 4.5**. Jej zawartość pokazano na rysunku 1.7.



Rysunek 1.7. *Zawartość grupy programów Roger ACS 4.5*

Grupa programów **Roger ACS 4.5** zawiera następujące elementy:

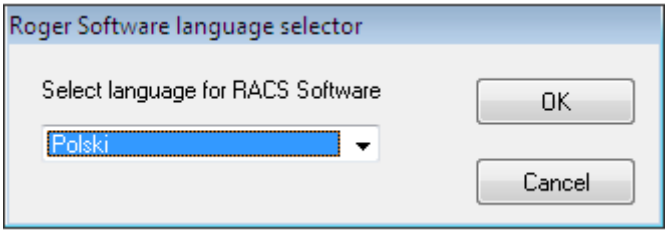
- **PR Master 4.5** — aplikacja PR Master
- **Repair database indexes** — narzędzie do naprawiania indeksów w bazie danych.
- **Select language** — narzędzie do zmiany wersji językowej programu PR Master. Niektóre wersje językowe mogą wymagać licencji. Wersja polska oraz angielska nie podlegają licencjonowaniu.
- **Drivers** – grupa sterowników do interfejsu komunikacyjnych USB-RS485

Jeśli aplikacja PR Master była wcześniej używana na komputerze, na którym przeprowadzamy instalację, to przed uruchomieniem instalatora, a po odinstalowaniu aplikacji, najlepiej usunąć ręcznie katalog z pozostałymi plikami. Najczęściej ścieżka do tego katalogu to **C:\Program Files\Roger\Access Control System 4.5** lub **C:\Roger\Access Control System 4.5**

Usunięcie wszystkich plików z poprzedniej instalacji da nam pewność, że po zainstalowaniu będziemy mieli „czystą" kopię systemu.

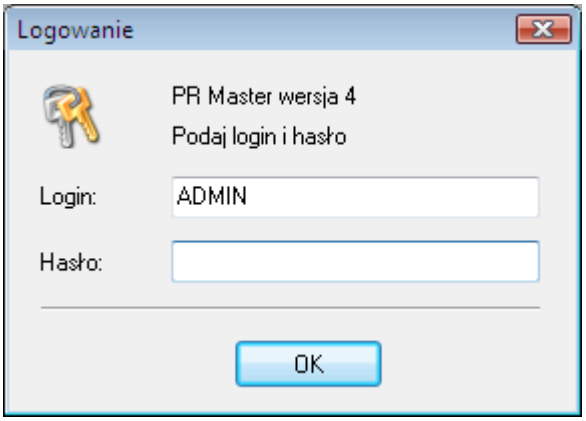
1.2. PIERWSZE URUCHOMIENIE PROGRAMU

Po zainstalowaniu, przy pierwszym uruchomieniu programu PR Master, wyświetla się okno wyboru języka (rysunek 1.8)



Rysunek 1.8. *Wybór języka dla programu PR Master*

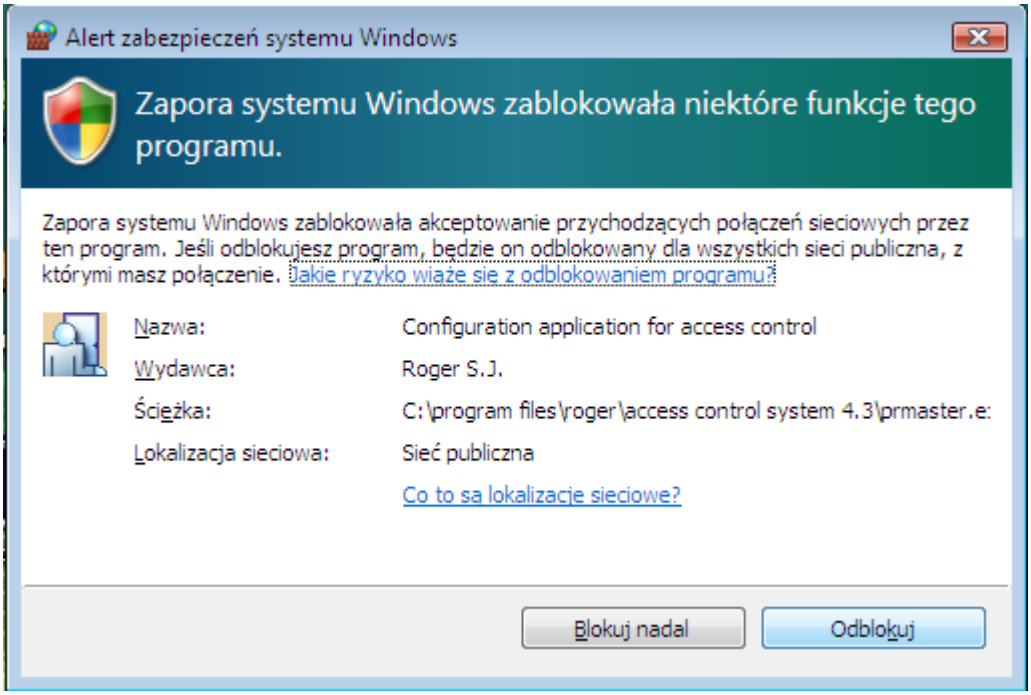
W tym oknie należy wskazać język interfejsu użytkownika i kliknąć **OK**. Wyświetli się jeszcze okno z potwierdzeniem, w którym również należy kliknąć **OK**. Następnie wyświetli się okno informacyjne zawierające listę komponentów systemu, dla których zmieniono ustawienia języka. W nim również należy kliknąć **OK**. Dopiero teraz wyświetla się początkowy ekran logowania systemu PR Master (rysunek 1.9).



Rysunek 1.9. *Ekran logowania programu PR Master*

Domyślnie hasło użytkownika ADMIN jest puste. Klikamy OK. Program wyświetli pytanie, czy wczytać przykładową konfigurację (rysunek 1.10).

Program PR Master może nawiązywać połączenia sieciowe. W związku z tym, w zależności od ustawień zapory firewall systemu Windows, podczas uruchamiania może wyświetlić się okno ostrzegawcze podobne do tego, które pokazano na rysunku 1.11.



Rysunek 1.11. *Zapora systemu Windows informuje o zablokowaniu akceptowania połączeń sieciowych przez program PR Master*

W tym oknie, należy kliknąć **Odblokuj**. Teraz już program PR Master uruchomi się bez przeszkód.

1.3. LISTA PARAMETRÓW PROGRAMU PR MASTER

Program PR Master uruchomiony z różnymi parametrami oferuje dodatkowe niestandardowe funkcjonalności lub inny niestandardowy sposób działania. Lista dostępnych parametrów:

/NOEVDL – po wybraniu polecenia **Konfiguruj system teraz** – patrz **punkt 3.4.4**, program nie pobiera w ogóle zdarzeń tylko od razu zaczyna przesyłać konfigurację do urządzeń.

/MONITOR - po uruchomieniu program przechodzi automatycznie do monitorowania - patrz **rozdział 4**. Gdy w sekcji [Autologin] pliku config.ini podany jest login i hasło operatora to okno logowania jest automatycznie uzupełniane podczas uruchamiania programu.

/AUTOEVENT – program jest uruchamiany jedynie w celu automatycznego pobrania zdarzeń do bazy danych - patrz **punkt 3.4.1** i następnie jest zamykany.

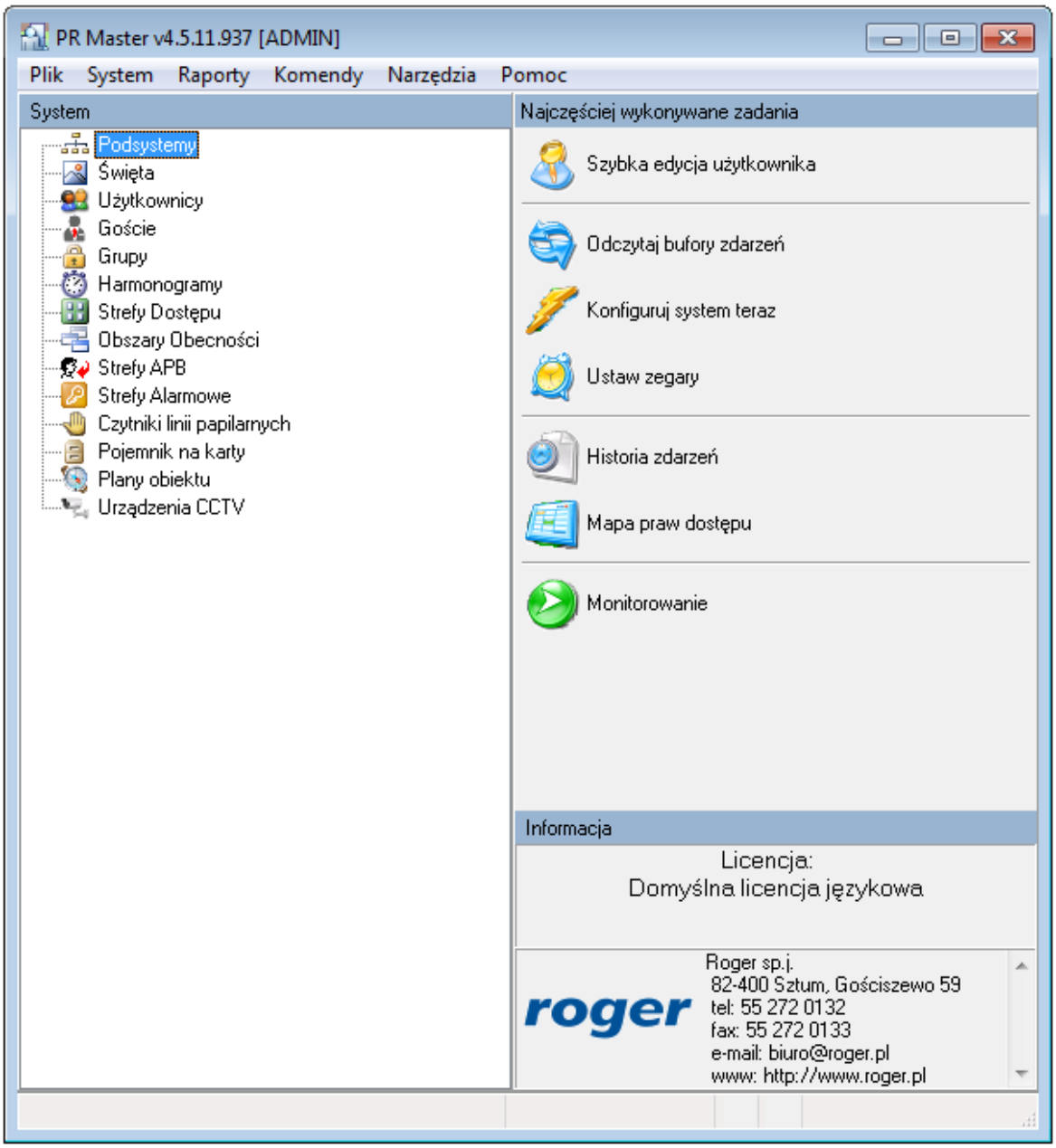
/EVLIMIT=x – parametr umożliwia zwiększenie maksymalnej ilości zdarzeń przetwarzanych przez program z 300 tys. na wartość x - patrz **punkt 3.3.7**

/CPRNETPORT=x – parametr umożliwia zmianę domyślnego i normalnie niekonfigurowalnego portu UDP do komunikacji programu z centralami CPR32-NET na wartość x.

/USE_CPR_PORT – parametr umożliwia programowi rozróżnianie central CPR32-NET nie tylko po ich adresach IP ale dodatkowo też po portach. Dzięki temu możliwa jest obsługa central CPR32-NET za ruterem gdy stosowane jest przekierowywanie portów.

1.4. SZYBKI START

Po uruchomieniu wyświetla się główne okno programu PR Master (rysunek 1.12).



Rysunek 1.12. Główne okno *programu PR Master*

W górnej części okna programu znajduje się główne menu. Z lewej strony wyświetla się drzewo **System**, natomiast z prawej lista najczęściej wykonywanych zadań. Są to trzy sposoby korzystania z poleceń programu PR Master. Sposoby są ze sobą równoważne, choć tylko menu główne daje dostęp do pełnego zakresu funkcji programu.

Aby przygotować system do pracy, należy wykonać następujące czynności:

1. Stwórz czystą bazę danych. W tym celu należy użyć polecenia **Plik**/**Nowy system** (patrz **punkt 3.1.1**).

2. W panelu **System** kliknij ikonę **Podsystemy** lub z menu **System** wybierz polecenie **Podsystemy** (patrz **punkt 3.2.8**).

3. Dodaj nowy podsystem (patrz **punkt 3.2.8.1**). Pamiętaj o nadaniu podsystemowi opisowej nazwy. Jeśli tego nie zrobisz, system domyślnie będzie nadawał podsystemom nazwy Podsystem A, Podsystem B, itd.

4. Dodaj kontrolery do podsystemu (patrz **punkt 3.2.8.4**). Także w tym przypadku pamiętaj o nadaniu kontrolerom opisowych nazw pozwalających na ich późniejszą identyfikację. W tym celu wybierz kontroler, naciśnij przycisk Właściwości i następnie wprowadź opisową nazwę w polu **Nazwa kontrolera**. Dodatkowo możliwe jest nadanie nazw czytnikom kontrolera w tym samym oknie poprzez wybranie zakładki **Terminal ID0** i/lub **Terminal ID1** i wpisanie nazwy w polu **Nazwa czytnika**.

5. Powtórz kroki 1–4 dla pozostałych podsystemów w systemie kontroli dostępu.

6. Kiedy wszystkie podsystemy zostaną skonfigurowane, możesz zdefiniować strefy dostępu. Należy to zrobić w porozumieniu z użytkownikiem końcowym systemu (właścicielem). Informacje na temat sposobu definiowania stref dostępu można znaleźć w **punkcie 3.2.7**.

7. Po zdefiniowaniu stref dostępu zdefiniuj harmonogramy czasowe obowiązujące w systemie. Informacje na ten temat można znaleźć w **punkcie 3.2.6**. Kiedy zdefiniujesz harmonogram zdefiniuj święta w wybranym roku kalendarzowym. Informacje na temat definiowania świąt można znaleźć w **punkcie 3.2.2**.

8. Możesz teraz zdefiniować grupy użytkowników. Zapoznaj się z **punktem 3.2.5**. Przeczytaj dokładnie informacje o związku grup z uprawnieniami dostępu w systemie RACS 4. Określ uprawnienia dostępu dla każdej z grup w poszczególnych strefach dostępu. W tym celu przypisz do poszczególnych stref harmonogramy czasowe. Opisują one przedziały czasu, w których grupa ma uprawnienia w danej strefie.

9. Teraz możesz przejść do wprowadzania użytkowników oraz ich identyfikatorów. Przed przystąpieniem do tej czynności, można zebrać karty zbliżeniowe użytkowników i seryjnie dodać je do Pojemnika na karty. Informacje o sposobie tworzenia Pojemnika na karty znajdziesz w **punkcie 3.2.13**. O sposobie zarządzania użytkownikami możesz przeczytać w **punkcie 3.2.3**.

10. Prześlij ustawienia konfiguracyjne do wszystkich kontrolerów w systemie. W tym celu użyj polecenia **Konfiguruj system teraz** znajdującego się na liście najczęściej wykonywanych zadań z prawej strony okna głównego. Więcej informacji na temat polecenia konfigurowania całego systemu znajdziesz w **punkcie 3.4.4**.

W tym momencie, po przesłaniu ustawień do wszystkich kontrolerów, system jest wstępnie przygotowany do pracy. Nie obejmuje co prawda konfiguracji zaawansowanej (np. obszarów obecności, stref alarmowych, stref APB), ale te czynności można wykonać później i mniejszym nakładem pracy. W związku z tym, teraz należy wykonać kopię zapasową systemu, aby w przypadku błędów, utraty danych, itp. można było odtworzyć podstawowe ustawienia. Warto zadbać o to, aby kopię zapasową zapisać na nośniku zewnętrznym. Dzięki temu będzie ona dostępna także w przypadku awarii dysku. O sposobie wykonywania kopii zapasowej można przeczytać w **punkcie 3.5.12**.

ROZDZIAŁ 2.
UŻYTKOWANIE SYSTEMU

A zatem system RACS 4 został przekazany użytkownikowi końcowemu. Aby można było z niego poprawnie korzystać trzeba wykonać szereg zadań, które po pierwsze zapewnią systemowi bezpieczną pracę, a po drugie pozwolą na maksymalne wykorzystanie jego możliwości. Wszystkie te zadania zostaną opisane w niniejszym rozdziale.

2.1. WSTĘPNE CZYNNOŚCI EKSPLOATACYJNE

2.1.1. Nadanie hasła użytkownikowi ADMIN

Po zainstalowaniu systemu, hasło użytkownika ADMIN jest puste. Ponieważ użytkownik ten ma w programie PR Master nieograniczone prawa, należy zadbać o to, by konto ADMIN było chronione bezpiecznym hasłem.

Aby nadać hasło użytkownika ADMIN:

1. Wybierz polecenie **Narzędzia**/**Operatorzy programu**.
2. Zaznacz użytkownika ADMIN.
3. Kliknij przycisk **Ustaw hasło**. Wyświetli się okno dialogowe **Zmień hasło**.
4. Ponieważ hasło użytkownika ADMIN jest domyślnie puste, pozostaw puste pole **Stare hasło**.
5. W polu **Nowe hasło** wpisz hasło, które ma obowiązywać od tego momentu.
6. Ponownie wpisz hasło w polu **Potwierdź hasło**.

Dla bezpieczeństwa warto zadbać o to, aby hasło było odpowiednio trudne do odgadnięcia. Najlepiej, gdyby nie było to żadne słowo dostępne w słownikach, by zawierało co najmniej jedną cyfrę i jakiś znak — np. **{**, **[**, **)**. Tak nadane hasło należy zapamiętać. Można również je zapisać na kartce papieru, zamknąć w opisanej kopercie i schować w sejfie.

Pod żadnym pozorem nie wolno zapisywać hasła na samoprzylepnej kartce przyklejanej na monitorze.

2.1.3. Zdefiniowanie operatorów programu

W rozbudowanym systemie KD zadania eksploatacyjne mogą być podzielone na kilka osób. W szczególności można wyznaczyć osobę odpowiedzialną za dopisywanie użytkowników oraz inną za wykonywanie kopii zapasowych. Aby osoby te nie miały pełnych uprawnień w systemie KD i by nie mogły zniszczyć konfiguracji, należy zdefiniować dla nich osobne konta. Sposób definiowania kont o ograniczonym dostępie opisano w **punkcie 3.5.8**.

2.1.3. Zdefiniowanie użytkownika INSTALLER

Definiowanie użytkownika **Instalator** ma sens jedynie wtedy gdy w systemie RACS 4 są wykorzystywane kontrolery serii PRxx1. Jedynie w przypadku tej serii kontrolerów standardowych możliwe jest wejście do trybu programowania instalatora i następnie ręczna konfiguracja kontrolerów za pomocą poleceń z klawiatury – patrz instrukcja **Opis funkcjonalny kontrolerów serii PRxx1**.

Użytkownik INSTALLER ma uprawnienia do wejścia w tryb programowania instalatora w odniesieniu do kontrolerów serii PRxx1, ale nie posiada uprawnień do otwierania drzwi. Ten specjalny użytkownik nie ma przypisanego numeru ID, więc nie jest widoczny na liście użytkowników. Aby zdefiniować w systemie użytkownika INSTALLER, należy skorzystać z polecenia **System**/**Instalator**. Więcej informacji na ten temat można znaleźć w **punkcie 3.2.1**.

2.1.4. Opracowanie harmonogramu wykonywania kopii zapasowych

System kontroli dostępu jest obiektem dynamicznym, w którym bardzo szybko zachodzi wiele zdarzeń. W związku z tym, warto zadbać o to, by często były wykonywane kopie zapasowe. Dzięki nim, w przypadku awarii, można odtworzyć zdarzenia i konfigurację systemu. Ponieważ przy rozbudowanej bazie danych wykonanie pełnej kopii zapasowej może zająć sporo czasu, można tak skonfigurować wykonywanie kopii zapasowych, aby system robił to automatycznie w czasie najmniejszego obciążenia systemu. Szczegółowy sposób definiowania takiego harmonogramu kopii zapasowych opisano w **punkcie 3.5.12**.

Zaleca się regularne tworzenie kopii zapasowych konfiguracji systemu RACS 4 gdyż nie jest możliwe odzyskanie takiej konfiguracji z urządzeń RACS 4 w przypadku awarii komputera z programem PR Master.

2.1.5. Opracowanie harmonogramu przesyłania ustawień do systemu

System RACS 4 składa się z części kontrolującej przejścia (kontrolerów, central i połączeń) oraz części zarządzającej (programu PR Master). Są to komponenty, które muszą zawierać zgodne ustawienia. Tylko wtedy mogą ze sobą dobrze współdziałać. Ponieważ urządzenia techniczne mogą podlegać awariom, zakłóceniom lub ingerencji osób trzecich, a w programie mogą być modyfikowane ustawienia, należy zadbać o to, aby co jakiś czas system automatycznie się synchronizował. Taka synchronizacja polega na przesłaniu do systemu wszystkich ustawień wprowadzonych w programie PR Master. Ponieważ przy rozbudowanym systemie kontroli dostępu przesyłanie ustawień może zajmować dużo czasu, można tak je skonfigurować, aby system robił to automatycznie w czasie najmniejszego obciążenia. Szczegółowy sposób definiowania harmonogramu przesyłania konfiguracji systemu opisano w **punkcie 3.4.5**.

2.1.6. Opracowanie harmonogramu odczytywania buforów zdarzeń

W systemie RACS 4 zdarzenia są rejestrowane na bieżąco i przez cały czas, niezależnie od tego, czy aplikacja PR Master działa, czy nie i niezależnie od tego, w jakim trybie pracuje. Jeśli program PR Master nie działa w trybie monitorowania, to zdarzenia są gromadzone w buforach kontrolerów oraz centrali CPR32-SE/CPR32-NET (o ile system jest w nie wyposażony). Odczytanie buforów zdarzeń następuje na żądanie oraz każdorazowo przy przejściu do trybu monitorowania. Aby nie dopuścić do zbyt dużych rozbieżności pomiędzy zawartością bazy danych, a zdarzeniami zarejestrowanymi na bieżąco w systemie KD, można skonfigurować harmonogram wykonywania odczytu buforów zdarzeń. W tym celu można skorzystać z polecenia **Komendy**/**Odczytaj bufory zdarzeń później**. Polecenie to opisano szczegółowo w **punkcie 3.4.2**.

2.2. ZAAWANSOWANE CZYNNOŚCI EKSPLOATACYJNE

Do zaawansowanych czynności eksploatacyjnych można zaliczyć:

- konfigurację funkcji Anti-Passback,
- definiowanie obszarów obecności,
- definiowanie stref alarmowych.
- definiowanie planów obiektu.

Zagadnienia te zostaną opisane w poniższych punktach.

2.2.1. Konfigurowanie mechanizmu Anti-passback

System kontroli dostępu ma wiele możliwości kontrolowania przejść w zarządzanych obiektach. Pozwala on między innymi na zablokowanie możliwości przekazywania kart zbliżeniowych (np. przez okno), po to by mogły być wykorzystane przez osoby nieuprawnione. Do tego celu służy funkcja Anti-Passback. Jeśli się ją skonfiguruje, użytkownik nie będzie mógł dwa razy wejść do strefy APB, jeśli wcześniej z niej nie wyszedł. Więcej informacji na temat definiowania stref APB oraz konfigurowania tej funkcji w systemie RACS 4 można znaleźć w **punkcie 3.2.10**.

2.2.2. Definiowanie obszarów obecności

Obszary obecności to jeden z mechanizmów systemu RACS 4 pozwalający na kontrolowanie miejsca przebywania użytkownika w obiekcie. Obszar obecności należy rozumieć jako fragment obszaru kontrolowanego przez system kontroli dostępu, do którego można wejść poprzez wskazaną grupę punktów identyfikacyjnych oraz wyjść przez odrębną grupę punktów identyfikacyjnych.

Obszary obecności definiuje się w celu sporządzania raportów obecności (**Raporty**/**Obecności**), które z kolei można wykorzystać do uproszczonej rejestracji czasu pracy. **Raport obecności** pokazuje godzinę wejścia/wyjścia użytkownika do/z obszaru oraz łączny czas jego przebywania w obszarze. Można również sporządzić raport informujący o tym, kto wchodził jako pierwszy do danego obszaru i jako ostatni z niego wychodził w zdefiniowanym zakresie czasowym. Szczegółowy sposób definiowania obszarów obecności zamieszczono w **punkcie 3.2.9**.

2.2.3. Definiowanie stref alarmowych

Strefy alarmowe pozwalają na wskazanie grupy kontrolerów, które będą współbieżnie przezbrajane np. zgodnie z ustalonym harmonogramem. Można również stworzyć hierarchię stref alarmowych. Dzięki temu będą one przezbrajane w określonym porządku, zgodnie z zasadami podrzędności lub nadrzędności.

Więcej informacji na temat szczegółów definiowania stref alarmowych w programie PR Master można znaleźć w **punkcie 3.2.11**.

2.2.4. Definiowanie planów obiektów

Plany obiektu to narzędzie umożliwiające graficzne monitorowanie kontrolowanego obiektu. Dzięki tej własności użytkownik może umieścić na rzucie pięter lub planie obiektu ikony kontrolerów, a potem oglądać je w trybie graficznym. Począwszy od wersji 4.3.3.522, PR Master pozwala na zdefiniowanie do 20 rozłącznych planów. Po zdefiniowaniu można je później wyświetlać w trybie monitorowania. Więcej informacji na temat definiowania i korzystania z planów obiektu, można znaleźć w **punkcie 3.2.14**.

2.3. CODZIENNA EKSPLOATACJA SYSTEMU

System kontroli dostępu po dokładnym wstępnym skonfigurowaniu, zdefiniowaniu wszystkich ustawień, praw, stref i opcji, staje się systemem ustabilizowanym, w którym wykonuje się tylko kilka rodzajów operacji. Jest ich znacznie mniej w porównaniu z fazą wdrażania, kiedy trzeba skonfigurować wszystkie elementy. Do codziennych zadań eksploatacyjnych w programie PR Master należą:

- zarządzanie użytkownikami — wprowadzanie nowych użytkowników, usuwanie użytkowników, zmiana przyporządkowania do grup.
- wykonywanie kopii zapasowych.
- monitorowanie.

Czynności te zostały opisane w poniższych punktach.

2.3.1. Zarządzanie użytkownikami

Do zarządzania użytkownikami służy kartoteka użytkowników. Można ją wywołać z panelu **System** w lewej części głównego okna PR Master, albo wybrać polecenie **Użytkownicy** z menu **System**. Można również skorzystać z polecenia **Szybka edycja użytkowników** z menu **Narzędzia** lub z panelu **Najczęściej wykonywane zadania**. Funkcja **Szybka edycja użytkowników** jest również dostępna w trybie monitorowania (w menu **Narzędzia**).

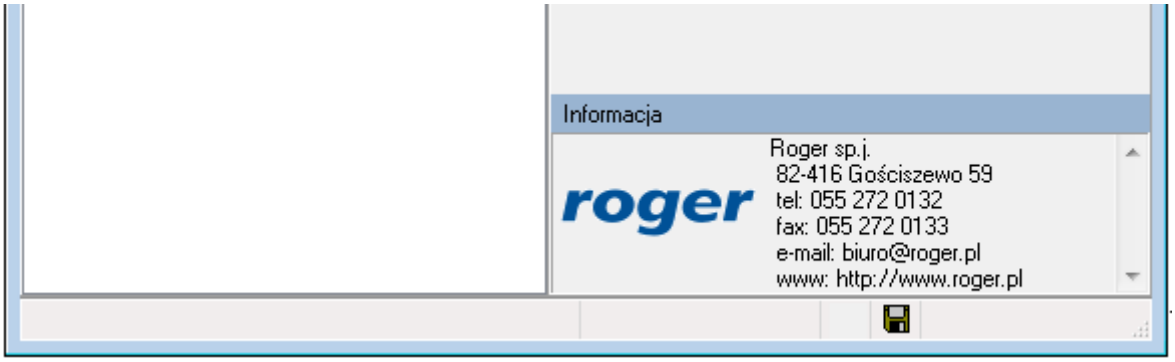
Każdorazowa zmiana właściwości użytkownika — tzn. zmiana przydziału do grupy, wymiana karty zbliżeniowej, czy kodu PIN wymaga przesłania danych do kontrolerów. Podstawowa różnica pomiędzy posługiwaniem się kartoteką użytkowników wywoływaną z menu **System**, a funkcją **Szybka edycja użytkowników** polega na zakresie przesyłania informacji do kontrolerów. W pierwszym przypadku do kontrolerów przesyłane są wszystkie ustawienia, w tym ustawienia użytkowników natomiast w drugim przypadku przesyłane są jedynie dane użytkownika. W związku z tym pierwsza metoda jest bardziej czasochłonna w porównaniu do drugiej.

Sposób posługiwania się kartoteką użytkowników opisano w **punkcie 3.2.3**, natomiast funkcję **Szybka edycja użytkowników** opisano w **punkcie 3.5.2**.

2.3.2. Wykonywanie kopii zapasowych

Baza danych programu PR Master zawiera dużo danych. Ewentualna ich utrata i konfigurowanie systemu od początku, zwłaszcza w przypadku rozbudowanego systemu kontroli dostępu może zajmować bardzo dużo czasu. W związku z tym, należy dbać o to, by często były wykonywane kopie zapasowe.

Program PR Master posiada mechanizm, który informuje o tym, że w systemie zaszły zmiany. Jest to ikona dyskietki na pasku stanu w głównym oknie programu PR Master (rysunek 2.1). Pojawienie się takiej ikony jest sygnałem, że konfiguracja się zmieniła i że warto wykonać kopię zapasową.



Rysunek 2.1. *Ikona dyskietki na pasku stanu informuje o potrzebie wykonania kopii zapasowej*

Szczegółowy sposób definiowania harmonogramu wykonywania kopii zapasowych opisano w **punkcie 3.5.12**.

2.3.3. Monitorowanie systemu

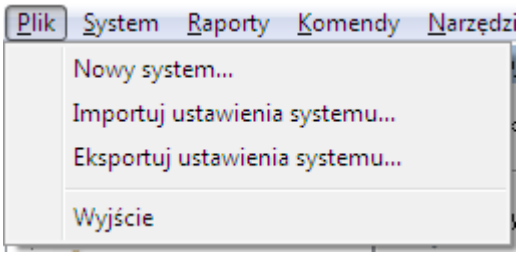
System PR Master ma dwa zasadnicze tryby pracy: definiowania konfiguracji oraz monitorowania. Tryb definiowania konfiguracji, jak łatwo odgadnąć służy do wprowadzania szeregu czynności konfiguracyjnych, natomiast tryb monitorowania pozwala na obserwację tego, co dzieje się w systemie. Zwykle tę funkcje wykorzystuje się na co dzień, w stabilnym i skonfigurowanym systemie kontroli dostępu. Aby wywołać funkcję **Monitorowanie**, można kliknąć ikonę **Monitorowanie** w panelu **Najczęściej wykonywane zadania** lub wybrać polecenie **Monitorowanie** z menu **Narzędzia**.

Tryb monitorowania programu PR Master został szczegółowo opisany w **rozdziale 4**.

ROZDZIAŁ 3.
OPIS FUNKCJI SYSTEMU

3.1. MENU PLIK

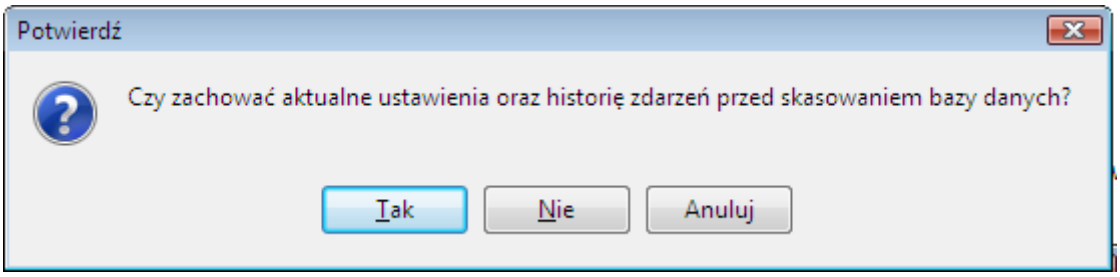
Menu **Plik** pokazano na rysunku 3.1.



Rysunek 3.1. *Menu Plik*

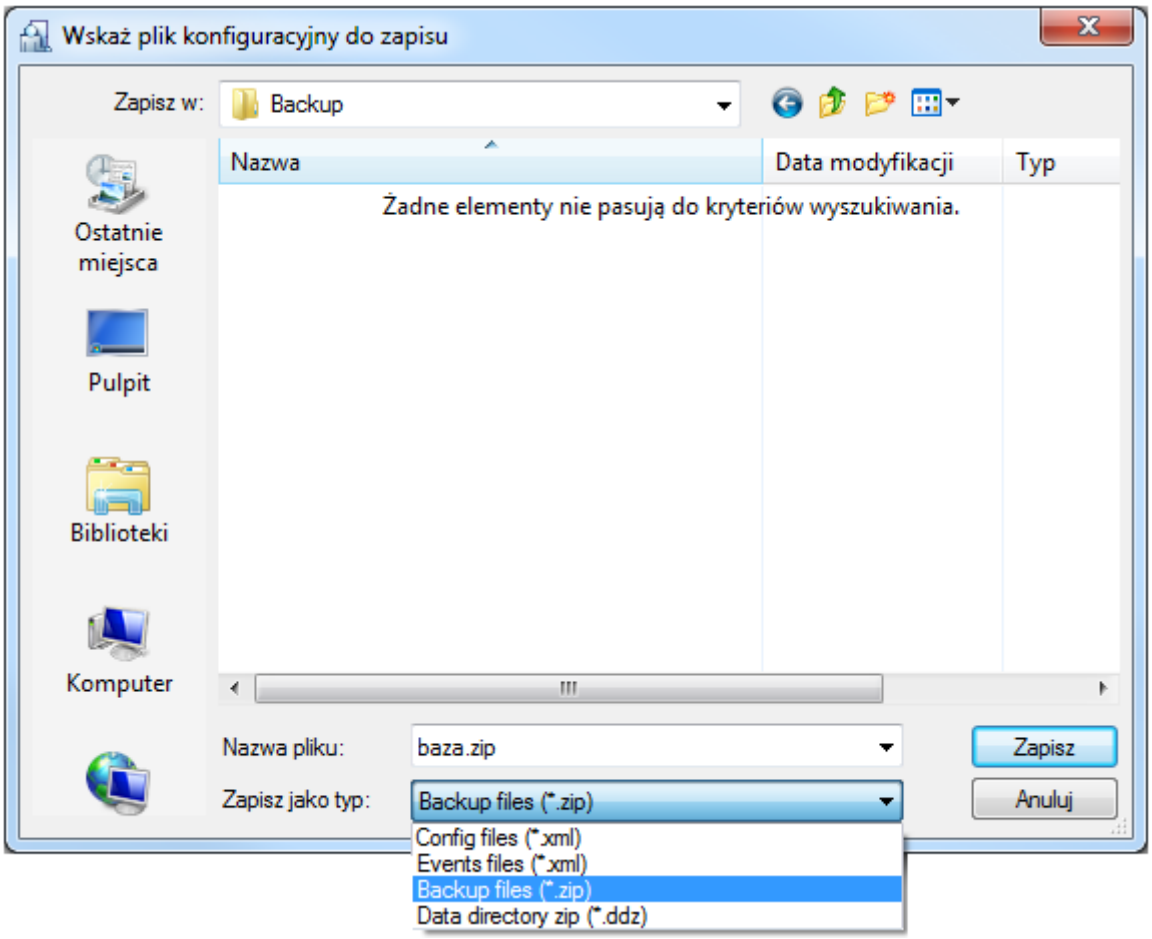
3.1.1. Polecenie Nowy System...

Polecenie **Nowy System...** służy do zerowania zawartości bazy danych. Wykonuje się je w celu zdefiniowania nowego systemu od podstaw. Wybranie polecenia spowoduje wyświetlenie okna dialogowego pokazanego na rysunku 3.2.



Rysunek 3.2. *Potwierdzenie zamiaru wyzerowania bazy danych*

Odpowiedź **Tak** na to pytanie spowoduje wyświetlenie okna dialogowego, w którym można wskazać plik, gdzie ma być zapisana kopia zapasowa aktualnej bazy danych (rysunek 3.3). Użytkownik może zapisać ustawienia systemu i zdarzenia systemowe w formacie skompresowanym **Backup files (*.zip**), wyeksportować cały folder bazy danych **Data directory zip (*.ddz)**, jedynie ustawienia systemu **Config files (*.xml)** lub też jedynie zdarzenia systemowe (**Events files (*.xml)**).



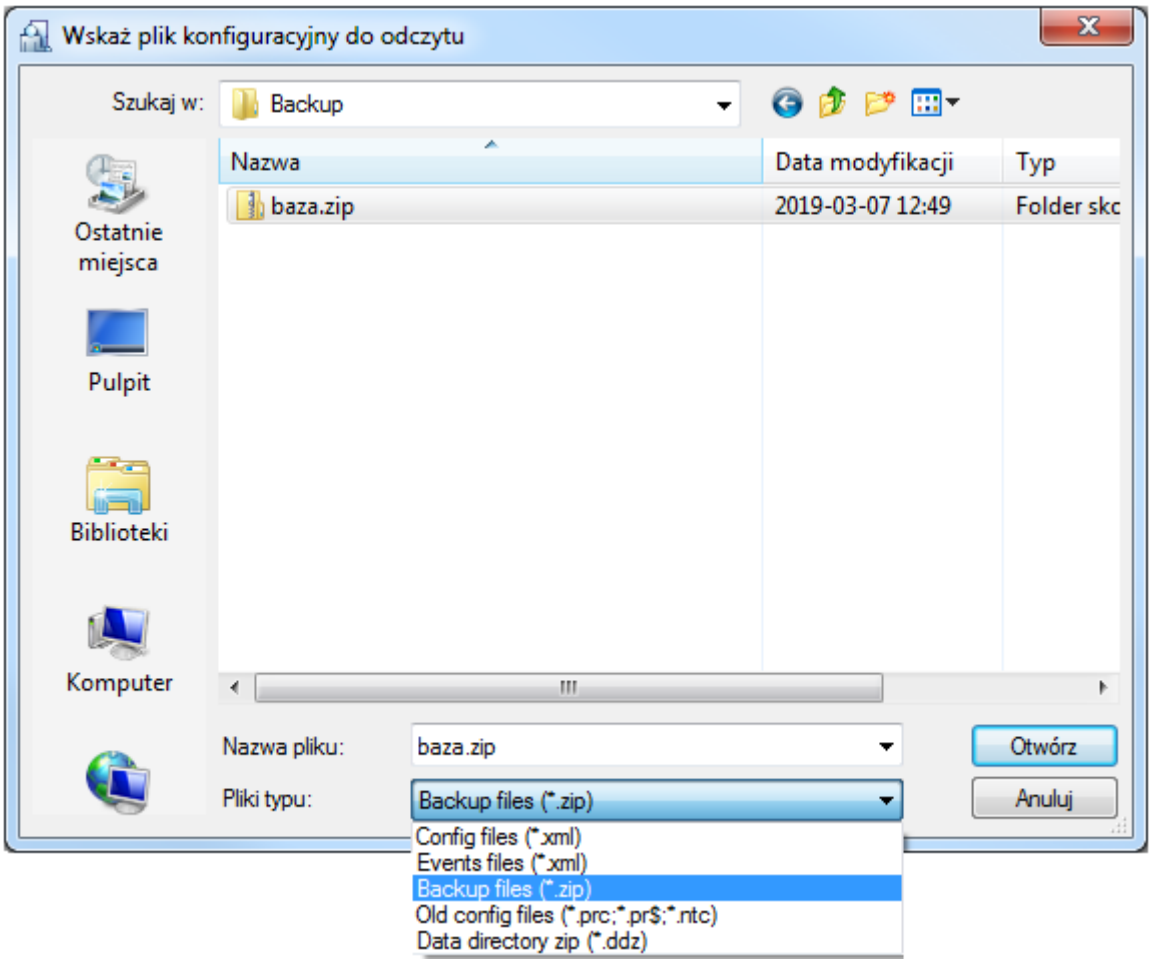
Rysunek 3.3. *Wybór pliku, w którym będą zapisane ustawienia systemu*

Uruchomienie polecenia **Nowy System...** bez zapisania bieżących ustawień spowoduje utratę wszystkich danych, które były dotychczas zapisane w bazie danych — znikną dane o podsystemach, kontrolerach, harmonogramach, użytkownikach, zdarzeniach itp. W celu ochrony własnej pracy zaleca się zachowanie ostrożności podczas korzystania z tej funkcji oraz częste wykonywanie kopii zapasowych.

Po wykonaniu polecenia **Nowy System...** baza danych jest pusta. Można to zaobserwować w oknie głównym programu PR Master — nie ma w nim poprzednio wpisywanych danych.

3.1.2. Polecenie Importuj ustawienia systemu...

Polecenie **Importuj ustawienia systemu...** pozwala na import wcześniej zapisanej konfiguracji i zdarzeń. Po wybraniu tego polecenia wyświetla się okno wyboru pliku do zaimportowania (rysunek 3.4.)



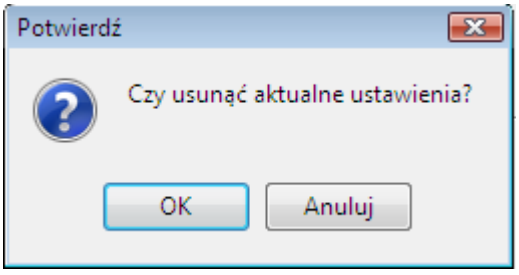
Rysunek 3.4. *Wybór pliku do zaimportowania danych*

Użytkownik ma do wyboru następujące formaty plików, z których mogą być importowane dane:

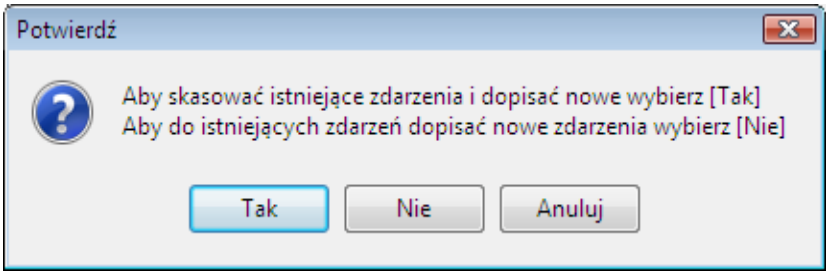
- plik konfiguracji (**Config files (*.xml)**);
- plik zdarzeń (**Events files (*.xml)**);
- plik konfiguracji i zdarzeń (**Backup files (*.zip)**);
- plik bazy danych **(Data directory zip (*.ddz)**;
- plik konfiguracyjny pochodzący ze starszych wersji (**Old config files (*.prc; *.pr$; *.rtc)**).

W zależności od wybranego formatu, system zadaje różne pytania o potwierdzenie dalszych działań związanych z importem (rysunek 3.5).

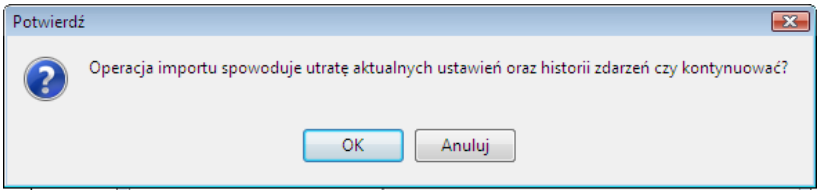
A — pliki konfiguracyjne



B — pliki zdarzeń



C — pliki kopii zapasowych lub pliki konfiguracyjne starszych wersji



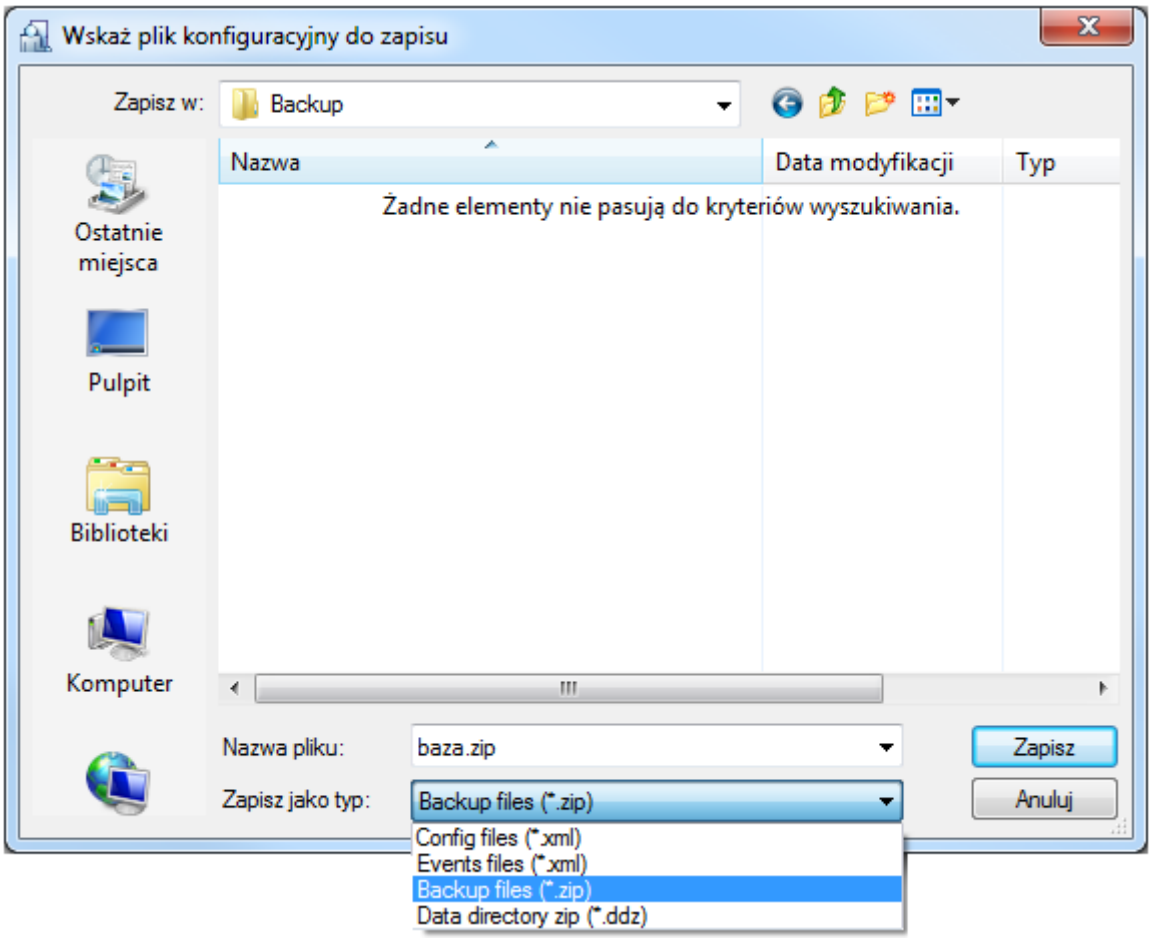
Rysunek 3.5. *Pytania o potwierdzenie zamiaru importowania danych*

W zależności od wybranej opcji system odpowiednio zaimportuje wskazane informacje. W czasie wykonywania operacji importu wyświetla się wskaźnik postępu.

Zaimportowanie danych z pliku zewnętrznego powoduje trwałą zmianę zawartości bazy danych. Przed skorzystaniem z tej funkcji warto wykonać kopię zapasową bieżącej zawartości bazy danych tak, by w przypadku niepowodzenia importu można było wrócić do poprzednich danych.

3.1.3. Polecenie Eksportuj ustawienia systemu...

Polecenie **Eksportuj ustawienia systemu...** pozwala na eksport bieżącej konfiguracji, zdarzeń lub całej zawartości bazy danych do pliku zewnętrznego. Po wybraniu tego polecenia wyświetla się okno wyboru pliku, do którego mają być wyeksportowane dane (rysunek 3.6.)

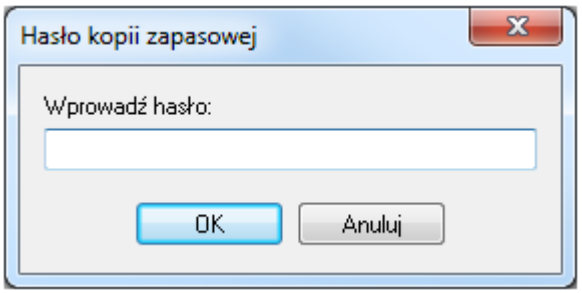


Rysunek 3.6. *Wybór pliku do wyeksportowanie ustawień*

Użytkownik ma do wyboru następujące formaty plików, do których można eksportować dane:

- plik konfiguracji (**Config files (*.xml)**);
- plik zdarzeń (**Events files (*.xml)**);
- plik konfiguracji i zdarzeń (**Backup files (*.zip)**);
- plik bazy danych **(Data directory zip (*.ddz)**;

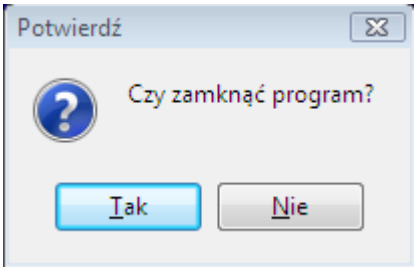
W przypadku wybrania pliku konfiguracji i zdarzeń jak też pliku bazy danych, system pozwala na wprowadzenie opcjonalnego hasła, które będzie chroniło plik przed dostępem osób niepowołanych (rysunek 3.7).



Rysunek 3.7. *Wprowadzanie hasła do ochrony pliku archiwum z kopią zapasową bazy danych*

3.1.4. Polecenie Wyjście

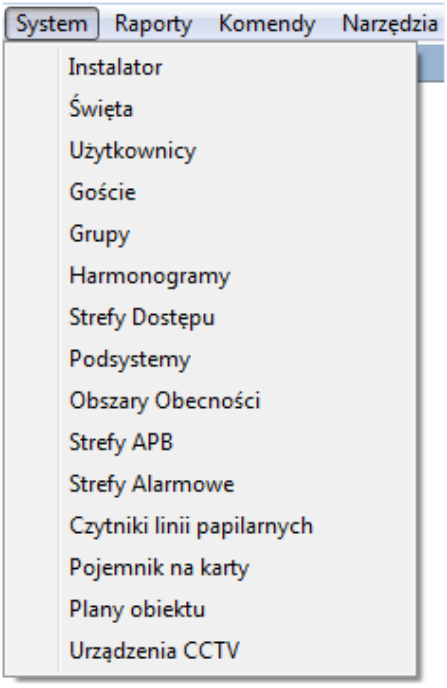
Polecenie **Wyjście** powoduje zakończenie bieżącej sesji z programem. Przed zakończeniem pracy, system wyświetla pytanie o potwierdzenie zamiaru zakończenia pracy (rysunek 3.8).



Rysunek 3.8. *Potwierdzenie zamiaru zakończenie pracy*

3.2. MENU SYSTEM

Menu **System** pokazano na rysunku 3.9.



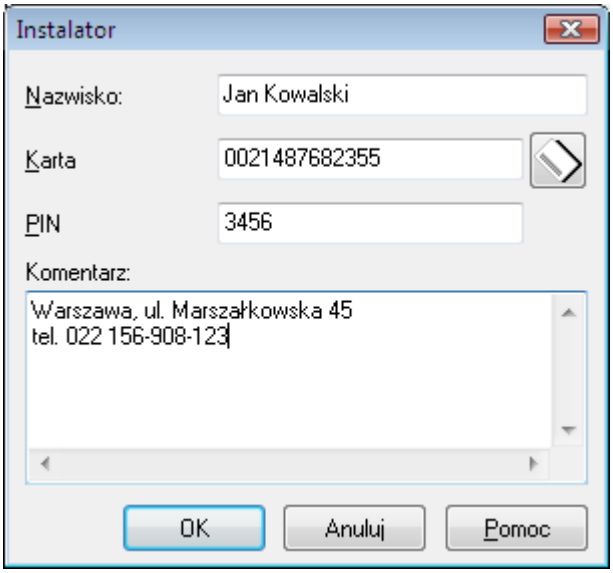
Rysunek 3.9. *Menu System*

3.2.1. Polecenie Instalator

Definiowanie użytkownika **Instalator** ma sens jedynie wtedy gdy w systemie RACS 4 są wykorzystywane kontrolery serii PRxx1 bo w przypadku tej serii kontrolerów możliwe jest wejście do trybu programowania instalatora i następnie ręczna konfiguracja kontrolerów za pomocą poleceń z klawiatury – patrz instrukcja **Opis funkcjonalny kontrolerów serii PRxx1**.

Użytkownik INSTALLER ma uprawnienia do wejścia w tryb programowania instalatora w odniesieniu do kontrolerów serii PRxx1, ale nie posiada uprawnień do otwierania drzwi. Ten specjalny użytkownik nie ma przypisanego numeru ID, więc nie jest widoczny na liście użytkowników.

Wybranie polecenia **Instalator** powoduje otwarcie okna dialogowego **Instalator** (rysunek 3.10).



Rysunek 3.10. *Okno dialogowe do definiowania użytkownika INSTALLER*

Przycisk znajdujący się obok pola **Karta** umożliwia przypisanie karty użytkownikowi INSTALLER. W polu **Komentarz** można podać dowolne informacje, na przykład dane kontaktowe użytkownika INSTALLER.

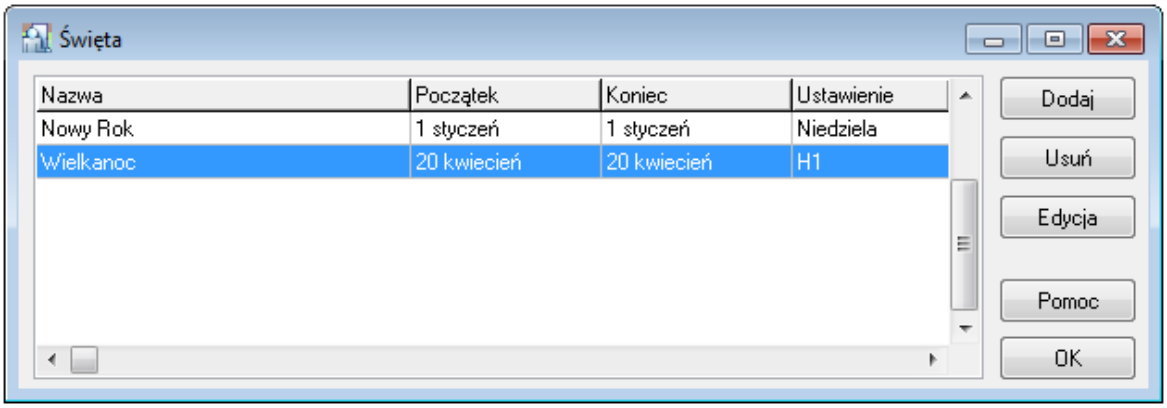
3.2.2. Polecenie Święta

W systemie obowiązują różne harmonogramy czasowe (ogólnego przeznaczenia, trybu drzwi, trybu identyfikacji, itd.). Są one definiowane dla poszczególnych dni tygodnia. Więcej informacji na temat harmonogramów można znaleźć w **punkcie 3.2.6**. Polecenie **Święta** służy do definiowania świąt obowiązujących w danym roku.

Dla dni świątecznych można zdefiniować specjalne ustawienia, inne niż te które wynikałyby z przyjętego harmonogramu tygodniowego. Dla świąt dostępne są w sumie cztery harmonogramy specjalne H1–H4.

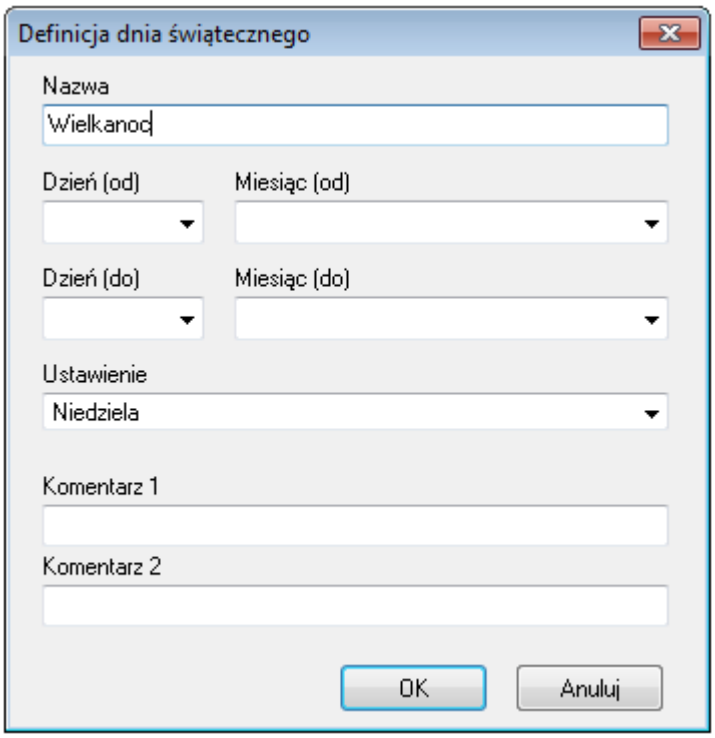
Definiując święto, użytkownik może określić przedział czasu, w jakim trwa dane święto. Oznacza to, że zdefiniowanie odrębnego harmonogramu dla np. długiego weekendu wymaga wskazania tylko jego początku i końca.

Wybranie polecenie **Święta** spowoduje wyświetlenie kartoteki świąt — okna dialogowego pokazanego na rysunku 3.11.



Rysunek 3.11. *Święta zdefiniowane w systemie*

Przycisk **Dodaj** umożliwia zdefiniowanie nowego święta w systemie (rysunek 3.12).



Rysunek 3.12. *Definiowanie nowego święta*

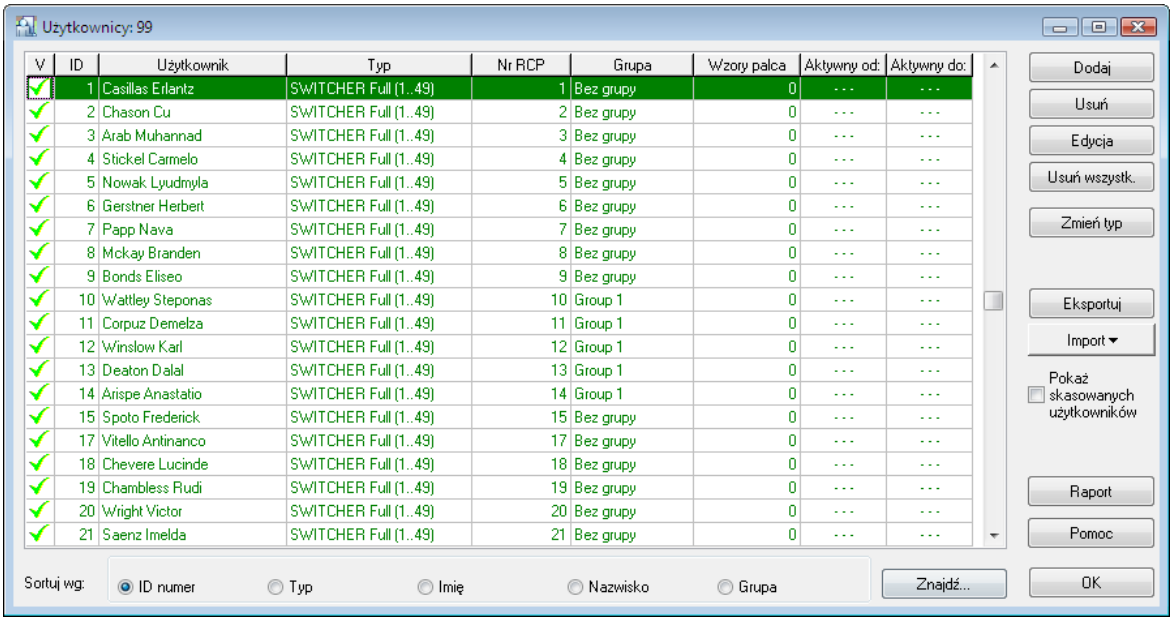
Przycisk **Edycja** służy do edycji zdefiniowanego wcześniej dnia, natomiast przycisk **Usuń** pozwala skasować wcześniej zdefiniowane święto.

3.2.3. Polecenie Użytkownicy

W systemie RACS 4 występują 4 typy użytkowników:

- **MASTER** — uprawnienia do otwierania drzwi, przezbrajania kontrolerów oraz do wejścia w tryb programowania ręcznego. Posiada numer identyfikacyjny 0.
- **SWITCHER Full** — uprawnienia do otwierania drzwi oraz do przezbrajania kontrolerów. Są im przypisywane numery identyfikacyjne od 01 do 49.
- **SWITCHER Limited** — uprawnienia do przezbrajania kontrolerów, nie ma prawa otwierania drzwi. Są im nadawane numery identyfikacyjne od 50 do 99.
- **NORMAL** — uprawnienia wyłącznie do otwierania drzwi. Użytkownicy tego typu posiadają numery identyfikacyjne od 100 do 3999. Użytkownicy typu NORMAL o ID powyżej 1000 mogą dodatkowo posiadać atrybut **Local SWITCHER** który uprawnia ich do przezbrajania tego kontrolera, na którym ten atrybut został im nadany.

Polecenie **Użytkownicy** otwiera kartotekę użytkowników systemu (rysunek 3.13).



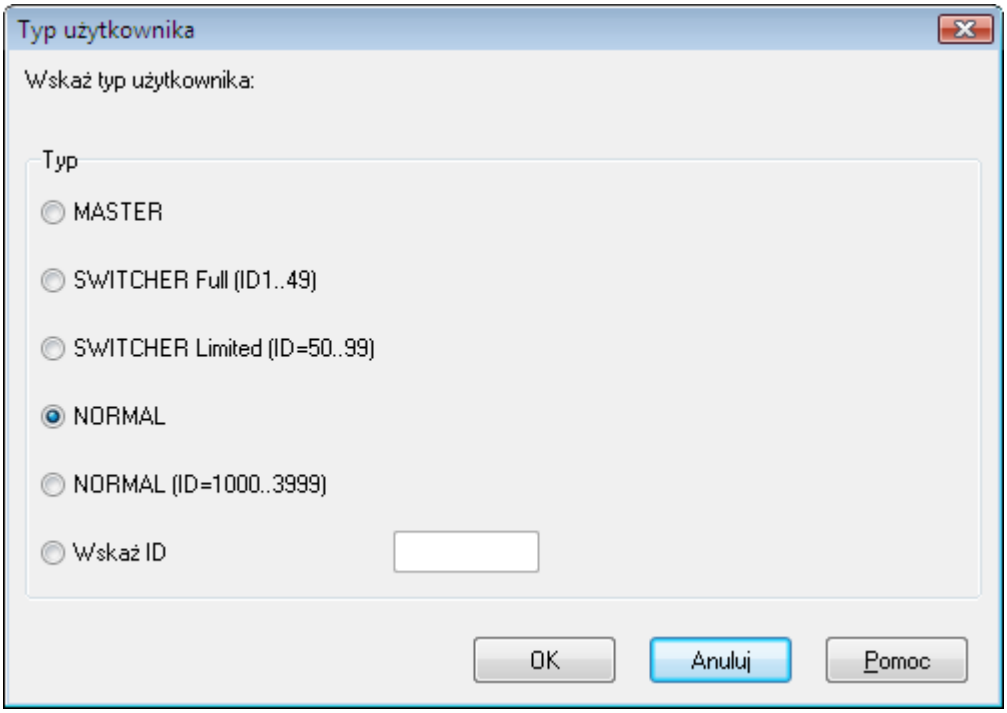
Rysunek 3.13. *Kartoteka użytkowników systemu*

Posługując się tym poleceniem można dodawać nowych użytkowników, usuwać ich, modyfikować właściwości, zmieniać typ, a także sortować według różnych kryteriów. Można również wyświetlić użytkowników usuniętych, wyeksportować listę zdefiniowanych użytkowników lub zaimportować użytkowników z pliku zewnętrznego. Z poziomu okna **Użytkownicy** można również wygenerować raport zawierający listę użytkowników zdefiniowanych w systemie. W tytule okna za słowem „Użytkownicy" wyświetla się aktualna liczba użytkowników zdefiniowanych w systemie (w przypadku pokazanym na rysunku jest ich 99). Znaczek ✓ w kolumnie **V** oznacza, że dany użytkownik jest aktywny, z kolei dla użytkowników nieaktywnych wyświetla się znaczek ⊘.

W poniższych punktach opisano podstawowe operacje wykonywane z poziomu kartoteki użytkowników.

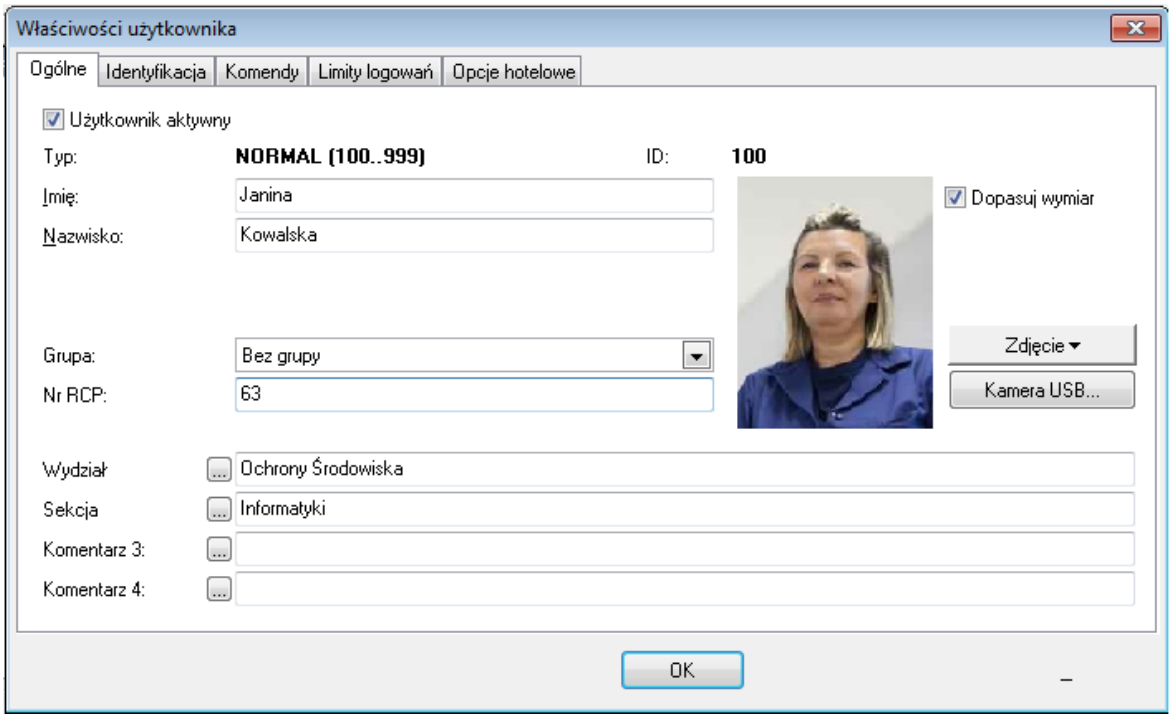
3.2.3.1. Dodawanie nowego użytkownika

Aby dodać nowego użytkownika, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Typ Użytkownika** (rysunek 3.14). Można tu wybrać określony typ użytkownika (wówczas system przydzieli użytkownikowi pierwszy wolny identyfikator z wybranej grupy) lub wpisać identyfikator po uprzednim zaznaczeniu przełącznika **Wskaż ID** (wówczas system określi typ użytkownika na podstawie wartości podanego identyfikatora.



Rysunek 3.14. *Wybór typu użytkownika*

Kliknięcie **OK** powoduje otwarcie okna **Właściwości użytkownika** (rysunek 3.15).



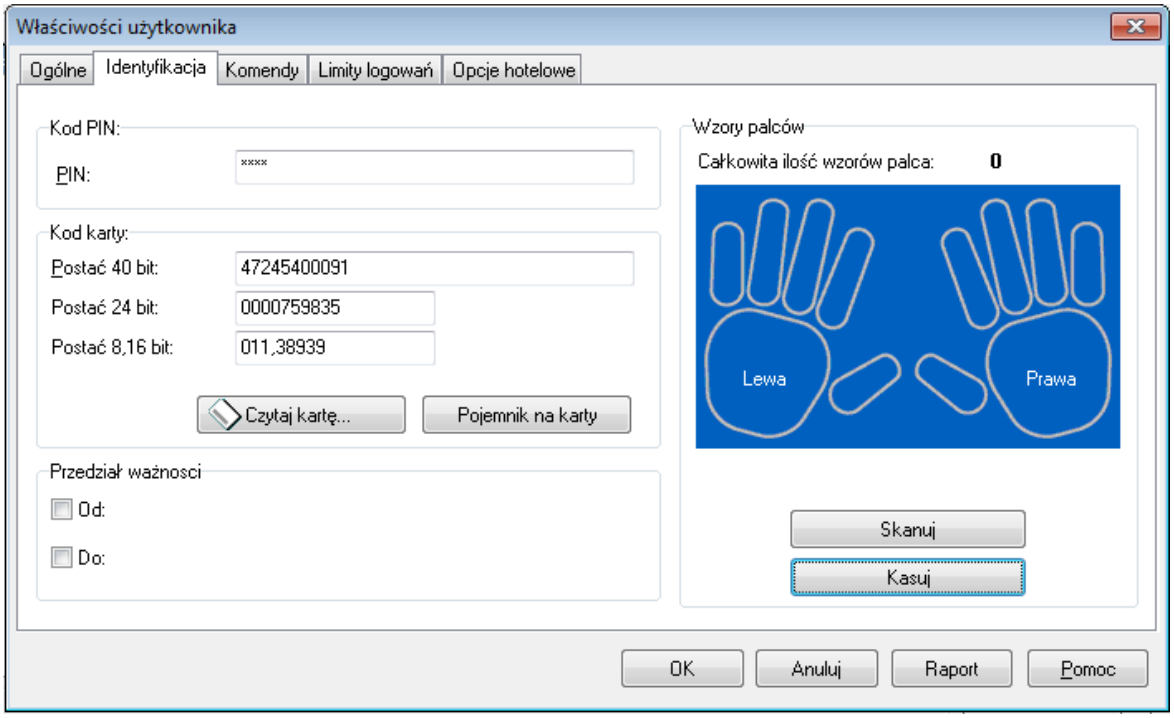
Rysunek 3.15. *Właściwości użytkownika*

Okno **Właściwości użytkownika** jest podzielone na 5 zakładek:

Ogólne (rysunek 3.15)— ogólne dane dotyczące użytkownika w tym imię i nazwisko oraz grupa dostępu dla której definiowane są prawa dostępu. W dolnej części okna znajdują się cztery pola

komentarzy, które mogą służyć do przechowywania różnych informacji (np. Wydziału i Sekcji). Aby zmienić nazwę pola komentarza, należy kliknąć przycisk [...].

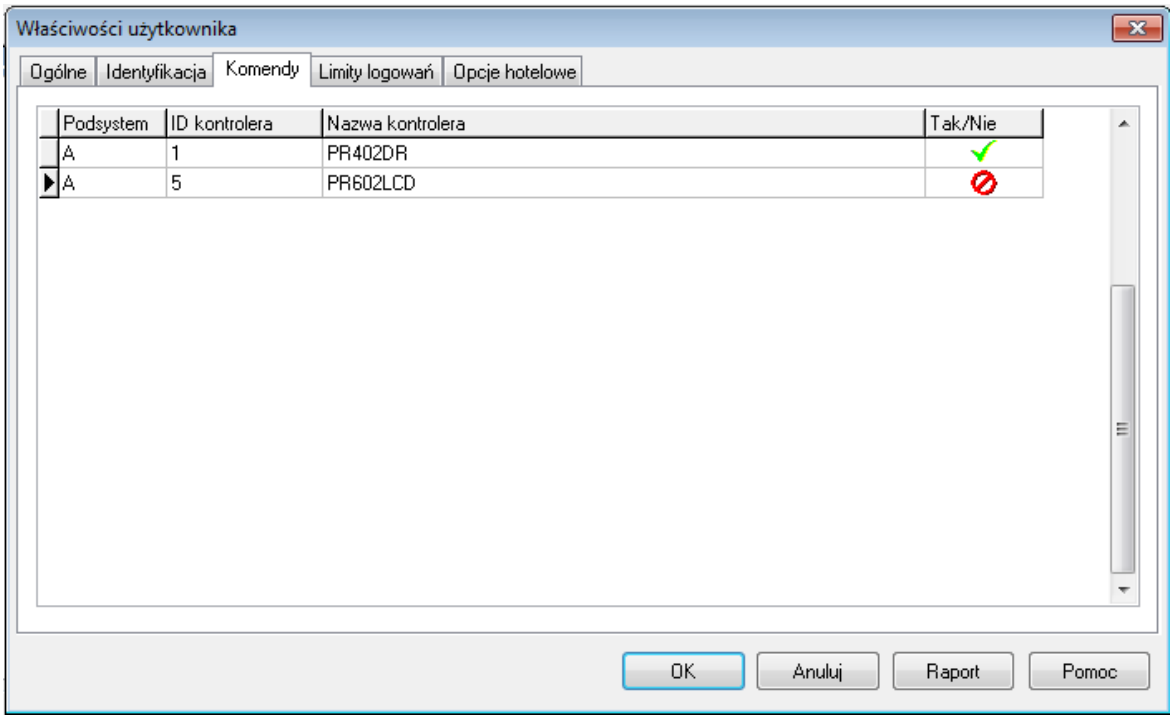
Identyfikacja (rysunek 3.16) — informacje identyfikujące użytkownika — karta, PIN oraz wzory linii papilarnych.



Rysunek 3.16. *Właściwości użytkownika — zakładka Identyfikacja*

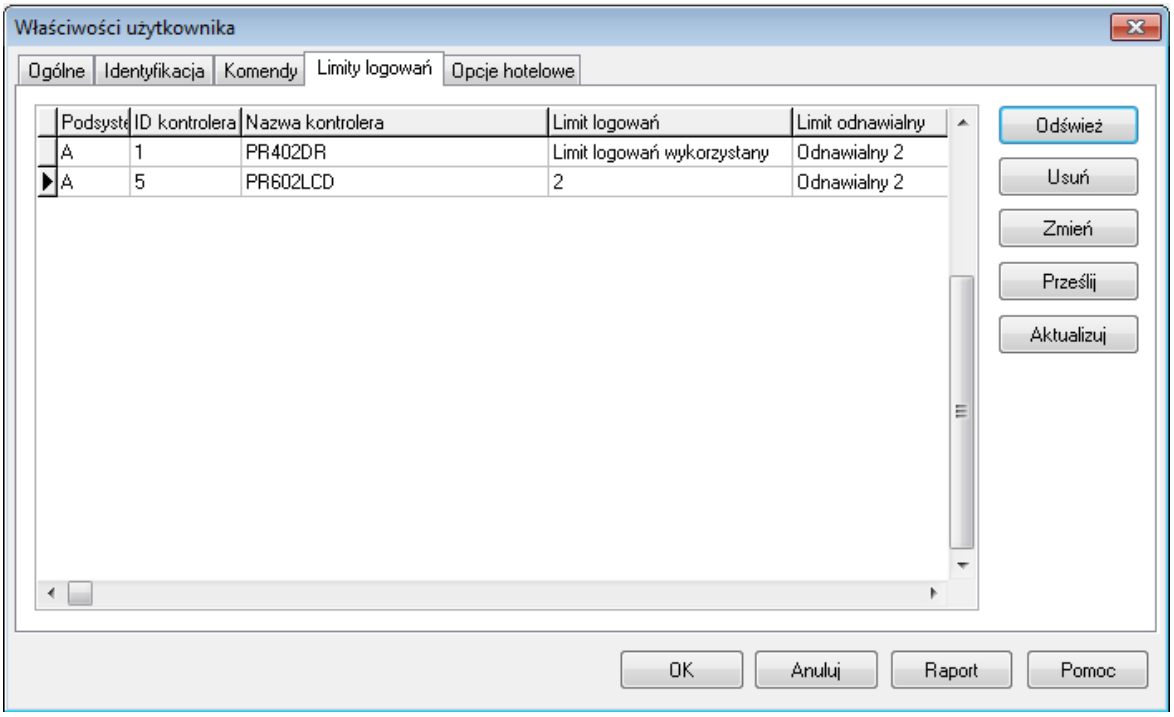
W tej zakładce podajemy podstawowe dane identyfikujące użytkownika. Do wczytywania kart mamy do dyspozycji dwa przyciski: **Czytaj kartę** i **Pojemnik na karty**. Wybranie pierwszego powoduje wyświetlenie okna wyboru czytnika, na którym będziemy czytać kartę. W pewnych sytuacjach, jeśli w pobliżu stanowiska operatora programu nie ma żadnego czytnika, opcja ta jest jednak niewygodna. W takim przypadku można skorzystać z opcji **Pojemnik na karty**. Daje ona dostęp do kartoteki wczytanych wcześniej kart. Sposób tworzenia pojemnika na karty opisano w **punkcie 3.2.13**. W obszarze **Przedział ważności** można podać okres ważności uprawnień nadanych użytkownikowi. Obszar **Wzory palców** umożliwia zarządzanie wzorami linii papilarnych przypisanych do wybranego użytkownika. Można je zaimportować z czytnika linii papilarnych za pomocą przycisku **Importuj z czytnika** (nie dotyczy czytnika RFT1000) lub zeskanować na wskazanym czytniku (przycisk **Skanuj...**). Za pomocą przycisku **Kasuj** można usuwać wzory linii papilarnych przypisane do użytkownika.

Komendy (rysunek 3.17) — okno, w którym można użytkownikowi udzielić lub zablokować prawa do wprowadzania komend z klawiatury na wskazanych kontrolerach.



Rysunek 3.17. *Właściwości użytkownika — zakładka Komendy*

Limity logowań (rysunek 3.18) — okno pozwalające na odczyt limitów logowań z kontrolerów i zarządzanie nimi w odniesieniu do wskazanego użytkownika. Po określeniu limitu logowania kontroler pozwoli zalogować się użytkownikowi na wskazanym kontrolerze tylko określoną liczbę razy. Można definiować zarówno jednorazowe jak i odnawialne limity logowań. Więcej informacji na ten temat podano w dokumencie **Opis funkcjonalny kontrolerów serii PRxx2**. Każdorazowa zmiana limitu logowania wymaga przesłania danych do kontrolera.



Rysunek 3.18. *Właściwości użytkownika — zakładka Limity logowań*

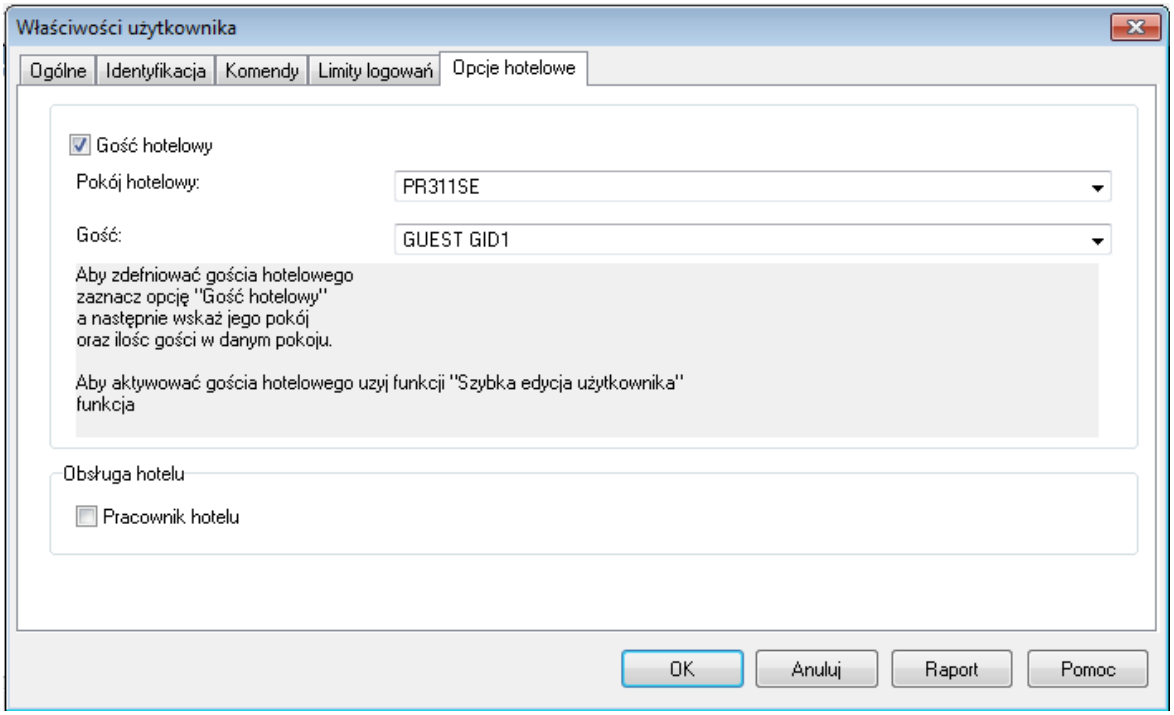
Opcje hotelowe (rysunek 3.19) — okno pozwalające na określenie, że wybrany użytkownik jest gościem hotelowym oraz wskazanie „numeru gościa" w wybranym pokoju hotelowym.

Rolę „pokoju hotelowego" mogą pełnić przede wszystkim kontrolery PR821-CH i PR621-CH jak też kontrolery standardowe serii PRxx1.

Zaleca się definiowanie użytkowników typu Gość poleceniem **Goście** w oknie głównym programu – patrz **punkt 3.2.4**.

Aby zdefiniować „pokój hotelowy" należy uaktywnić okno właściwości kontrolera, który ma pełnić tę rolę i zaznaczyć na nim opcję **Pokój hotelowy**.

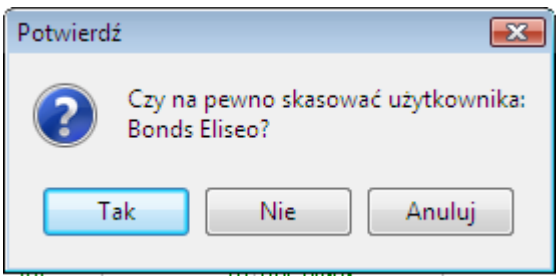
Aktywacja opcji hotelowych wymaga przesłania konfiguracji do kontrolera.



Rysunek 3.19. *Właściwości użytkownika — zakładka Opcje hotelowe*

3.2.3.2. Usuwanie użytkownika

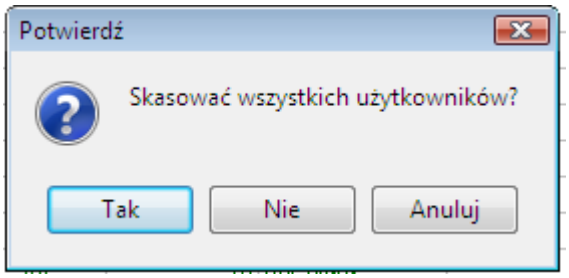
Do usuwania użytkowników służy przycisk **Usuń**. Po jego kliknięciu wyświetla się okno z potwierdzeniem zamiaru usunięcia użytkownika (rysunek 3.20).



Rysunek 3.20. *Potwierdzanie zamiaru usunięcia użytkownika*

Jeśli klikniemy **Tak**, użytkownik zostanie usunięty. System zapyta jeszcze, czy karta użytkownika ma być zwrócona do tzw. skrzynki, czyli pojemnika na karty, tak by można było ją przypisać innemu użytkownikowi.

Można również usunąć wszystkich użytkowników zdefiniowanych w systemie. Do tego celu służy przycisk **Usuń wszystk.** . Kliknięcie tego przycisku spowoduje wyświetlenie okna dialogowego z pytaniem o potwierdzenie zamiaru usunięcia wszystkich użytkowników (rysunek 3.21).

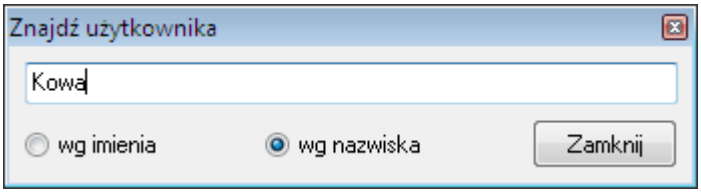


Rysunek 3.21. *Potwierdzanie zamiaru usunięcia wszystkich użytkowników*

Aby zapobiec przypadkowemu usunięciu wszystkich użytkowników z systemu, warto zadbać o częste wykonywanie kopii zapasowej danych. Można również wyeksportować listę użytkowników. Robi się to za pomocą przycisku **Import** w oknie **Użytkownicy**.

3.2.3.3. Wyszukiwanie użytkowników

Do wyszukiwania użytkowników służy przycisk **Znajdź** w oknie kartoteki użytkowników. Jest to opcja szczególnie przydatna w przypadku dużej liczby użytkowników w systemie. Kliknięcie przycisku powoduje wyświetlenie okna **Znajdź użytkownika** (rysunek 3.22), które pozwala na wyszukiwanie użytkowników według imienia lub według nazwiska. Podczas wpisywania nazwiska(imienia) do wyszukiwania), system automatycznie sortuje użytkowników wg wybranego pola i wyszukuje pierwszy rekord spełniający kryteria wyszukiwania.



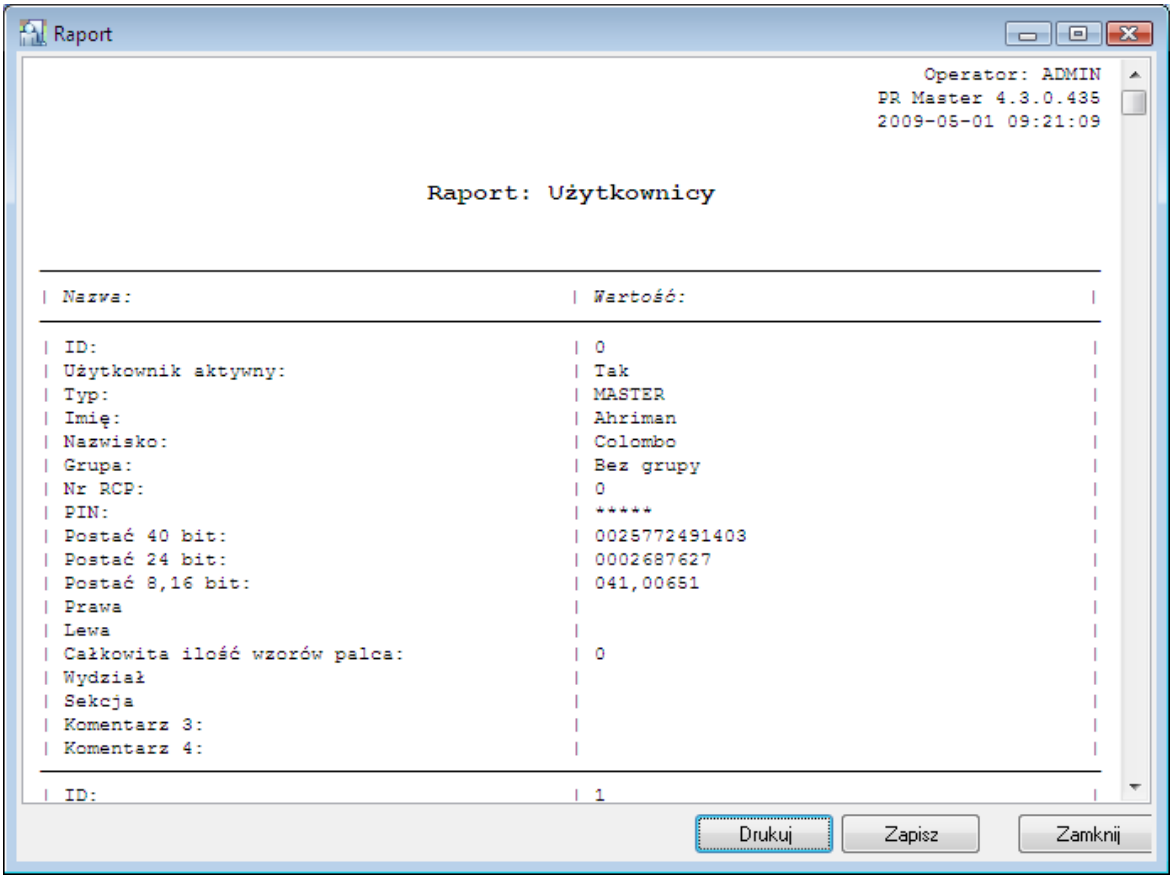
Rysunek 3.22. *Wyszukiwanie użytkowników*

3.2.3.4. Eksport i import listy użytkowników

Do eksportowania i importowania listy użytkowników służą odpowiednio przyciski **Eksportuj** i **Import** w oknie głównym kartoteki użytkowników. Po wybraniu polecenia **Eksportuj** wyświetla się okno dialogowe **Eksport użytkowników do pliku**, w którym należy wskazać plik, dokąd będą wyeksportowane dane. Z kolei przycisk **Importuj** pozwala na zaimportowanie danych użytkowników z wcześniej wyeksportowanej listy.

3.2.3.5. Generowanie raportu użytkowników

Po wprowadzeniu danych wszystkich użytkowników można sporządzić drukowany raport, który dokumentuje informacje wprowadzone do systemu. Do tego celu służy przycisk **Raport** w głównym oknie kartoteki użytkowników. Jego kliknięcie powoduje wyświetlenie raportu Użytkownicy w oknie **Raport** (rysunek 3.23).



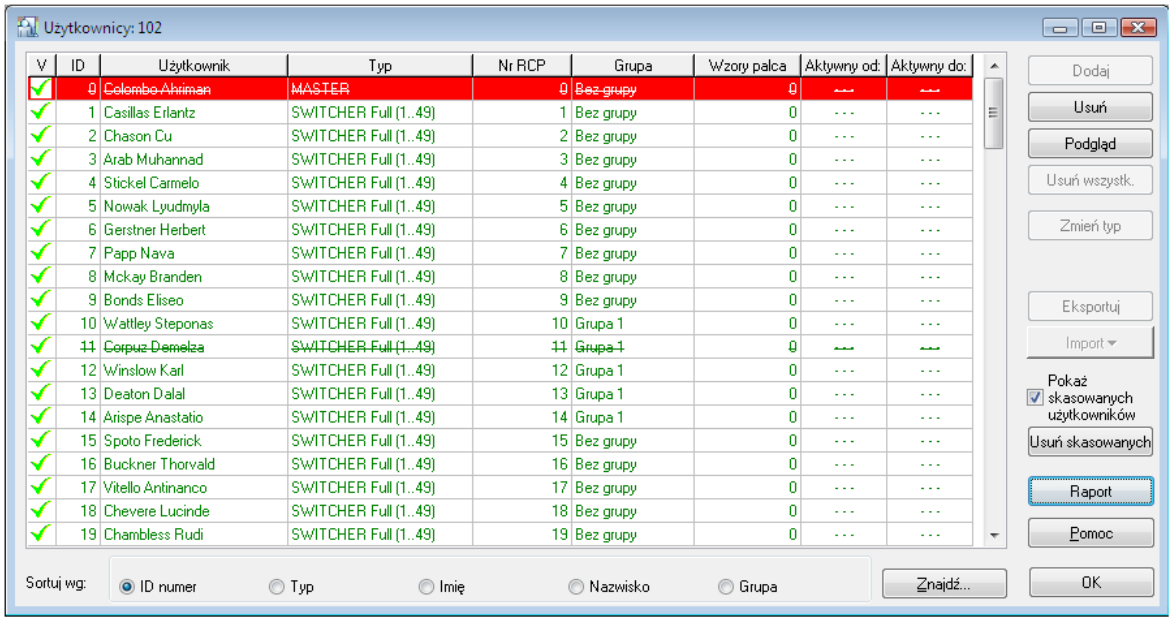
Rysunek 3.23. *Raport „Użytkownicy”*

Z poziomu okna **Raport** można wydrukować raport na wskazanej drukarce (przycisk **Drukuj**) lub zapisać w pliku (przycisk **Zapisz**).

3.2.3.6. Wyświetlanie i kasowanie wcześniej usuniętych użytkowników

Pole wyboru **Pokaż skasowanych użytkowników** pozwala wyświetlić użytkowników, którzy zostali z systemu usunięci. Po zaznaczeniu tego pola na liście użytkowników w oknie kartoteki wyświetlają się zarówno użytkownicy istniejący jak też usunięci, którzy są przekreśleni (rysunek 3.24). Użytkownicy skasowani nie zajmują puli dostępnych identyfikatorów dla użytkowników a ich powiązania z zarejestrowanymi zdarzeniami są zachowywane. Program PR Master od wersji 4.5.22 zgodnie z wymogami RODO umożliwia usunięcie skasowanego użytkownika za pomocą przycisku **Usuń**. Takie usunięcie kasuje całkowicie użytkownika z systemu, w tym również jego powiązania ze zdarzeniami zarejestrowanymi w przeszłości przez system.

Gdy liczba skasowanych użytkowników jest duża to może być wskazane ich całkowite usunięcie z bazy danych w celu poprawienia wydajności jej działania. Można to zrobić za pomocą przycisku **Usuń skasowanych** po zaznaczeniu pola wyboru **Pokaż skasowanych użytkowników**.



Rysunek 3.24. *Lista użytkowników wraz z użytkownikami usuniętymi z systemu*

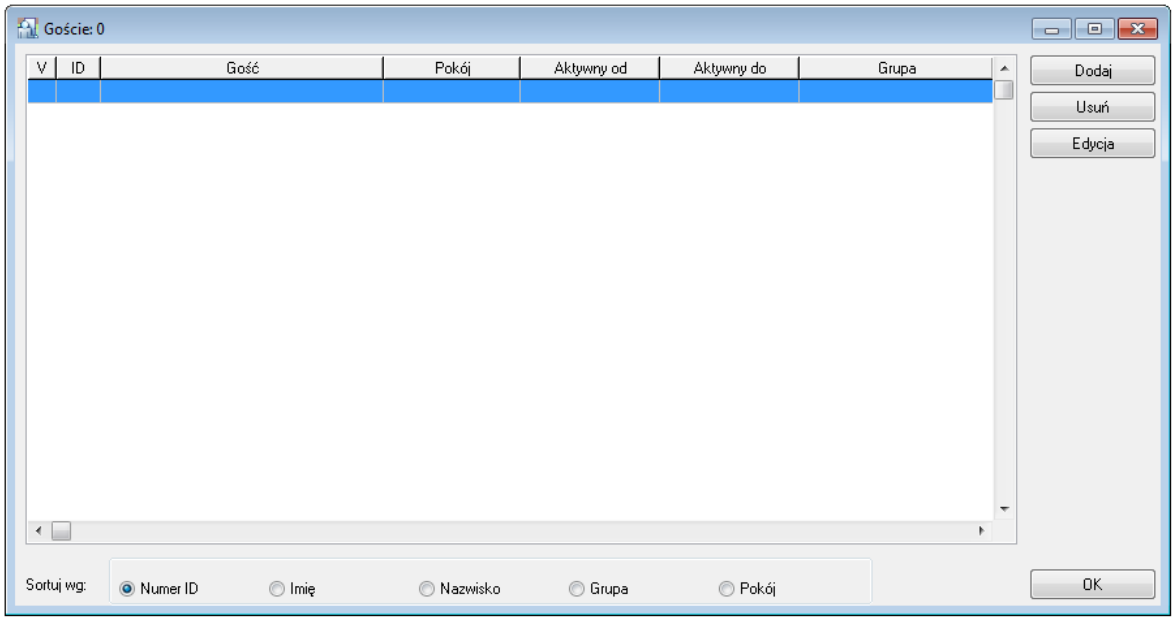
3.2.4. Polecenie Goście

Polecenie **Goście** w odróżnieniu od polecenia **Użytkownicy** umożliwia definiowanie specjalnej kategorii użytkowników systemu RACS 4 w sposób uproszczony i dużo szybszy bo niewymagający przesyłania pełnej konfiguracji do kontrolerów. Polecenie jest przeznaczone do wykorzystania w systemach hotelowych, w których z kolei zalecane jest stosowanie kontrolerów typu PR821-CH i PR621-CH czyli kontrolerów wyposażonych w kieszeń na kartę. Polecenie może być również stosowane w odniesieniu do kontrolerów serii PRxx1. Aby umożliwić dodawanie Gości na wymienionych urządzeniach konieczne jest załączenie opcji **Pokój hotelowy** we właściwościach kontrolerów w zakładce **Ogólne**. Z kolei gdy wymagane jest szybkie dodawanie użytkowników wszystkich możliwych typów w systemie z dowolnymi kontrolerami Roger to zaleca się stosowanie polecenia **Szybka Edycja Użytkownika** (patrz **punkt 3.5.2**).

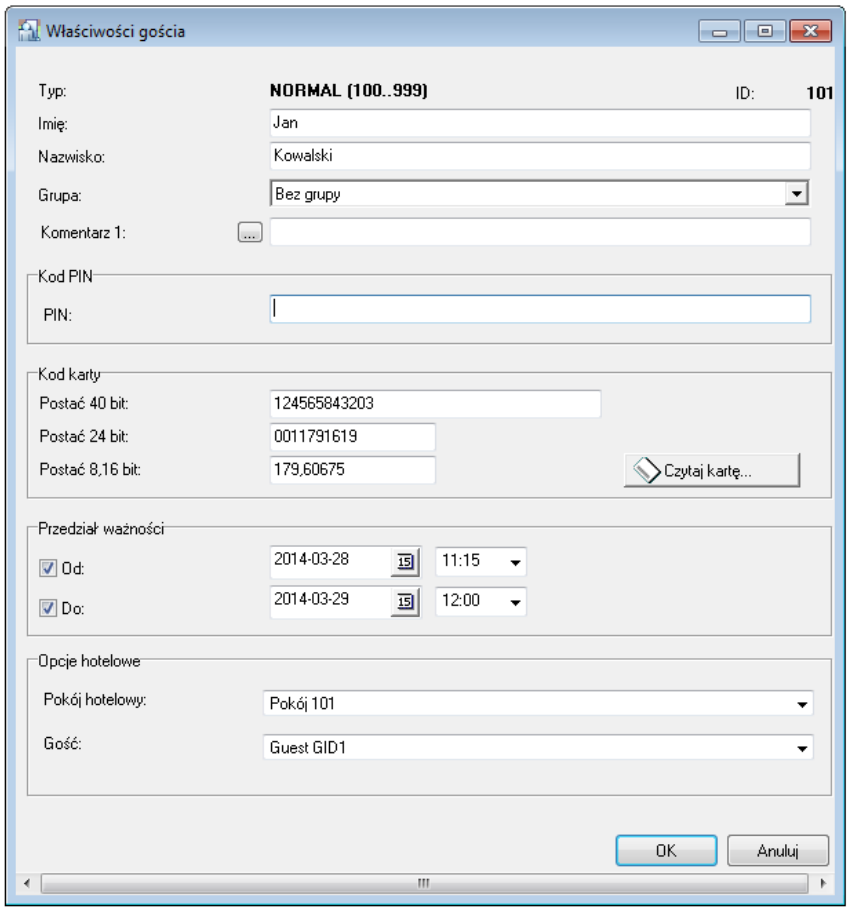
Po wybraniu polecenia **Goście** wyświetlana jest kartoteka (rysunek 3.25) zawierająca jedynie użytkowników typu NORMAL z atrybutami Gość. W oknie pokazanym na rysunku można dodawać nowych Gości, usuwać ich oraz modyfikować. Możliwe jest również sortowanie Gości wg. takich kryteriów jak numer ID, imię, nazwisko, nazwa pokoju, grupa dostępu.

Po wybraniu przycisku **Dodaj** wyświetlane jest okno definiowania Gościa bez potrzeby wybierania typu użytkownika (domyślnie wybierany jest typ NORMAL). Nowe okno opracowano poprzez uproszczenie standardowego okna właściwości użytkownika więc elementy okna **Właściwości gościa** w zasadzie funkcjonują w taki sam sposób jak w przypadku okna **Właściwości użytkownika** (rysunki 3.15 do 3.19). Różnice polegają na:

- konieczności stosowania czytnika RUD-2 lub RUD-3 podczas odczytu numeru karty za pomocą przycisku **Czytaj kartę...**
- możliwości zdefiniowania domyślnej grupy w polu **Grupa** (patrz **punkt 3.2.5.1**)
- możliwości zdefiniowania domyślnego czasu wymeldowania w polu **Do** (patrz **punkt 3.5.11.4**)



Rysunek 3.25. *Kartoteka użytkowników typu Goście*



Rysunek 3.26. *Okno właściwości Gościa*

3.2.5. Polecenie Grupy

W systemie RACS 4 użytkownicy mogą być podzieleni na 250 grup. Każdy użytkownik może być przydzielony do jednej z nich. Użytkownicy należący do tej samej grupy mają takie same

uprawnienia dostępu do pomieszczeń i pięter. Definiowanie praw dostępu w systemie RACS 4 polega na określeniu zasad kiedy i gdzie użytkownikom danych grup będzie przydzielony dostęp. Dla każdej grupy można dodatkowo określić uprawnienia do 32 pięter (0–31) dla czterech wind. Uprawnienia do pięter nie mogą być ograniczane za pomocą harmonogramów czasowych.

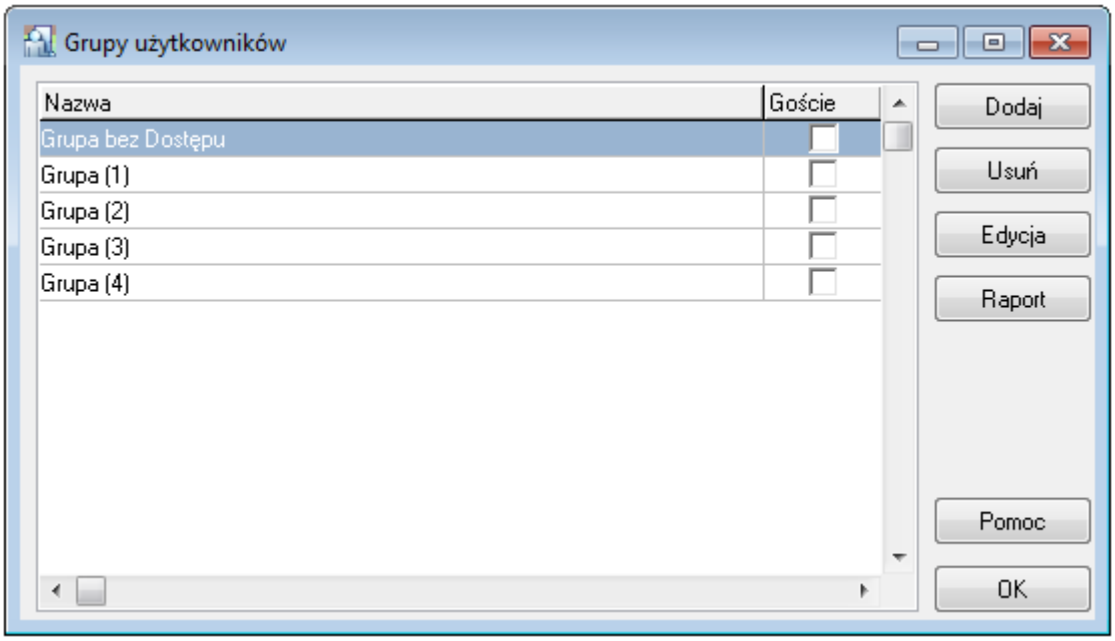
Każdy nowo zarejestrowany w systemie użytkownik może być przypisany do jednej z wbudowanych grup tj. do grupy o nazwie **Bez Grupy** i wtedy ma on prawo dostępu do wszystkich pomieszczeń oraz pięter bez żadnych ograniczeń czasowych lub do grupy o nazwie **Grupa bez Dostępu** i nie ma wtedy żadnych praw dostępu. Administrator systemu może zdefiniować również własne grupy dostępu i przypisać do nich użytkowników.

Użytkownicy **Bez grupy** tracą dostęp do pomieszczenia jedynie w przypadku:

- gdy wyzwolona jest linia wejściowa kontrolera z funkcją **Blokada dostępu**
- gdy na kontrolerze ustawiony jest tryb drzwi **Drzwi Zablokowane**
- gdy kontroler znajduje sie w trybie uzbrojonym oraz jednocześnie załączona jest opcja **Blokuj dostęp gdy kontroler jest w stanie uzbrojenia** we właściwościach kontrolera

Wykorzystując ten ostatni mechanizm można uzyskać efekt polegający na tym że dostęp użytkowników **Bez grupy** będzie mógł podlegać czasowemu blokowaniu w takt przełączania kontrolera pomiędzy trybami uzbrojony-rozbrojony

Polecenie **Grupy** otwiera kartotekę grup systemu (rysunek 3.27).



Rysunek 3.27. *Kartoteka grup*

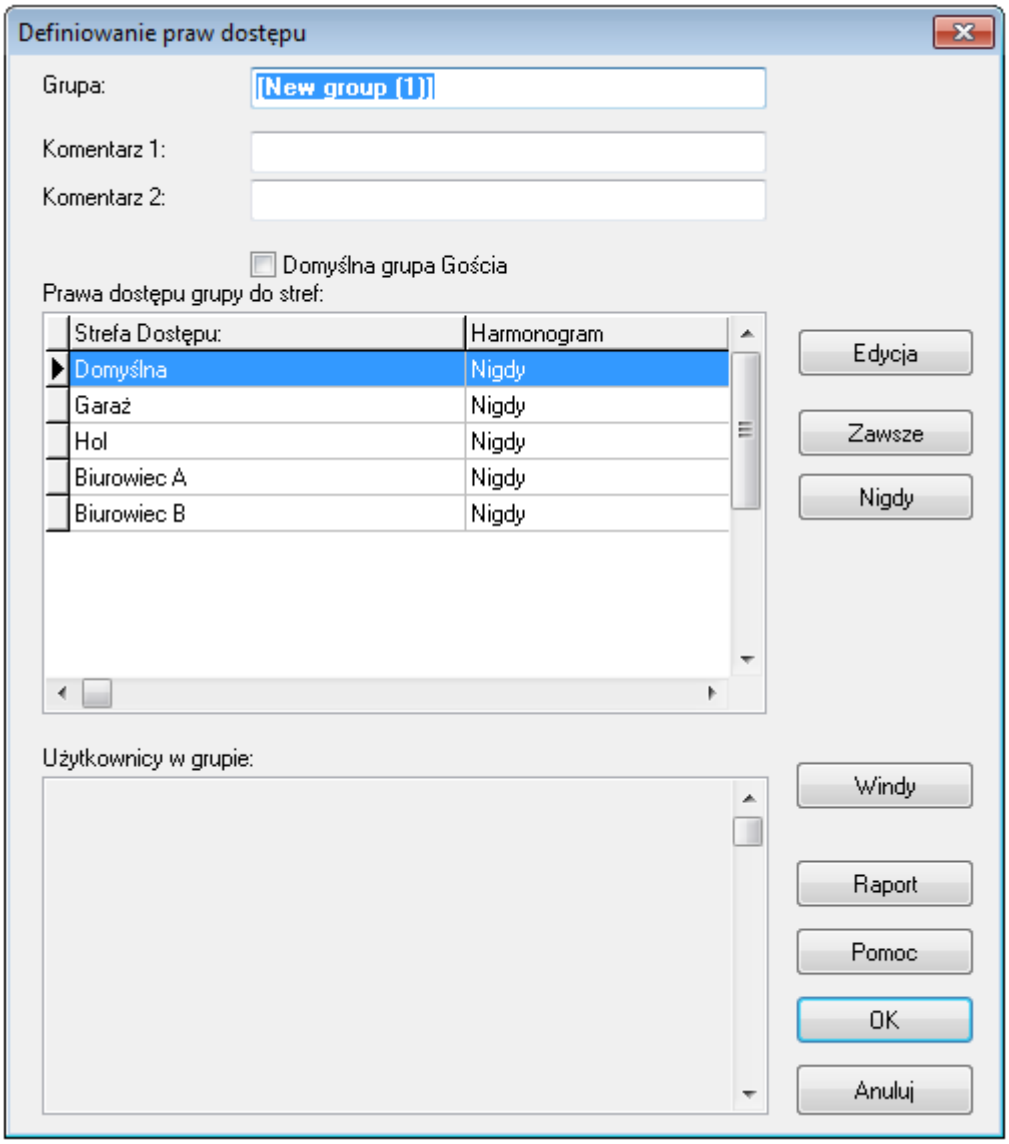
Pojęcie grup wiąże się z definiowaniem uprawnień dostępu w systemie RACS 4. Od strony fizycznej (sprzętu) terminale sterowane przez kontrolery tworzą tzw. strefy dostępu (patrz **punkt 3.2.7**). Z kolei użytkownicy należą do grup, a grupy mają prawa dostępu do wskazanych stref dostępu. Dodatkowo obowiązują harmonogramy czasowe (patrz **punkt 3.2.6.**). Za ich pomocą można określić, że np. użytkownik Jan Kowalski należący do grupy **Mechanicy** ma dostęp do strefy **Garaż** od poniedziałku do piątku w godzinach od 7.30 do 15.30.

Aby można było właściwie zdefiniować grupę, należy najpierw wyznaczyć strefy dostępu i zdefiniować harmonogramy czasowe. Następnie określić prawa dostępu grupy w poszczególnych strefach zgodnie z przypisanymi do nich harmonogramami czasowymi. Niezależnie od tego należy określić uprawnienia grupy do poszczególnych pięter (jeśli system kontroli dostępu steruje

dostępem do pięter). Później wystarczy już tylko przypisać użytkowników do wskazanej grupy. Użytkownicy ci uzyskają wszystkie uprawnienia przypisane danej grupie.

3.2.5.1. Dodawanie nowej grupy

Aby dodać nową grupę, należy kliknąć przycisk **Dodaj** w oknie kartoteki grup (rysunek 3.27) Wyświetli się okno dialogowe **Definiowanie praw dostępu** (rysunek 3.28). Można w nim nadać grupie nazwę, wprowadzić opisowe komentarze oraz określić uprawnienia grupy do stref dostępu zdefiniowanych w systemie. Domyślnie, w momencie dodawania, grupa nie ma żadnych uprawnień w strefach dostępu zdefiniowanych w systemie (do wszystkich stref dostępu jest przypisany harmonogram czasowy **Nigdy**. Opcjonalnie można również zaznaczyć przycisk wyboru **Domyślna grupa Gościa** tak by ta wskazana grupa użytkowników była automatycznie wybierana podczas definiowania gościa za pomocą opcji **Goście** (patrz **punkt 3.2.4**).

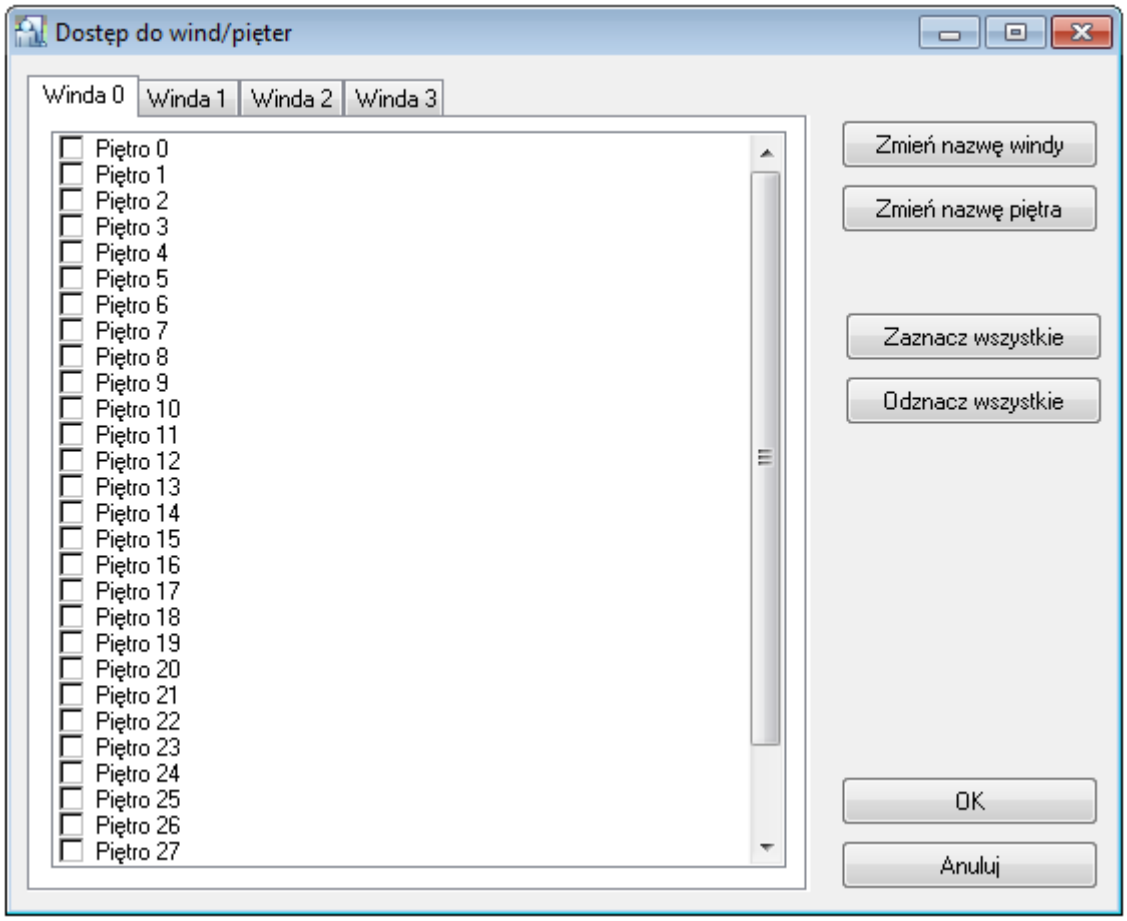


Rysunek 3.28. *Kartoteka grup*

W polu **Grupa** należy podać nazwę grupy. Domyślnie system przyjmuje nazwę **Nowa grupa(*nr*)**, gdzie ***nr*** oznacza kolejny numer grupy. W polach **Komentarz 1** i **Komentarz 2** podajemy dowolny opis grupy.

Aby zmienić harmonogram czasowy dla wszystkich stref dostępu z **Nigdy** na **Zawsze**, wystarczy kliknąć przycisk **Zawsze**. Z kolei kliknięcie przycisku **Nigdy** ustawia harmonogramy dostępu do wszystkich stref dostępu na **Nigdy**. Można również określić indywidualne harmonogramy czasowe dla każdej strefy oddzielnie. Do tego celu służy przycisk **Edycja**.

Przycisk **Windy** otwiera okno dialogowe **Dostęp do wind/pięter** (rysunek 3.29).

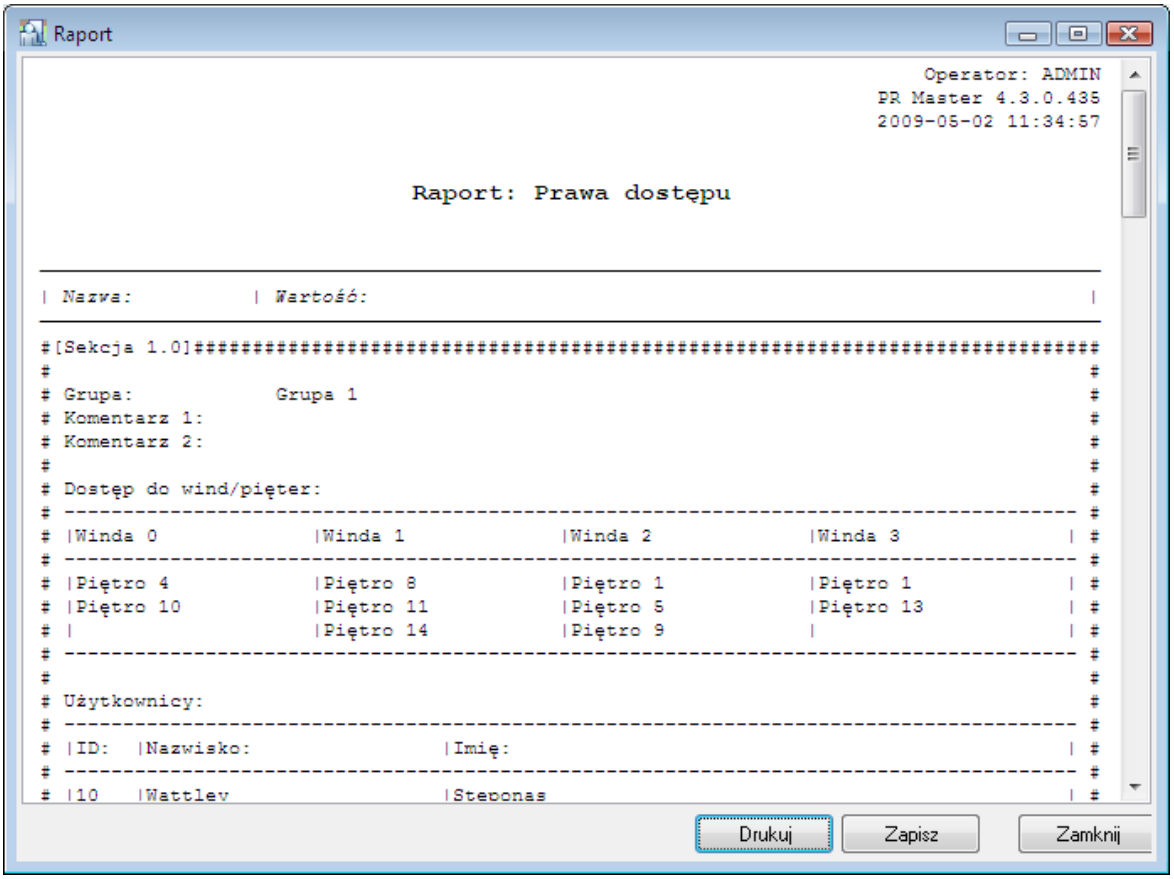


Rysunek 3.29. *Definiowanie dostępu do pięter*

Okno jest podzielone na cztery zakładki o domyślnych nazwach **Winda 0**, **Winda 1**, **Winda 2**, **Winda 3**. Nazwy te można zmienić za pomocą przycisku **Zmień nazwę windy**. Poszczególne piętra są oznaczone nazwami domyślnymi **Piętro 0**..**Piętro 31**. Aby zmienić nazwę jakiegoś piętra wystarczy je podświetlić i skorzystać z przycisku **Zmień nazwę piętra**. Aby określić uprawnienia grupy do wybranego piętra, należy zaznaczyć związane z nim pole wyboru. Przycisk **Zaznacz wszystkie** zaznacza wszystkie piętra, natomiast przycisk **Odznacz wszystkie** anuluje zaznaczenie wszystkich pięter.

Aby umożliwić kontrolę dostępu w windach konieczne jest zastosowanie kontrolerów serii PRxx2 oraz ekspanderów XM-8. Ekspandery XM-8 muszą być dodatkowo załączone we właściwościach kontrolera w zakładce **Opcje**.

Po zdefiniowaniu wszystkich praw dostępu wybranej grupy, można wygenerować raport, w którym będą wyszczególnione wszystkie zdefiniowane prawa dostępu wskazanej grupy. W tym celu, należy kliknąć przycisk **Raport** w oknie dialogowym **Definiowanie praw dostępu**. Wyświetli się okno z raportem **Prawa dostępu** (rysunek 3.30).



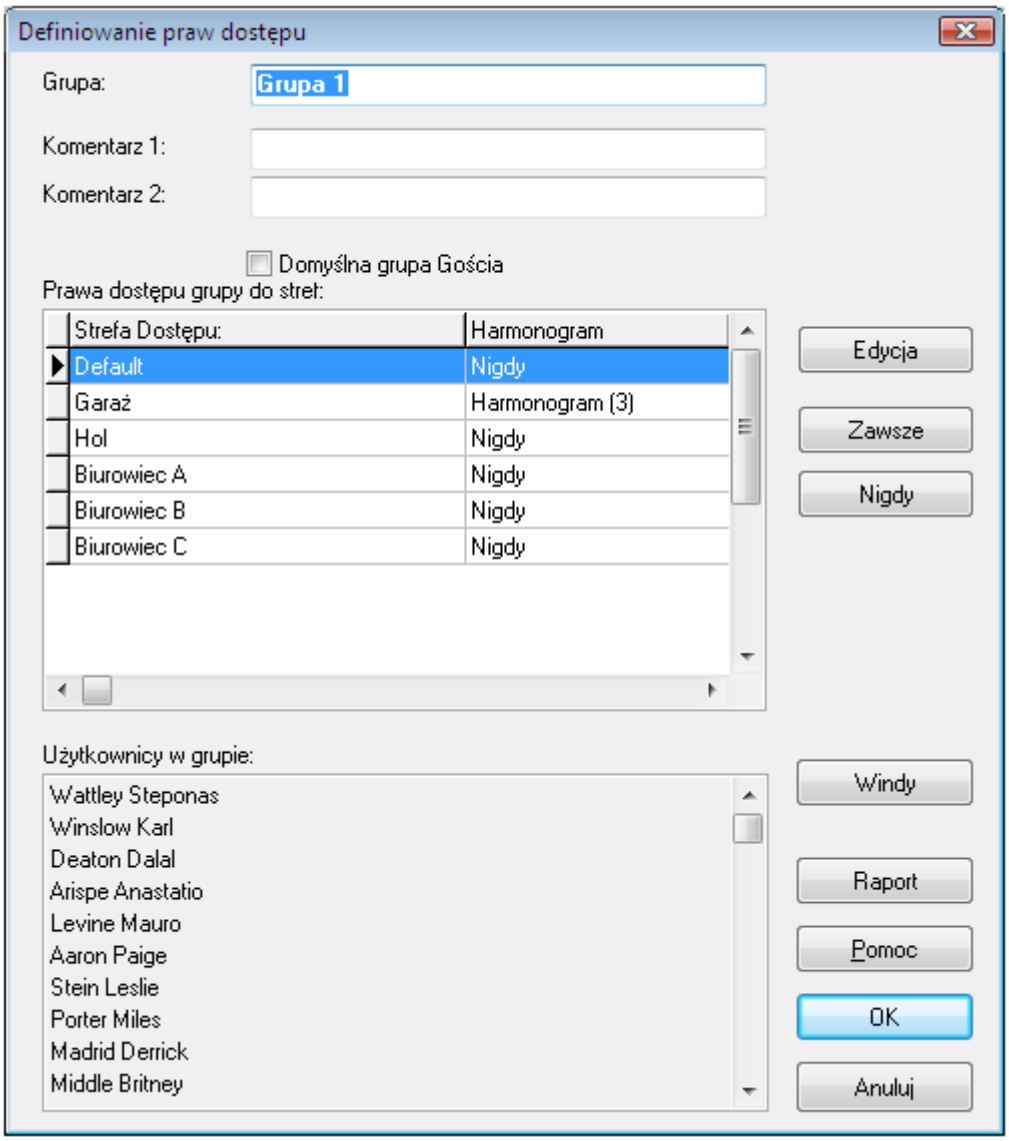
Rysunek 3.30. *Raport Prawa dostępu*

3.2.5.2. Przypisywanie użytkowników do grupy

Aby przypisać użytkownika do grupy, należy skorzystać z kartoteki użytkowników. Po wybraniu polecenia **Użytkownicy** z menu **System** (lub kliknięciu ikony **Użytkownicy** w panelu **System** głównego okna programu), należy wybrać użytkownika i kliknąć przycisk **Edycja**. W oknie dialogowym **Właściwości użytkownika**, w polu **Grupa** na karcie **Ogólne**, należy wskazać grupę, do której należy wybrany użytkownik. Po wprowadzeniu zmiany, należy kliknąć **OK**.

Opisany sposób dotyczy sytuacji, w której grupa została zdefiniowana już po stworzeniu kartoteki użytkowników. Wygodniej jednak najpierw stworzyć grupy i przypisywać właściwe grupy użytkownikom na etapie wprowadzania danych użytkowników do bazy danych.

Kiedy użytkownicy zostaną przypisani do grupy, można wyświetlić listę użytkowników należących do określonej grupy. W tym celu wystarczy otworzyć kartotekę grup i kliknąć przycisk **Edycja**. Wyświetli się okno dialogowe **Definiowanie praw dostępu**(rysunek 3.31).



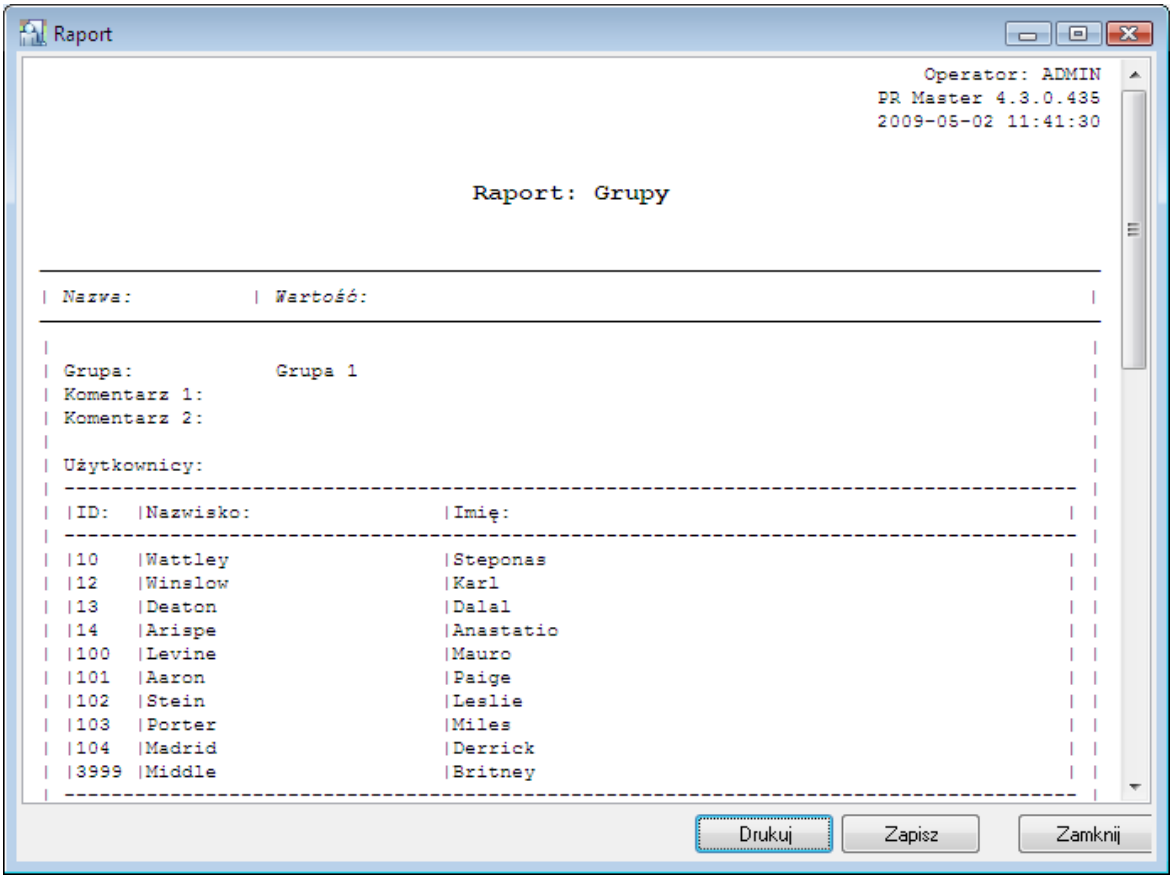
Rysunek 3.31. *Edycja właściwości grup. W obszarze „Użytkownicy w grupie" wyświetla się lista użytkowników należących do grupy*

3.2.5.3. Usuwanie grupy

Aby usunąć grupę, należy kliknąć przycisk **Usuń** w oknie dialogowym **Grupy użytkowników**. Przed usunięciem grupy wyświetla się okno **Potwierdź**, w którym użytkownik może potwierdzić zamiar usunięcia grupy bądź go anulować. Po usunięciu grupy, użytkownicy, którzy wcześniej do niej należeli są przypisani do grupy **Bez grupy**.

3.2.5.4. Generowanie raportu Grupy

Po wprowadzeniu danych wszystkich grup można sporządzić drukowany raport w celu udokumentowania informacji wprowadzonych do systemu. Do tego celu służy przycisk **Raport** w głównym oknie kartoteki grup. Jego kliknięcie powoduje wyświetlenie raportu **Grupy** w oknie **Raport** (rysunek 3.32).



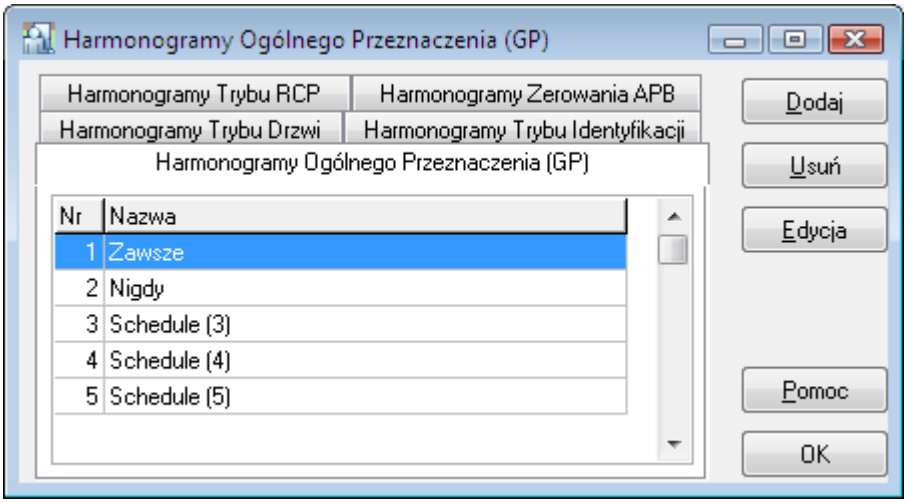
Rysunek 3.32. *Raport Grupy*

3.2.6. Polecenie Harmonogramy

Harmonogram czasowy to zbiór deklaracji przedziałów czasowych typu Od ... Do..... Przedziały czasowe definiuje sie dla każdego dnia tygodnia (od poniedziałku do niedzieli) oraz dla osobno dla dni świątecznych (H1, H2, H3 i H4). W systemie RACS 4 występuje pięć typów harmonogramów:

- ogólnego przeznaczenia
- trybu RCP
- zerowania funkcji APB
- trybu drzwi
- trybu identyfikacji

Do zarządzania harmonogramami czasowymi w systemie RACS 4 służy polecenie **Harmonogramy**. Po jego wybraniu otwiera się okno dialogowe pokazane na rysunku 3.33.



Rysunek 3.33. *Zarządzanie harmonogramami*

Okno jest podzielone na zakładki odpowiadające typom harmonogramów występujących w systemie RACS 4. Użytkownik może dodać nowy harmonogram (przycisk **Dodaj**), usunąć harmonogram (przycisk **Usuń**) lub zmodyfikować jego właściwości (przycisk **Edycja**).

3.2.6.1. Harmonogramy ogólnego przeznaczenia

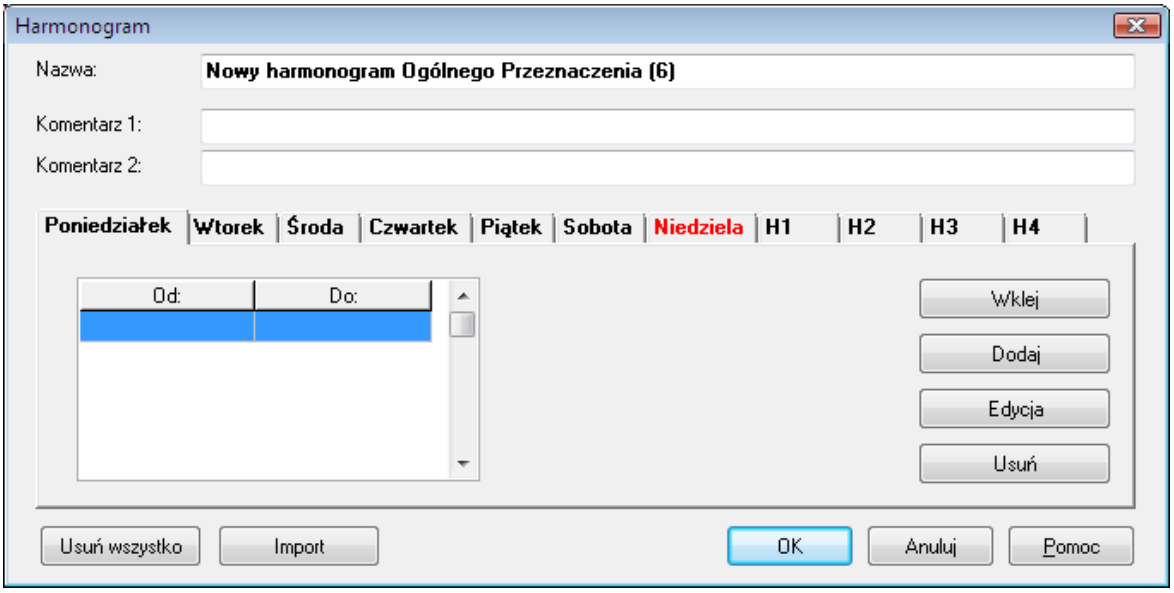
Harmonogram ogólnego przeznaczenia może być przypisany do jednej lub większej liczby funkcji sterujących w kontrolerze. Na przykład, ten sam harmonogram może być wykorzystywany do sterowania dostępem, linią wyjściową lub do blokowania odczytu linii wejściowej.

Domyślnie występują dwa harmonogramy ogólnego przeznaczenia: **Zawsze** i **Nigdy**. Harmonogramów tych nie można usunąć, ani zmodyfikować.

Harmonogramy ogólnego przeznaczenia wykorzystuje się do:

- definiowania uprawnień dostępu do stref — można, na przykład zdefiniować uprawnienie dostępu dla grupy **Mechanicy** do strefy **Garaż** w godzinach od 8.00 do 16.00 od poniedziałku do piątku;
- trybu wejścia komisyjnego — można określić przedziały czasowe, kiedy jest możliwe wejście komisyjne wymagające dwóch osób oraz ewentualnie spełnienia warunku dodatkowego;
- trybu aktywności opcji Kod Obiektu — ang. **Facility Code**;
- aktywności linii wejściowych;
- aktywności linii wyjściowych
- trybu High-Security

Aby dodać nowy harmonogram ogólnego przeznaczenia, należy wybrać zakładkę **Harmonogramy ogólnego przeznaczenia** w oknie kartoteki harmonogramów, a następnie kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Harmonogram** pozwalające na zdefiniowanie nowego harmonogramu (rysunek 3.34).



Rysunek 3.34. *Definiowanie nowego harmonogramu ogólnego przeznaczenia*

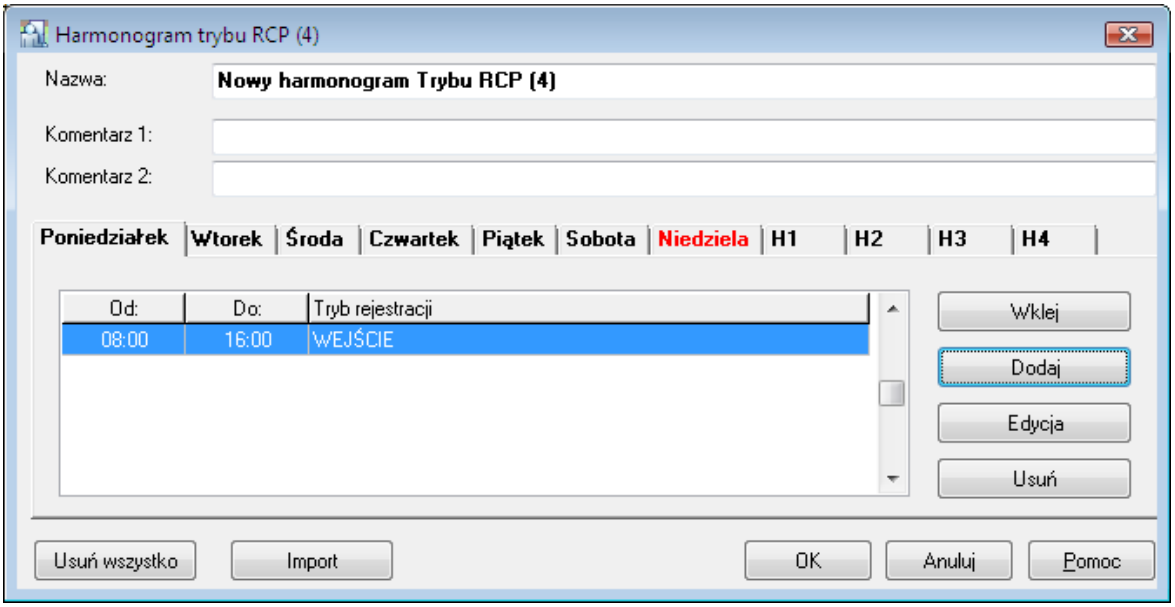
W polu **Nazwa** podajemy nazwę harmonogramu. W polach **Komentarz 1** i **Komentarz 2** podajemy dowolne opisowe komentarze. Przycisk **Dodaj** służy do definiowania nowego przedziału czasowego. Po jego kliknięciu wyświetla się okno **Przedział czasowy**, w którym podajemy godziny **Od**..**Do**. Przedziały czasowe należy zdefiniować dla wszystkich dni tygodnia, w których ma obowiązywać określony harmonogram. W tym celu należy kliknąć zakładkę odpowiedniego dnia tygodnia (**Poniedziałek**..**Niedziela**) lub dnia świątecznego (**H1**..**H4**) i wprowadzić obowiązujący przedział czasowy. Można również posłużyć się przyciskiem **Wklej**, który pozwala na skopiowanie przedziałów czasowych z innego dnia tygodnia. Przycisk **Usuń** usuwa wskazany zakres czasowy. Aby usunąć wszystkie zakresy czasowe, należy skorzystać z przycisku **Usuń wszystko**. Przycisk **Import** pozwala na zaimportowanie ustawień harmonogramu z innego harmonogramu ogólnego przeznaczenia. Definiowanie harmonogramu należy potwierdzić przyciskiem **OK**.

3.2.6.2. Harmonogramy trybu RCP

Harmonogramy trybu rejestracji czasu pracy (RCP) umożliwiają automatyczne przełączanie kontrolera pomiędzy różnymi trybami rejestracji RCP. Tryby RCP są stosowane gdy program PR Master współpracuje z programem RCP Master w celu zapewnienia rejestracji czasu pracy.

Harmonogram czasowy sterujący trybem rejestracji RCP określa przedziały czasowe (dni tygodnia, godziny), w których obowiązuje określony tryb rejestracji RCP. Dzięki temu punkt identyfikacji znajdujący się w kontrolerze może w zależności od potrzeb służyć do rejestracji różnych typów wejść i wyjść.

Harmonogram sterujący trybem pracy RCP ustalamy podobnie jak dla pozostałych harmonogramów. Trzeba jedynie ustalić jakiego typu zdarzenie (wejście, wyjście, wyjście służbowe itp.) ma być rejestrowane podczas obowiązywania harmonogramu (rysunek 3.35).



Rysunek 3.35. *Definiowanie nowego harmonogramu trybu RCP*

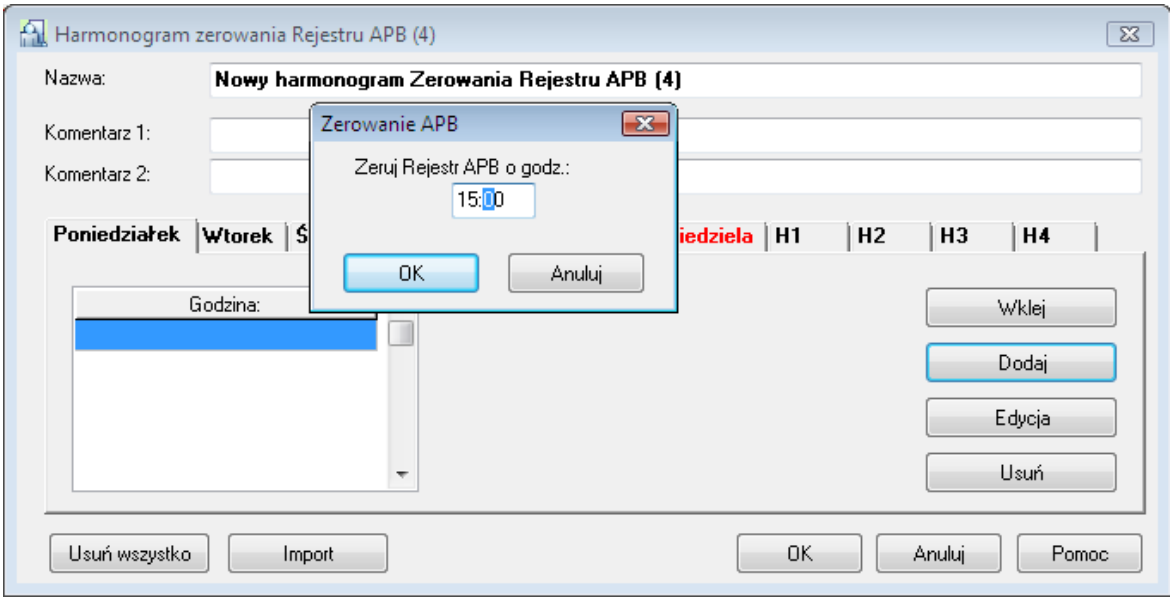
Domyślnie w systemie jest zdefiniowany harmonogram trybu RCP **Zawsze w Domyślnym Trybie RCP**. Harmonogramu tego nie można usunąć, ani zmodyfikować.

3.2.6.3. Harmonogramy zerowania funkcji APB

Funkcja Anti-Passback służy do zapobiegania ponownemu użyciu identyfikatora użytkownika na wejściu, jeśli wcześniej nie został on użyty na wyjściu. Inaczej mówiąc, użytkownik nie może dwa razy wejść do strefy APB, jeśli wcześniej z niej nie wyszedł. Funkcja ta ma na celu uniemożliwienie podania karty innej osobie, by ta mogła jej użyć do otwarcia drzwi. Więcej informacji na temat APB podano w instrukcji **Opis funkcjonalny kontrolerów serii PRxx2**.

Harmonogramy zerowania funkcji APB służą do zerowania statusu tej funkcji. Bezpośrednio po zerowaniu każdy z użytkowników zarejestrowanych na kontrolerze posiada w rejestrze APB status nieokreślony (nie można stwierdzić, czy ostatnio zalogował się na wejściu, czy na wyjściu). W związku z tym, każdy z użytkowników może użyć swojego identyfikatora zarówno na wejściu, jak i na wyjściu. Od momentu wyzerowania kontroler zaczyna egzekwować konieczność stosowania się do zasad APB.

Harmonogram definiuje się podobnie do harmonogramów ogólnego przeznaczenia. Zamiast przedziału czasowego trzeba jedynie ustalić konkretną godzinę zerowania rejestrów APB (rysunek 3.36).



Rysunek 3.36. *Definiowanie nowego harmonogramu zerowania APB*

Domyślnie w systemie jest zdefiniowany harmonogram zerowania APB o nazwie **Nigdy**. Oznacza on, że funkcja APB nigdy nie jest zerowana. Harmonogramu **Nigdy** nie można usunąć, ani zmodyfikować.

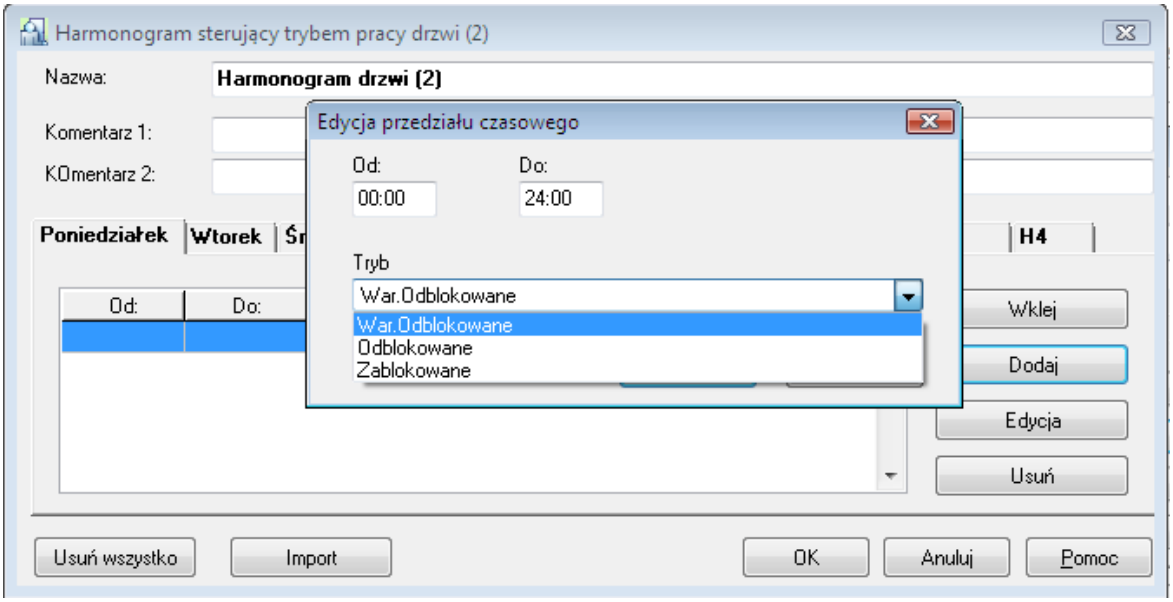
3.2.6.4. Harmonogramy trybu drzwi

W systemie RACS 4 można zdefiniować następujące tryby drzwi:

- **Normalny** – drzwi zamknięte dla osób bez praw dostępu
- **War.Odblokowane** — drzwi zamknięte do chwili otwarcia przez pierwszą z uprawnionych osób
- **Odblokowane** — drzwi otwarte dla wszystkich.
- **Zablokowane** — drzwi zamknięte dla wszystkich.

Domyślnym trybem drzwi jest tryb Normalny. Harmonogram sterowania trybem pracy drzwi umożliwia automatyczne przełączanie kontrolera pomiędzy różnymi trybami pracy drzwi. Definiowanie tego harmonogramu polega na określeniu przedziałów czasowych oraz wskazaniu jaki tryb drzwi ma obowiązywać w danym przedziale.

Dodawanie nowego harmonogramu następuje tak samo jak w przypadku harmonogramu ogólnego przeznaczenia. Podczas edycji przedziału czasowego trzeba jedynie ustalić tryb pracy drzwi (rysunek 3.37).



Rysunek 3.37. *Definiowanie nowego harmonogramu sterowania trybem pracy drzwi*

Domyślnie w systemie jest zdefiniowany harmonogram sterowania trybem pracy drzwi o nazwie **Zawsze w trybie Normalnym**. Oznacza on, że drzwi zawsze pracują standardowo. Harmonogramu tego nie można usunąć, ani zmodyfikować.

3.2.6.5. Harmonogramy trybu identyfikacji

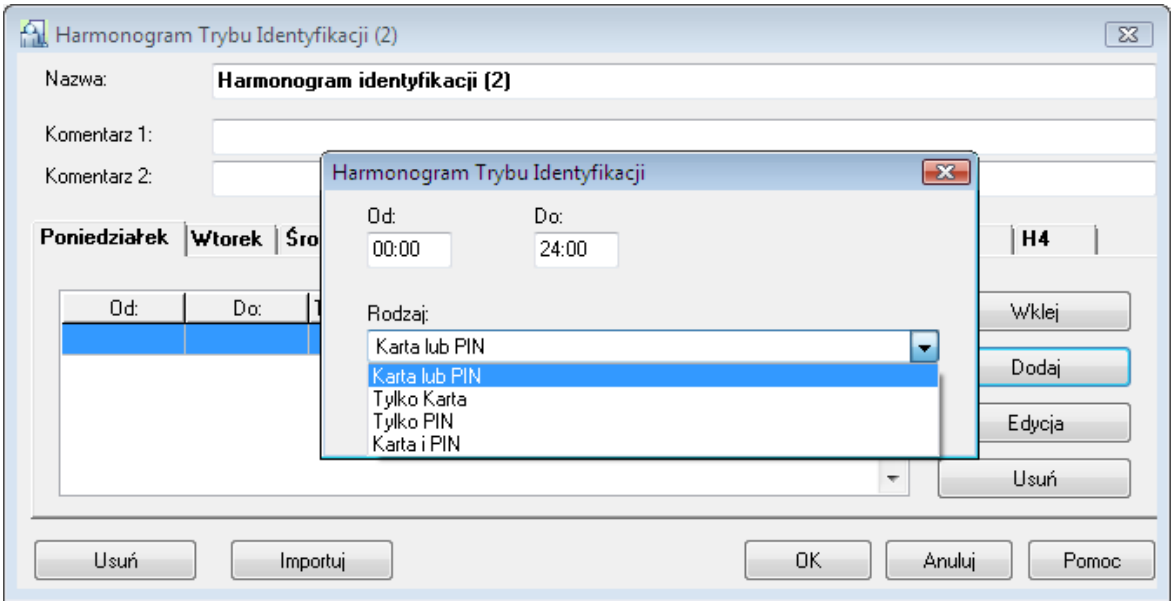
W systemie RACS 4 można zdefiniować następujące tryby identyfikacji:

- **Karta lub PIN** — użytkownik może użyć do identyfikacji karty bądź kodu PIN. Może ich używać zamiennie.
- **Tylko Karta** — użytkownik może użyć do identyfikacji wyłącznie karty.
- **Tylko PIN** — użytkownik może użyć do identyfikacji wyłącznie kodu PIN.
- **Karta i PIN** — w celu pomyślnej identyfikacji użytkownik musi użyć zarówno karty, jak i poprawnego kodu PIN.

Harmonogram sterowania trybem identyfikacji umożliwia automatyczne przełączanie kontrolera pomiędzy różnymi trybami identyfikacji. Definiowanie tego harmonogramu polega na określeniu przedziałów czasowych oraz wskazaniu jaki tryb identyfikacji ma obowiązywać w danym przedziale.

Poza okresami obowiązywania wskazanego trybu identyfikacji, obowiązuje domyślny tryb identyfikacji ustalony we właściwościach kontrolera.

Dodawanie nowego harmonogramu następuje tak samo jak w przypadku harmonogramu ogólnego przeznaczenia. Podczas edycji przedziału czasowego trzeba jedynie ustalić tryb identyfikacji (rysunek 3.38).



Rysunek 3.38. *Definiowanie nowego harmonogramu sterowania trybem identyfikacji*

Domyślnie w systemie jest zdefiniowany harmonogram sterowania trybem pracy drzwi o nazwie **Zawsze w Domyślnym Trybie Identyfikacji**. Oznacza on, że kontroler zawsze pracuje w ustalonym dla siebie domyślnym trybie identyfikacji. Harmonogramu tego nie można usunąć, ani zmodyfikować.

3.2.7. Polecenie Strefy dostępu

Strefa dostępu to zbiór wskazanych punktów identyfikacji (terminali), które w systemie RACS 4 są interpretowane jako spójny obszar. Strefę dostępu może tworzyć określone miejsce, np. Garaż, Hol, Biurowiec itp. Wyznaczenie stref dostępu umożliwia zdefiniowanie uprawnień dostępu nie dla pojedynczych drzwi, ale dla grupy urządzeń kontrolujących dostęp do pewnego obszaru w obiekcie.

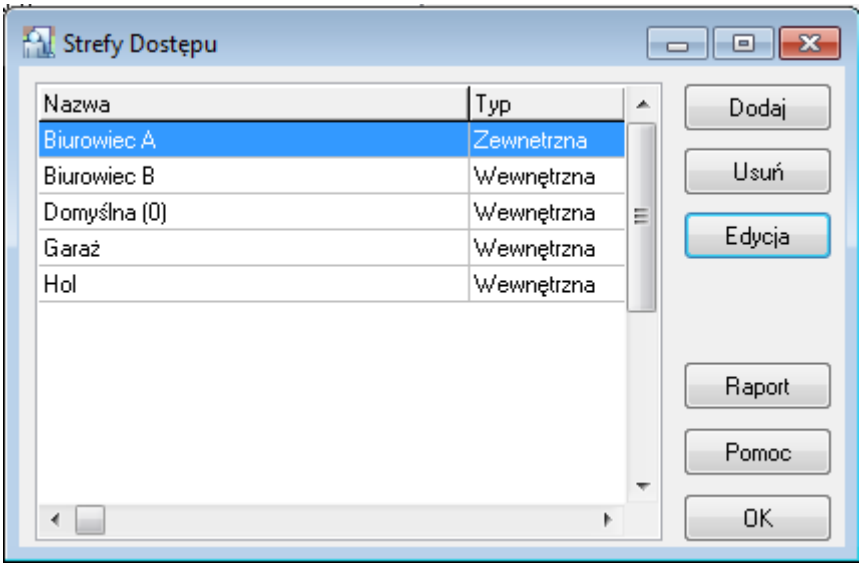
Każdy punkt dostępu (czytnik) podłączony do kontrola powinien być przypisany do strefy dostępu zdefiniowanej przez administratora systemu. Po dodaniu nowego kontrolera do systemu jego czytniki są przypisywane domyślnie do strefy **Domyślnej**.

Punkt dostępu to miejsce w obiekcie strzeżone za pomocą kontrolera. Ponieważ kontroler może sterować wejściem lub wyjściem, każdy z terminali nowszych typów kontrolerów można przypisać do osobnej strefy.

Terminal należy do tej strefy, do której umożliwia wejście (a nie wyjście).

W starszych typach kontrolerów (PR201, PR301, PR311) poszczególnych terminali nie można było przypisać do osobnych stref. Strefę dostępu przypisuje się w nich na poziomie kontrolera (tzn. oba terminale należą do tej samej strefy).

Wybranie polecenia menu **System**/**Strefy dostępu** powoduje wyświetlenie kartoteki stref dostępu (rysunek 3.39)



Rysunek 3.39. *Kartoteka stref dostępu*

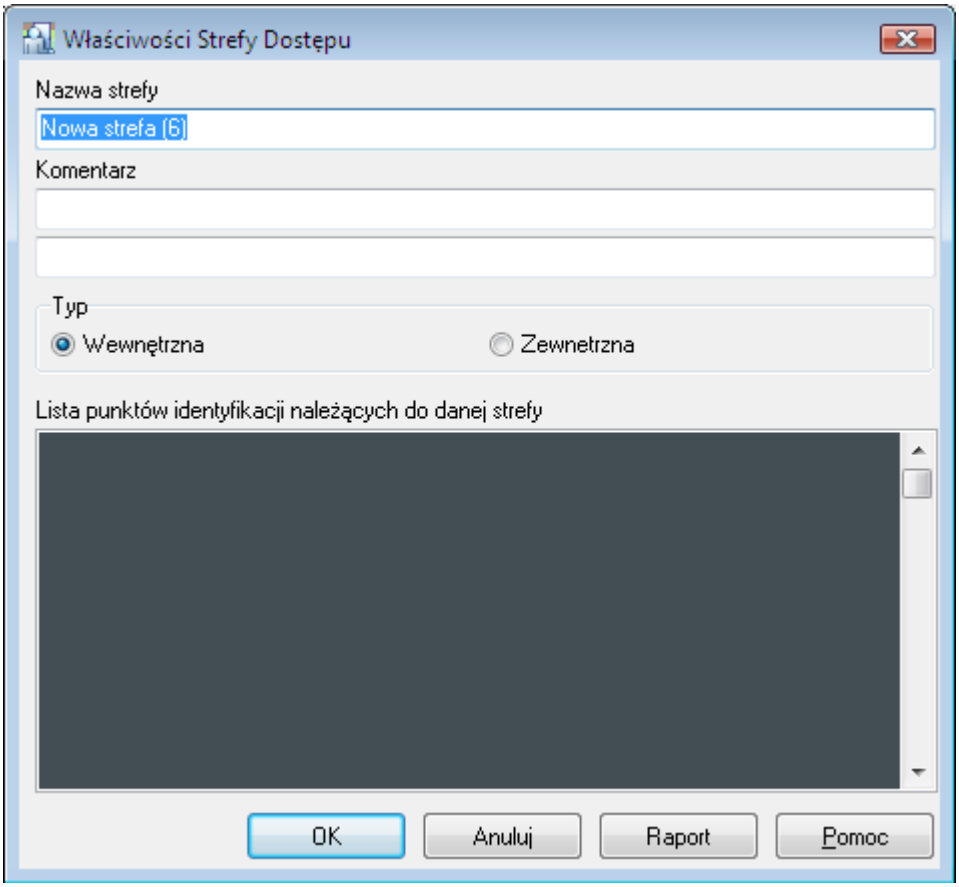
Z poziomu tego okna użytkownik może dodać nową strefę dostępu (przycisk **Dodaj**), usunąć wcześniej zdefiniowaną strefę (przycisk **Usuń**), zmodyfikować właściwości wskazanej strefy (przycisk **Edycja**), a także wydrukować raport **Strefy** zawierający listę stref zdefiniowanych w systemie.

3.2.7.1. Dodawanie nowej strefy dostępu

Aby dodać nową strefę dostępu, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Właściwości Strefy Dostępu** (rysunek 3.40). Można w nim nadać strefie nazwę, wprowadzić opisowe komentarze oraz określić, czy strefa jest **Zewnętrzna**, czy **Wewnętrzna**.

Strefa wewnętrzna znajduje się wewnątrz obiektu. **Strefa zewnętrzna** (publiczna) to wszystko to, co znajduje się na zewnątrz obiektu. Zgodnie z tym, do stref zewnętrznych należy przyporządkować wszystkie terminale, które pozwalają na wyjście z kontrolowanego obiektu (co jest tożsame z wejściem do strefy publicznej). Zazwyczaj w systemie występuje kilka stref wewnętrznych i jedna zewnętrzna. Można jednak wyobrazić sobie skomplikowany system, w którym można rozróżnić kilka stref zewnętrznych.

Pojęcie stref wewnętrznych i zewnętrznych pozwala na stwierdzenie ile osób w danym momencie znajduje się wewnątrz obiektu, a ile na zewnątrz. Do wyznaczania takiej klasyfikacji służy polecenie **Narzędzia**/**Liczba użytkowników w strefach dostępu**.



Rysunek 3.40. *Definiowanie nowej strefy dostępu*

W polu **Nazwa strefy** należy podać nazwę strefy dostępu. Domyślnie system przyjmuje nazwę **Nowa strefa(*nr*)**, gdzie ***nr*** oznacza kolejny numer strefy. W polach **Komentarz 1** i **Komentarz 2** podajemy dowolny opis strefy dostępu.

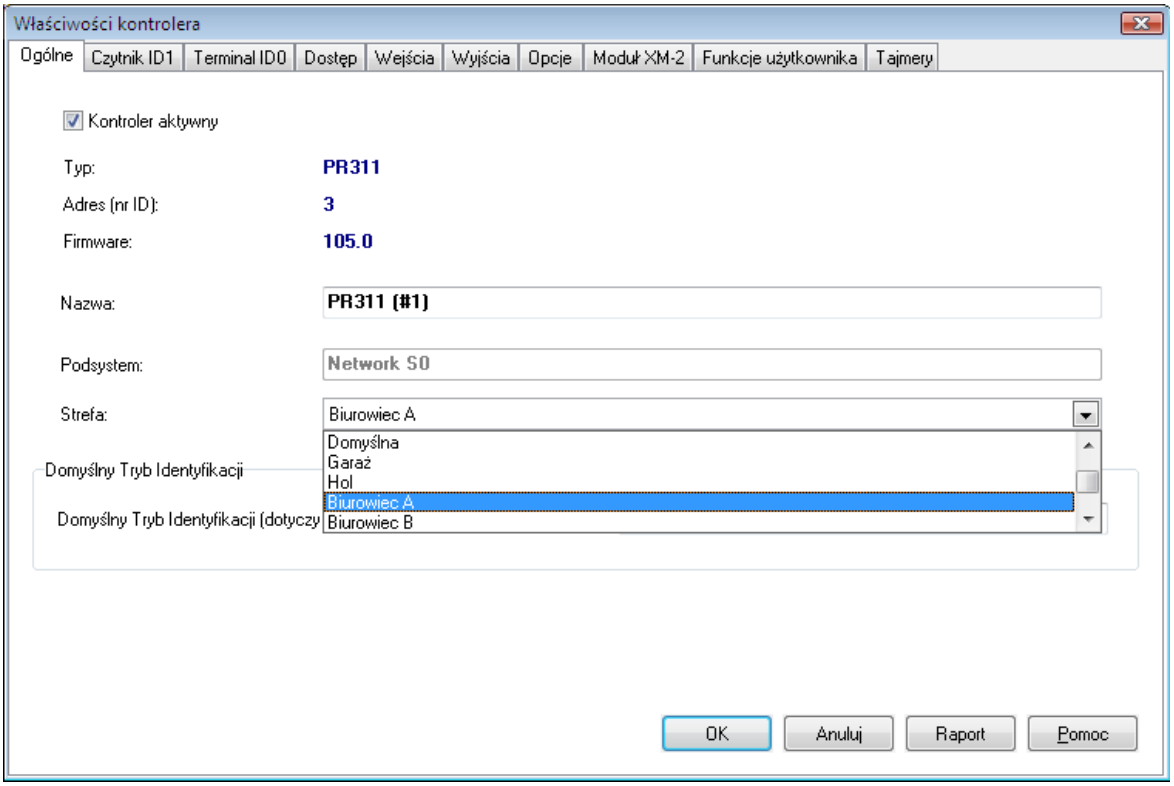
Po zdefiniowaniu strefy dostępu lista punktów identyfikacji, które do niej należą jest pusta. Strefa jest zdefiniowana w sposób kompletny dopiero wtedy, gdy przypiszemy do niej czytniki (terminale). Robi się to z poziomu okna właściwości kontrolera.

3.2.7.2. Usuwanie strefy dostępu

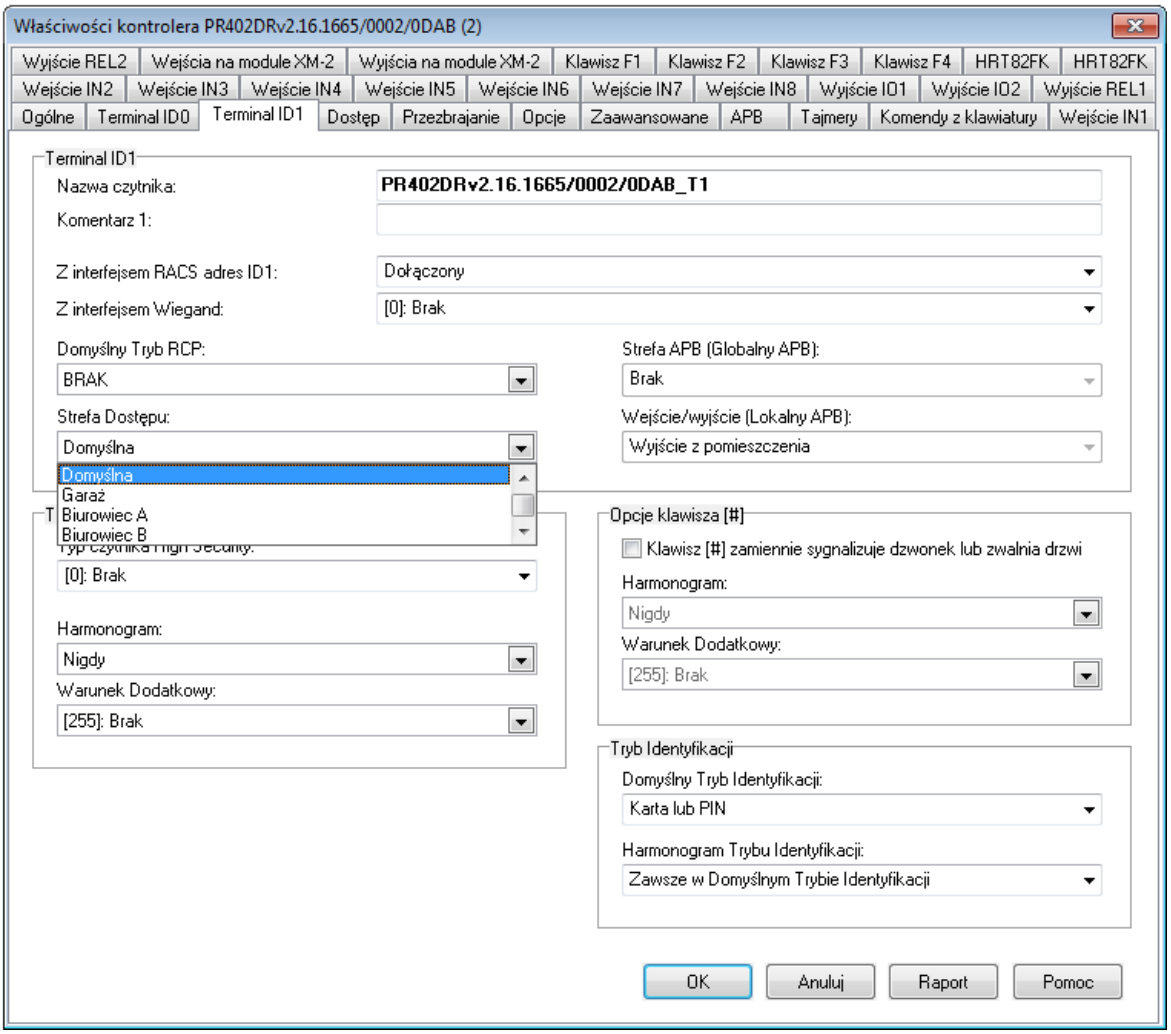
Aby usunąć strefę dostępu należy kliknąć przycisk **Usuń** w oknie dialogowym **Strefy Dostępu**. Przed usunięciem grupy wyświetla się okno **Potwierdź**, w którym użytkownik może potwierdzić zamiar usunięcia strefy bądź go anulować. Po usunięciu strefy dostępu, punkty identyfikacyjne, które wcześniej do niej należały będą przypisane do grupy **Domyślna**.

3.2.7.3. Przypisywanie punktów identyfikacyjnych do strefy

Aby przypisać punkt identyfikacyjny do strefy dostępu, należy otworzyć okno właściwości kontrolera. W zależności od typu kontrolera, określamy strefę dla kontrolera lub dla poszczególnych terminali (rysunki 3.41 i 3.42). Ogólnie rzecz biorąc, w starszych typach kontrolerów (PR 201, PR 301) oba terminale należą do tej samej strefy. W nowszych typach, każdy terminal można przypisać do osobnej strefy.



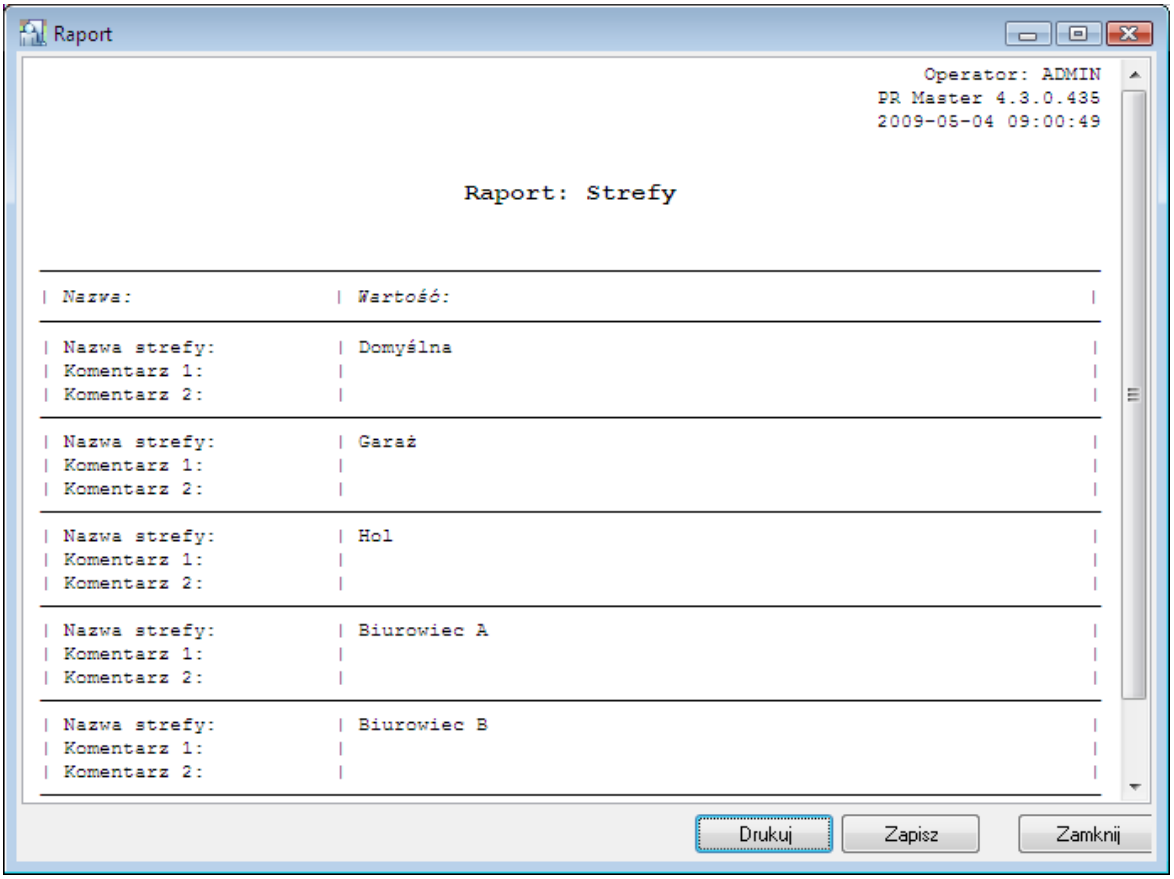
Rysunek 3.41. *Przypisywanie kontrolera do strefy — kontroler PR311*



Rysunek 3.42. *Przypisywanie terminala do strefy — kontroler PR402DR*

3.2.7.4. Generowanie raportu Strefy

Po wprowadzeniu danych wszystkich stref można sporządzić drukowany raport w celu udokumentowania konfiguracji systemu. Do tego celu służy przycisk **Raport** w głównym oknie kartoteki stref dostępu. Jego kliknięcie powoduje wyświetlenie raportu **Strefy** w oknie **Raport** (rysunek 3.43).



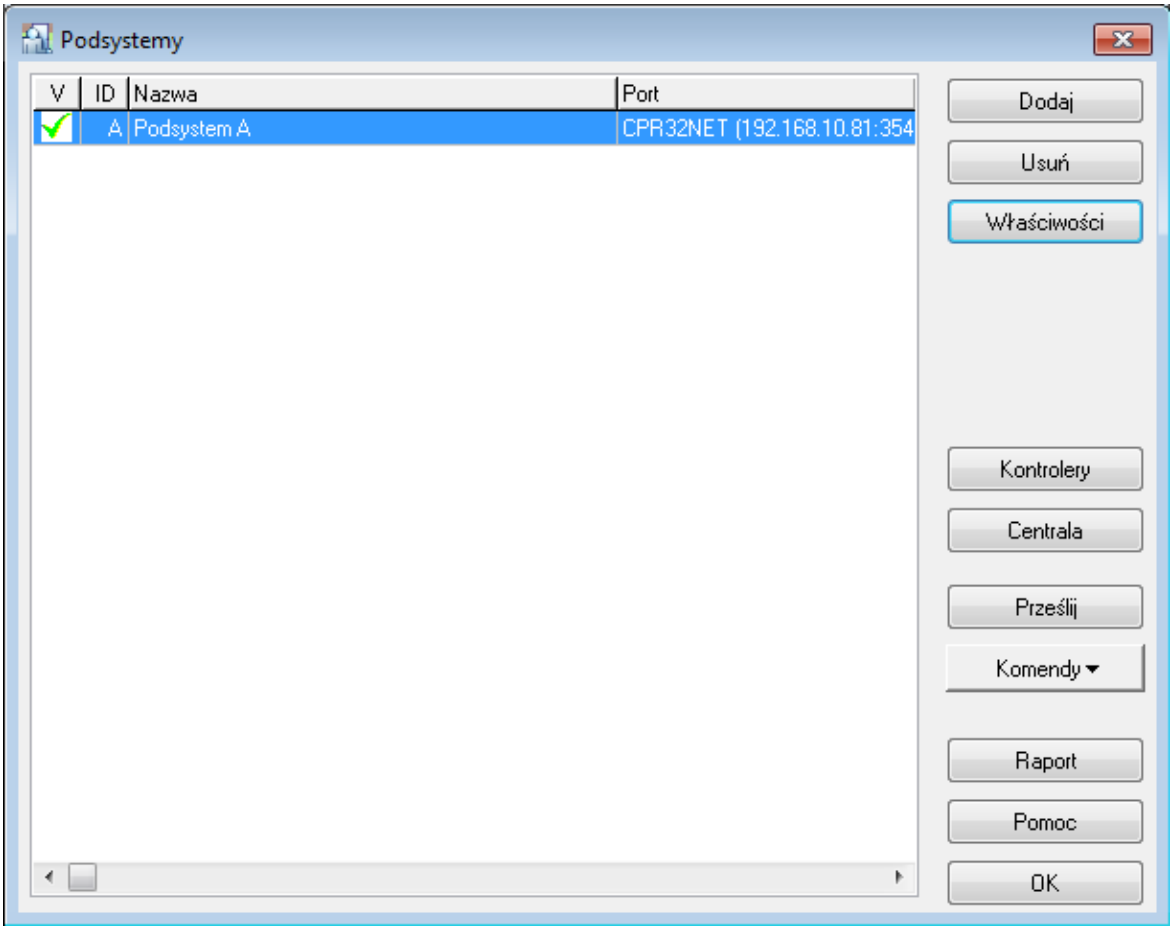
Rysunek 3.43. *Raport Strefy*

3.2.8. Polecenie Podsystemy

System Kontroli Dostępu RACS 4 może składać się z maksymalnie 250 podsystemów. W skład każdego z nich mogą wejść maksymalnie 32 kontrolery dostępu wraz z terminalami. Nie mniej maksymalna ilość kontrolerów w całym systemie nie powinna przekraczać 1000.

Każdy podsystem jest podłączony do komputera zarządzającego za pośrednictwem portu poprzez wskazany interfejs komunikacyjny (np. UT-2USB, UT-4DR). Rolę interfejsu komunikacyjnego może również pełnić centrala CPR32-NET.

Wybranie polecenia **System**/**Podsystemy** powoduje wyświetlenie okna zawierającego listę podsystemów w systemie kontroli dostępu (rysunek 3.44).



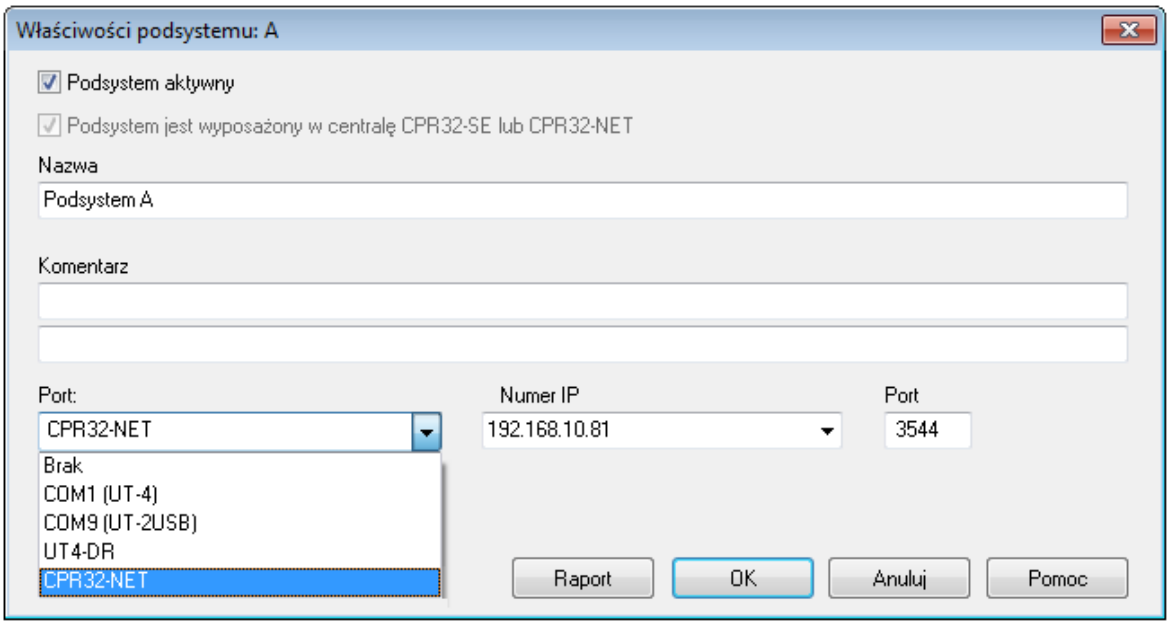
Rysunek 3.44. *Kartoteka podsystemów*

Z poziomu kartoteki podsystemów można wykonać następujące operacje:

- dodawanie nowego podsystemu (przycisk **Dodaj**),
- usuwanie podsystemu (przycisk **Usuń**),
- modyfikacja właściwości podsystemu (przycisk **Właściwości**),
- zarządzanie listą kontrolerów podsystemu (przycisk **Kontrolery**),
- wyświetlenie ustawień centrali CPR32-SE/CPR32-NET (przycisk **Centrala**),
- przesłanie ustawień do wszystkich kontrolerów we wskazanym podsystemie (przycisk **Prześlij**),
- wykonanie komend dla wskazanego podsystemu (przycisk **Komendy**),
- wygenerowanie raportu **Podsystemy** (przycisk **Raport**).

3.2.8.1. Dodawanie nowego podsystemu

Aby dodać nowy podsystem, należy kliknąć przycisk **Dodaj** w oknie kartoteki podsystemów. Wyświetli się okno dialogowe **Właściwości podsystemu** (rysunek 3.45).



Rysunek 3.45. *Dodawanie nowego podsystemu*

Dla nowo definiowanego podsystemu należy:

- określić czy podsystem jest aktywny, czy nie (system może być nieaktywny na przykład na etapie jego konfigurowania),
- zaznaczyć opcję określającą, czy podsystem jest wyposażony w centralę CPR,
- określić nazwę podsystemu (opcjonalnie z komentarzami),
- przypisać port komunikacyjny,
- opcjonalnie określić typ interfejsu.

Na szczególną uwagę zasługują operacje przypisywania portu komunikacyjnego, określania typu interfejsu, oraz oznaczenia, czy podsystem jest wyposażony w centralę CPR. Jeśli wykona się je nieprawidłowo, to komunikacja z podsystemem będzie niemożliwa.

Jeśli system jest wyposażony w centralę CPR32-SE, a instalator nie zaznaczy właściwego pola wyboru na etapie definiowania podsystemu, to program PR Master nie będzie w stanie prawidłowo komunikować się z urządzeniami. W związku z tym, pojawią się konflikty adresów, na przykład, podczas wykrywania kontrolerów.

Jeśli podczas definiowania nowego portu wirtualnego (na przykład dla urządzenia UT-4 lub UT-2USB) jest podłączona centrala CPR32-SE, system Windows może błędnie rozpoznać komunikację w porcie wirtualnym jako urządzenie **Microsoft Ballpoint**. W związku z tym, nie można przypisać portu do podsystemu, ponieważ program PR Master nie może otworzyć portu COM. Rozwiązaniem jest usunięcie urządzenia **Microsoft BallPoint** z systemu Windows (**Panel Sterowania**/**Menedżer urządzeń**) lub odłączenie centrali CPR32-SE na czas instalacji wirtualnego portu COM.

Typy portów komunikacyjnych

Każdy podsystem systemu kontroli dostępu jest podłączony do komputera zarządzającego za pomocą osobnego, dedykowanego kanału komunikacyjnego (fizycznego bądź wirtualnego). Do podłączenia podsystemu z komputerem wykorzystuje się następujące interfejsy komunikacyjne:

- UT-2 — służy do podłączenia podsystemu przez fizyczny port szeregowy RS232,

- UT-2USB/RCI-2 — służy do podłączenia podsystemu przez port USB,
- UT-4/UT-4DR— służą do podłączenia podsystemu przez sieć Ethernet.

Należy również wspomnieć, że centrala CPR32-NET posiada wbudowany interfejs komunikacyjny Ethernet-RS485, więc gdy podsystem jest wyposażony w ten typ centrali to instalacja jednego z wyżej wymienionych interfejsów komunikacyjnych jest zbędna.

Konfiguracja portów komunikacyjnych

Po zainstalowaniu danego interfejsu komunikacyjnego wystarczy go wybrać w polu **Port**. W przypadku interfejsu UT-2USB wyświetlana jest podpowiedź ułatwiająca wybór odpowiedniego portu COM (rysunek 3.45).

Urządzenia UT-4DR oraz CPR32-NET wymagają nie tylko ich wybrania w polu Port ale również wybrania z listy lub ręcznego wpisania adresu IP w polu **Numer IP** (rysunek 3.45)

Z kolei interfejs do komunikacji przez sieć Ethernet o oznaczeniu UT-4 wymaga jawnego zainstalowania sterowników i przyporządkowania wirtualnego portu COM. Aby go zainstalować, należy skorzystać z narzędzia **Digi Configurator**. Po skorzystaniu z narzędzia, port wirtualny związany z urządzeniem stanie się dostępny w systemie PR Master i będzie można za jego pośrednictwem podłączyć podsystem.

3.2.8.2. Usuwanie podsystemu

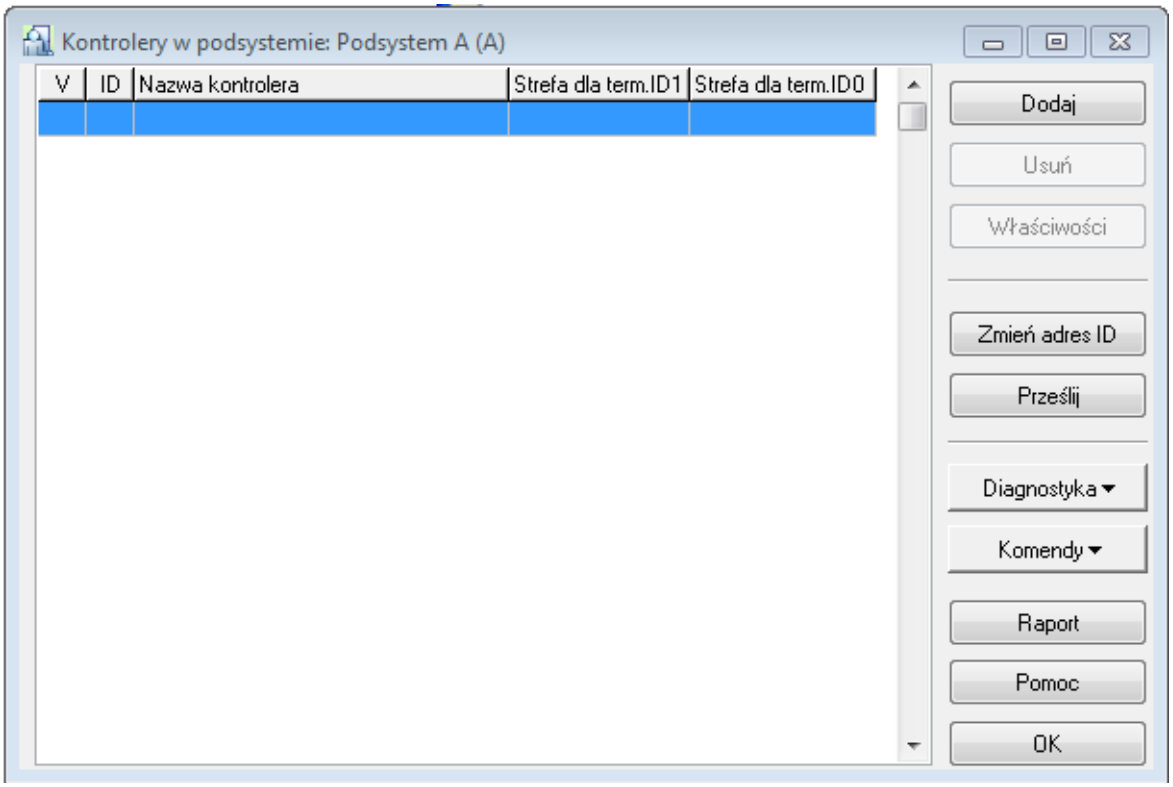
Do usuwania podsystemu służy przycisk **Usuń** w oknie kartoteki kontrolerów (rysunek 3.46). Jeśli podsystem zawiera jakieś kontrolery, to wybranie tego polecenia spowoduje jedynie wyświetlenie ostrzeżenia informującego o konieczności usunięcia wszystkich kontrolerów danego podsystemu. Można to zrobić za pośrednictwem przycisku **Kontrolery**. Jeśli lista kontrolerów jest pusta, system pozwoli na usunięcie podsystemu. Wcześniej jednak wyświetli okno dialogowe z pytaniem o potwierdzenie zamiaru usunięcia.

3.2.8.3. Modyfikacja właściwości podsystemu

Do zmiany niektórych właściwości podsystemu służy przycisk **Właściwości**. Kliknięcie tego przycisku spowoduje wyświetlenie okna dialogowego **Właściwości podsystemu** — takiego samego, jak to, które wyświetlało się na etapie dodawania nowego podsystemu. Z tego poziomu można zdezaktywować podsystem, zmienić ustawienia określające wyposażenie systemu w centralę CPR, zmienić nazwę, a także zmodyfikować ustawienia typu portu i interfejsu. Można również wyświetlić raport opisujący właściwości wybranego podsystemu.

3.2.8.4. Zarządzanie kontrolerami w podsystemie

Przycisk **Kontrolery** w oknie kartoteki podsystemów umożliwia zarządzanie kontrolerami danego podsystemu. Jego kliknięcie powoduje wyświetlenie listy kontrolerów w podsystemie (rysunek 3.46).



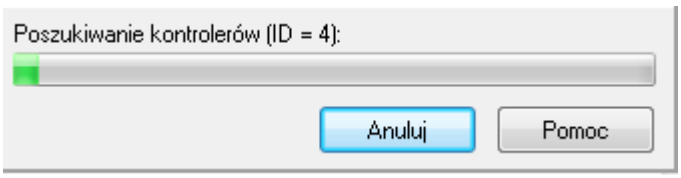
Rysunek 3.46. *Lista kontrolerów w podsystemie — po zdefiniowaniu nowego podsystemu jest pusta*

Z tego poziomu można wykonać następujące operacje dotyczące kontrolerów danego podsystemu:

- dodawać kontrolery,
- usuwać kontrolery,
- wyświetlać i modyfikować właściwości kontrolerów,
- zmieniać adres ID,
- przesyłać dane konfiguracyjne do wskazanego kontrolera,
- wykonywać operacje diagnostyczne,
- przesyłać komendy do kontrolera,
- wygenerować raport dotyczący kontrolerów w podsystemie.

Dodawanie kontrolerów w podsystemie

Po zdefiniowaniu nowego podsystemu, jego lista kontrolerów jest pusta. Aby dodać kontrolery, należy kliknąć przycisk **Dodaj**. System przystąpi do operacji wyszukiwania kontrolerów. W tym czasie wyświetla się wskaźnik postępu pokazujący aktualnie przeszukiwane adresy ID (rysunek 3.47).

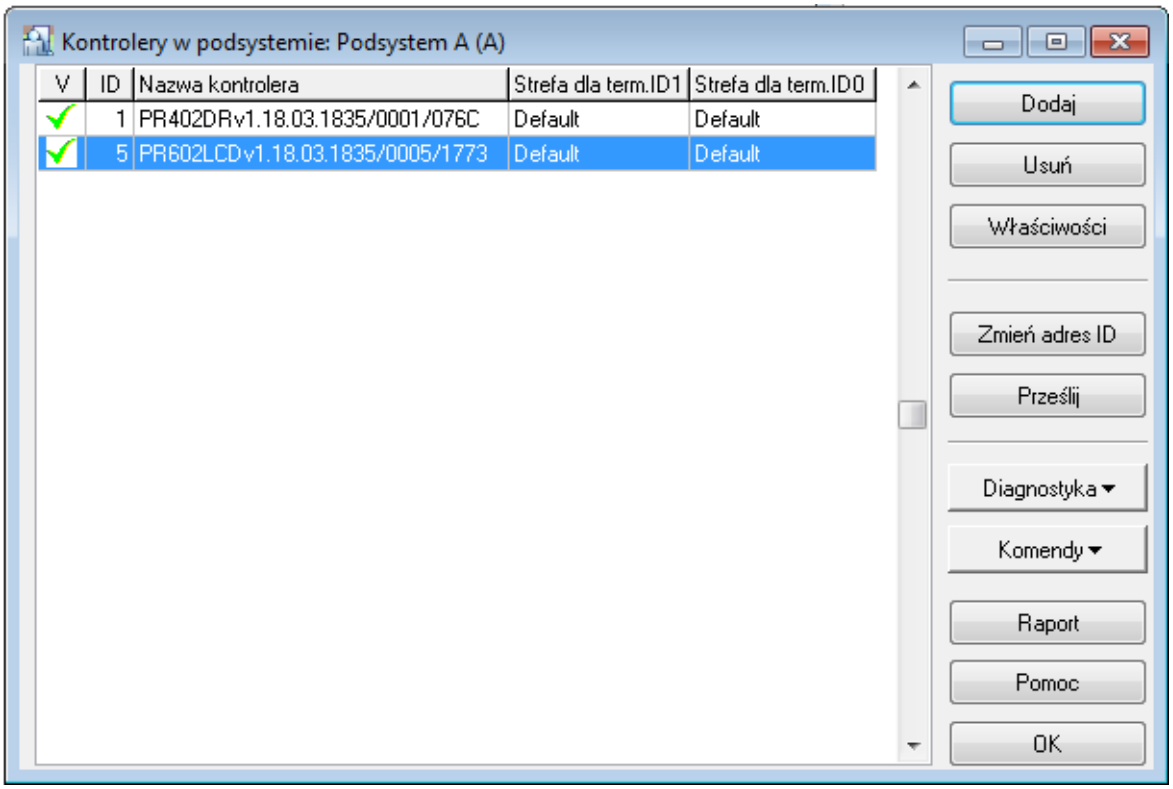


Rysunek 3.47. *Poszukiwanie kontrolerów w podsystemie*

Znalezione kontrolery są natychmiast wyświetlane w oknie z listą kontrolerów w podsystemie. Instalator może w każdej chwili przerwać proces wyszukiwania (np. jeśli jego zdaniem zostały wyszukane wszystkie kontrolery) poprzez wciśnięcie przycisku **Anuluj**. Jeśli proces wyszukiwania nie zostanie przerwany, system przeszuka adresy w zakresie od 00 do 100 i wyświetli końcowy komunikat o zakończeniu operacji wyszukiwania kontrolerów.

Jeśli podczas operacji wykrywania kontrolerów pojawi się duża liczba konfliktów, może to być oznaką, że system jest wyposażony w centralę CPR, a instalator nie zaznaczył właściwego pola wyboru na etapie definiowania podsystemu. W takim przypadku należy wrócić do okna właściwości podsystemu i zaznaczyć opcję wskazującą na to, że w podsystemie działa centrala CPR.

Po operacji dodawania kontrolerów, okno z listą kontrolerów w podsystemie może mieć następującą postać (rysunek 3.48).



Rysunek 3.48. *Lista kontrolerów po przeprowadzonej operacji wyszukiwania*

Jak można zauważyć, uaktywniły się teraz dwa przyciski: **Usuń** i **Właściwości** pozwalające odpowiednio na usuwanie kontrolera z podsystemu lub na zmianę jego konfiguracji.

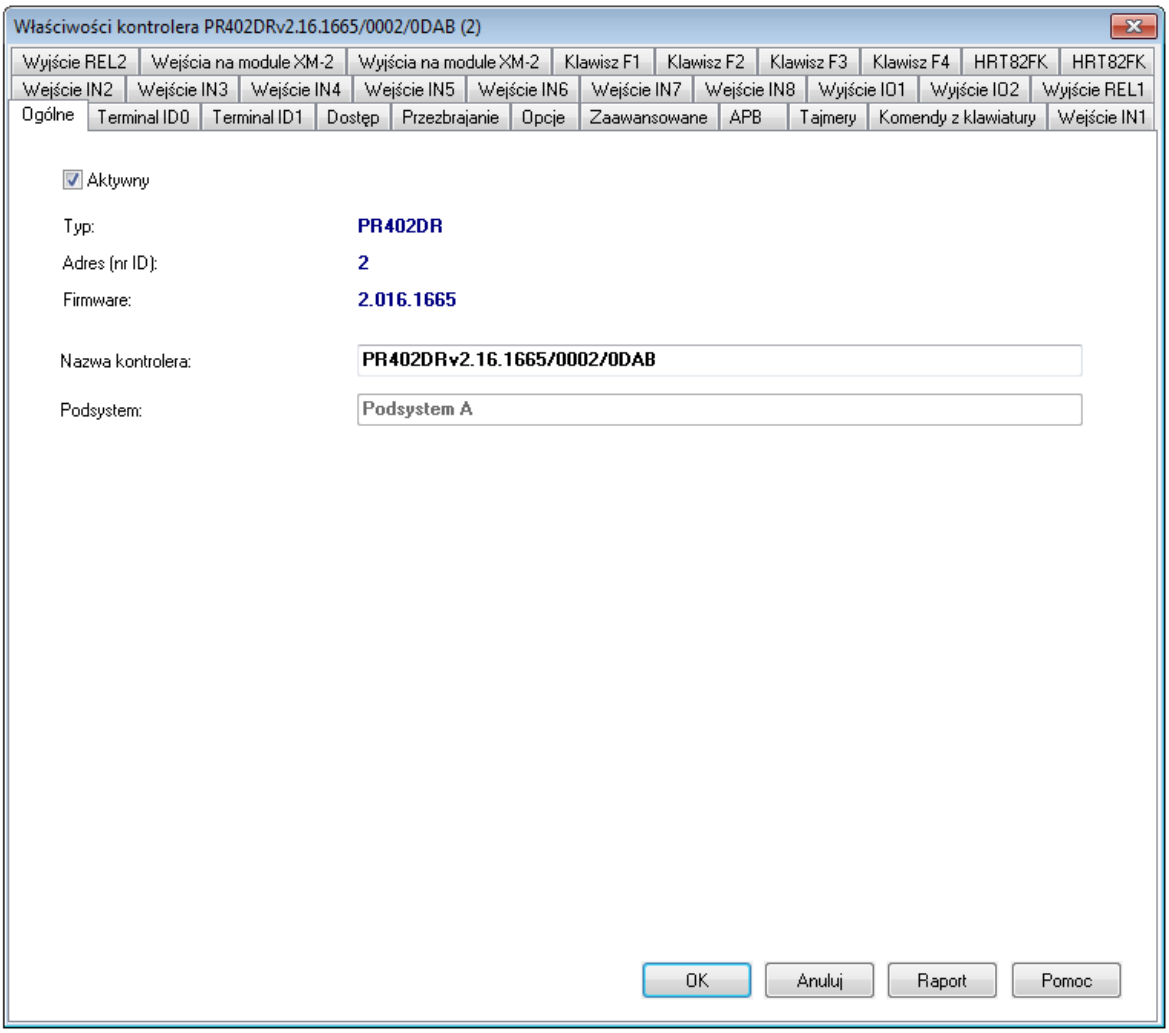
Usuwanie kontrolerów z podsystemu

Aby usunąć kontroler z podsystemu, należy kliknąć przycisk **Usuń**. Standardowo, przed usunięciem system wyświetli pytanie o potwierdzenie zamiaru usunięcia. Jeśli użytkownik odpowie twierdząco, kontroler zostanie usunięty z podsystemu.

Usuwanie kontrolera z podsystemu ma sens tylko wtedy, gdy kontroler został wcześniej fizycznie odłączony od systemu kontroli dostępu. W przypadku usunięcia kontrolera, który fizycznie występuje w systemie, program PR Master przestanie się z nim komunikować, w efekcie czego pozostaną na nim stare ustawienia uprawnień, użytkowników, itp. W związku z tym, wykonując operację usunięcia należy zachować ostrożność. W przypadku przypadkowego usunięcia istniejącego kontrolera, należy ponownie przeprowadzić operację wyszukiwania kontrolerów (przycisk **Dodaj**).

Przeglądanie (modyfikowanie) właściwości kontrolerów

Przycisk **Właściwości** wyświetla okno właściwości wybranego kontrolera. Jest to mechanizm pozwalający na zdefiniowanie konfiguracji kontrolera. Tę konfigurację należy później przesłać do kontrolera celem dokonania właściwej konfiguracji. W zależności od typu kontrolera okno właściwości może mieć różną postać. Przykład okna **Właściwości** dla kontrolera PR302 pokazano na rysunku 3.49.



Rysunek 3.49. *Właściwości kontrolera PR402DR*

Jak można zobaczyć na rysunku, okno jest podzielone na wiele zakładek i umożliwia przeprowadzenie szczegółowej konfiguracji kontrolera. Z tego poziomu, między innymi, przydziela się terminale kontrolera do stref dostępu, ustawia tryb identyfikacji oraz definiuje sposób działania klawiszy funkcyjnych.

Dokładny opis wszystkich ustawień z uwzględnieniem wielu typów kontrolerów wykracza poza ramy niniejszej instrukcji. W zdecydowanej większości przypadków ustawienia domyślne pozwalają na korzystanie z kontrolerów w instalacjach KD. Aby uzyskać szczegółowe informacje na temat opcji konfiguracyjnych, należy sięgnąć do instrukcji **Opis funkcjonalny kontrolerów serii PRxx2** lub instrukcji **Opis funkcjonalny kontrolerów serii PRxx1**.

Zmiana adresu ID kontrolera

Wszystkie kontrolery produkowane przez firmę Roger mają fabrycznie przydzielony adres ID=0. Aby była możliwa komunikacja za pośrednictwem magistrali RS-485, każde z urządzeń podłączonych do magistrali musi mieć przydzielony inny adres (w zakresie od 00 do 99). W związku z tym, na etapie instalacji systemu należy przydzielić poszczególnym kontrolerom unikatowe adresy (muszą być one unikatowe w ramach wybranego podsystemu). Istnieje wiele metod zmiany adresu ID kontrolera i są one szczegółowo opisane w instrukcjach instalacyjnych poszczególnych kontrolerów. Jedna z metod polega na wykorzystaniu programu PR Master.

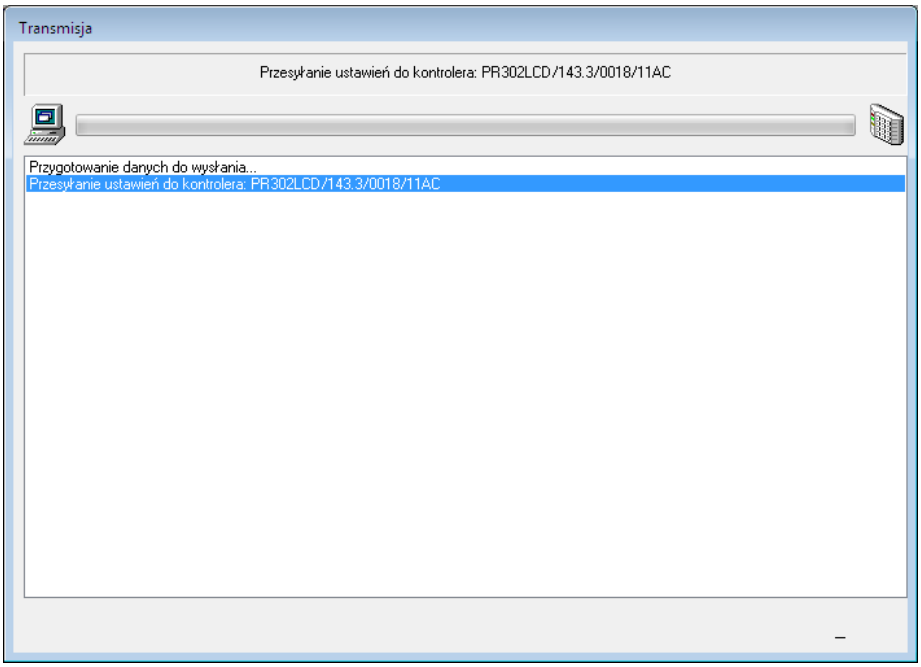
Aby zmienić adres ID wybranego kontrolera, należy kliknąć przycisk **Zmień adres ID**. Wyświetli się okno dialogowe **Zmiana numeru ID kontrolera** (rysunek 3.50).

Rysunek 3.50. *Zmiana adresu ID kontrolera*

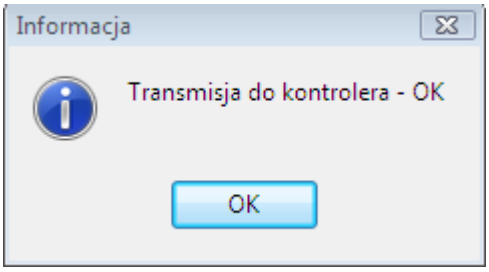
Po wprowadzeniu nowego adresu i zatwierdzeniu go przyciskiem **OK**, adres zostanie on automatycznie przesłany do kontrolera. Na liście kontrolerów wyświetli się uaktualniony adres.

Przesyłanie danych konfiguracyjnych do kontrolera

Po wprowadzeniu zmian konfiguracyjnych w oknie właściwości kontrolera, zmodyfikowaną konfigurację należy przesłać do kontrolera. Dopiero wtedy zmiany zaczną obowiązywać w systemie kontroli dostępu. W celu przesłania konfiguracji, należy wskazać kontroler na liście kontrolerów i kliknąć przycisk **Prześlij**. Jeśli w tym momencie w kontrolerze są zgromadzone jakieś zdarzenia, system przed przesłaniem ustawień ściągnie zdarzenia do bazy danych. Następnie wyświetli okno przesyłania danych do kontrolera (rysunek 3.51). Po zakończeniu transmisji wyświetla się okno z informacją o wyniku transmisji (rysunek 3.52).



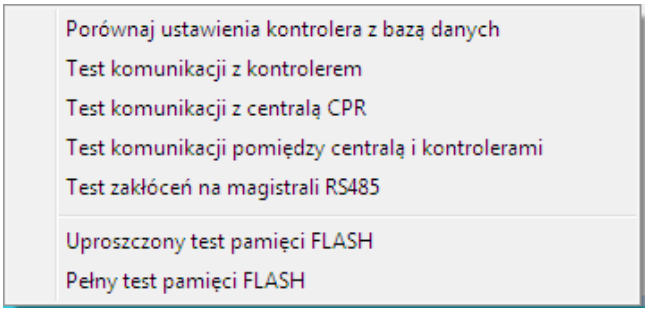
Rysunek 3.51. *Przesyłanie ustawień do kontrolera*



Rysunek 3.52. *Przesyłanie ustawień do kontrolera zakończone sukcesem*

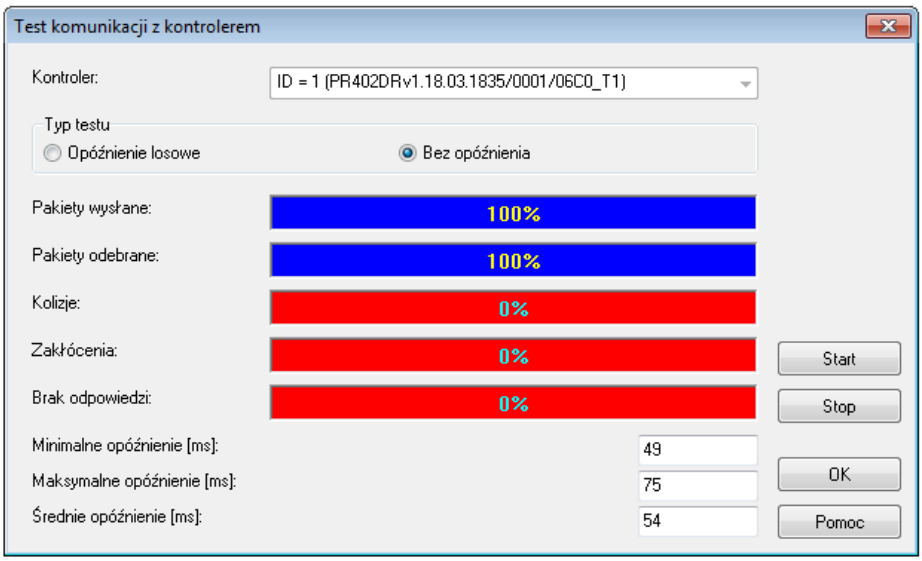
Wykonywanie operacji diagnostycznych

Przycisk **Diagnostyka** daje dostęp do menu operacji diagnostycznych (rysunek 3.53). Z tego menu można wykonać szereg operacji mających na celu weryfikację poprawności działania systemu. Można porównać, czy ustawienia w kontrolerze są takie same, jak w programie PR-Master, sprawdzić, czy program może się komunikować z kontrolerem i centralą CPR, sprawdzić komunikację pomiędzy centralą CPR a kontrolerami, zbadać zakłócenia na magistrali RS-485 oraz wykonać pełny lub uproszczony test pamięci FLASH.



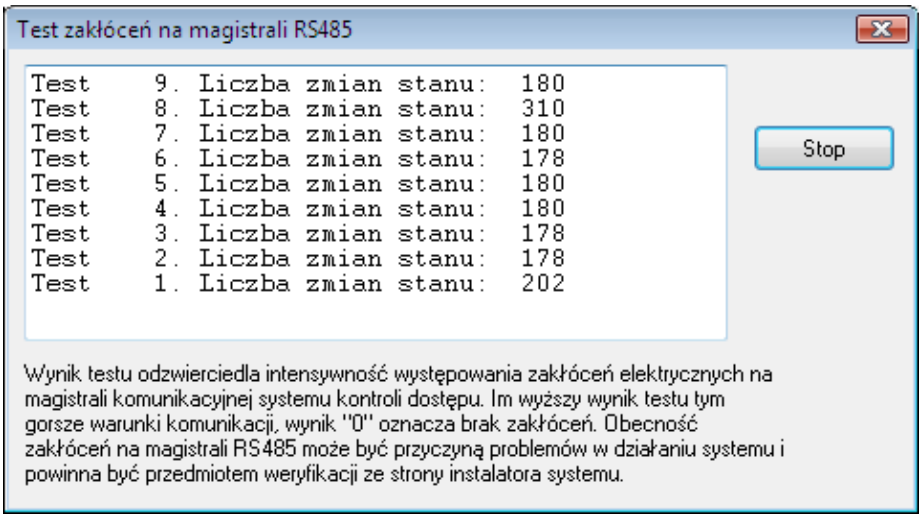
Rysunek 3.53. *Przesyłanie ustawień do kontrolera zakończone sukcesem*

Większość testów komunikacji dostępnych z poziomu tego menu jest wykonywanych na poziomie protokołu komunikacyjnego. Ze względu na bardzo dużą odporność systemu RACS 4 na zakłócenia, testy te mogą dawać zadowalające wyniki nawet wtedy, gdy na magistrali występują poważne zakłócenia elektryczne (rysunek 3.54).



Rysunek 3.54. *Test komunikacji z kontrolerem*

Najbardziej dokładnym testem umożliwiającym wykrycie problemów elektrycznych na magistrali, jest **Test zakłóceń na magistrali RS485** (rysunek 3.55). Uzyskanie liczby zmian stanu większej od zera oznacza, że na magistrali występują zakłócenia.

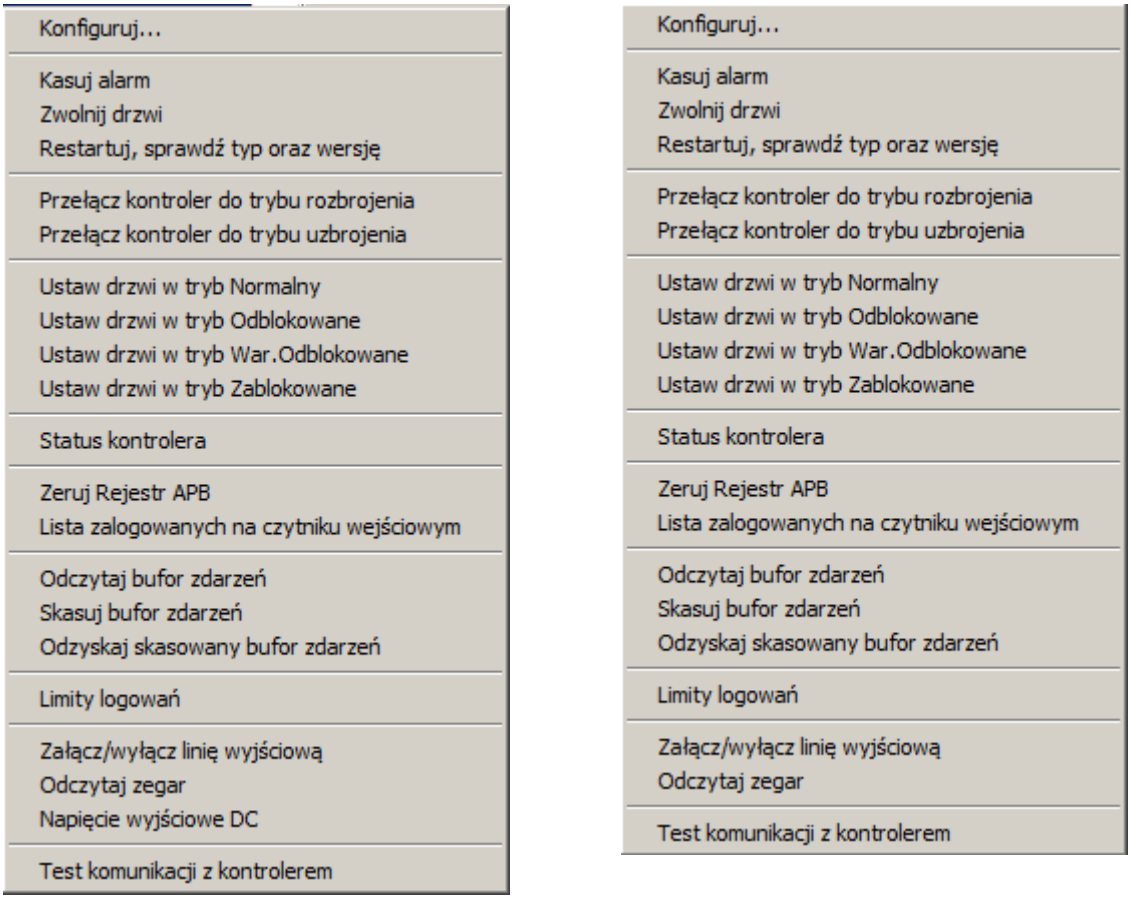


Rysunek 3.55. *Test zakłóceń na magistrali RS-485*

Uzyskanie wyników testów komunikacji świadczących o zakłóceniach może być sygnałem zakłóceń, ale również nieprawidłowego skonfigurowania podsystemu. Jeśli na przykład instalator nie zaznaczy, że system jest wyposażony w centralę CPR, a faktycznie centrala w nim występuje, testy komunikacji będą wykazywać błędy.

Przesyłanie komend do kontrolera

Przycisk **Komendy** daje dostęp do menu komend dostępnych dla wybranego kontrolera. W zależności od typu kontrolera zawartość menu **Komendy** jest różna. Na rysunku 3.56a pokazano menu **Komendy** dla kontrolera PR402DR, natomiast na rysunku 3.56b zaprezentowano analogiczne menu dla kontrolera PR602LCD.



a **b**

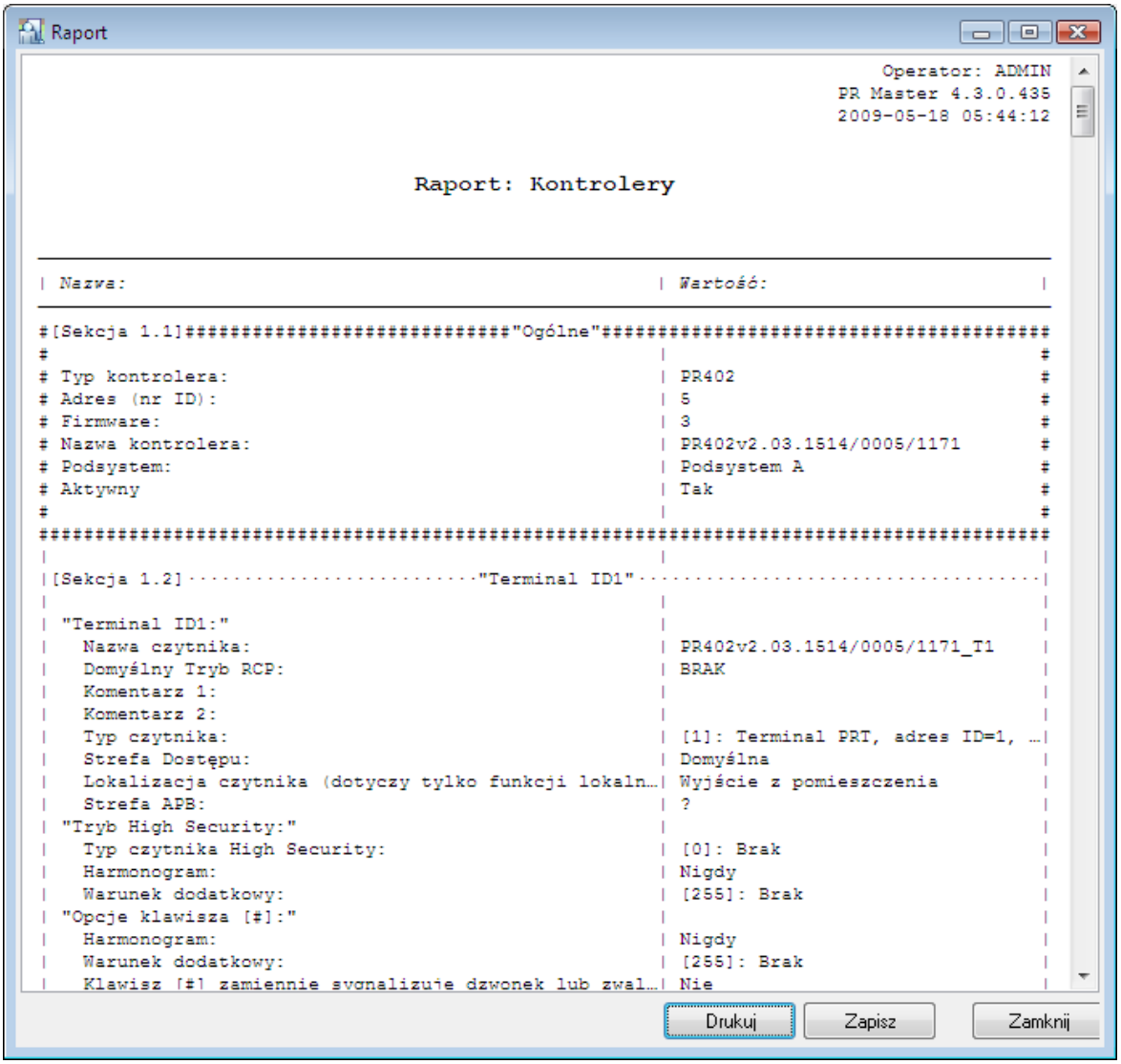
Rysunek 3.56. *Menu Komendy: (a) kontroler PR402DR; (b) kontroler PR602LCD*

Jak można zauważyć menu komend dla kontrolera PR402DR zawiera dodatkową komendę **Napięcie wyjściowe DC**, która jest niedostępna dla kontrolera PR602LCD.

Dokładny opis wszystkich komend z uwzględnieniem wielu typów kontrolerów wykracza poza ramy niniejszej instrukcji. Aby uzyskać szczegółowe informacje na temat komend, należy sięgnąć do instrukcji **Opis funkcjonalny kontrolerów serii PRxx2** lub instrukcji **Opis funkcjonalny kontrolerów serii PRxx1**.

Generowanie raportu dotyczącego kontrolerów w podsystemie

Po wprowadzeniu wszystkich danych konfiguracyjnych do kontrolera i przetestowaniu jego działania, można sporządzić drukowany raport w celu udokumentowania danych konfiguracji kontrolera. Do tego celu służy przycisk **Raport** w oknie kartoteki kontrolerów danego podsystemu. Aby sporządzić raport, należy wskazać kontroler i kliknąć przycisk **Raport**. Spowoduje to wyświetlenie raportu **Kontrolery** w oknie **Raport** (rysunek 3.57).



Rysunek 3.57. *Raport Kontrolery*

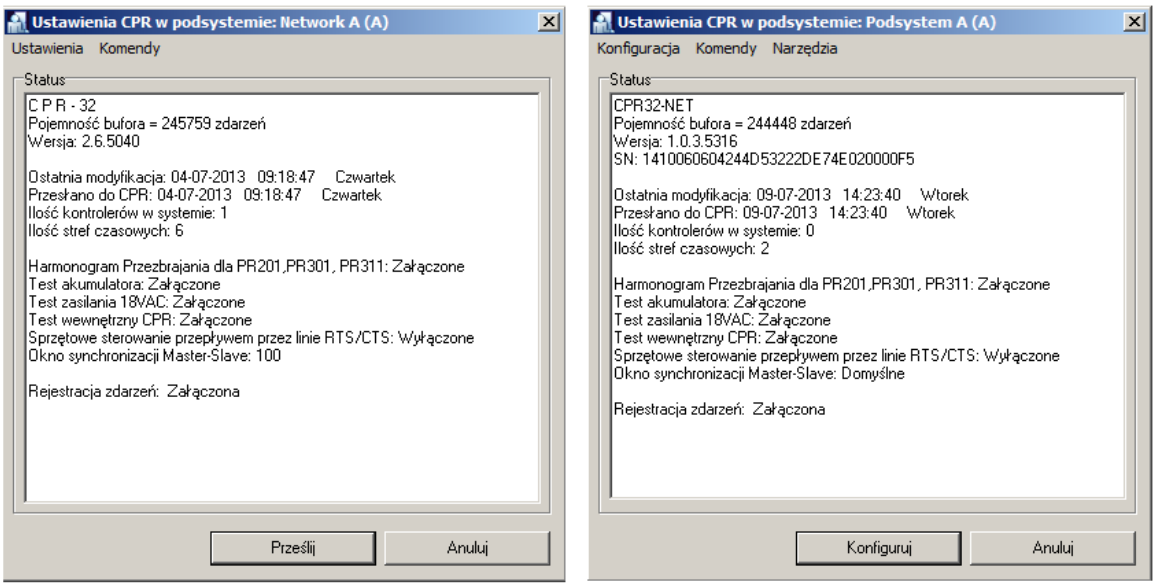
Raport **Kontrolery** zawiera szczegółowe informacje na temat konfiguracji wybranego kontrolera. Warto sporządzić drukowaną kopię takiego raportu po pomyślnym skonfigurowaniu systemu. Może być ona pomocna podczas rozwiązywania problemów w dalszej fazie użytkowania systemu.

3.2.8.5. Wyświetlanie ustawień centrali CPR

Centrala CPR32-SE jest urządzeniem, które spełnia w systemie RACS 4 rolę zewnętrznego bufora zdarzeń i synchronizuje ustawienia czasu na kontrolerach. Obecność centrali CPR32-SE w systemie RACS 4 jest opcjonalna i wynika z wymagań funkcjonalnych danej instalacji. W przypadku kontrolerów serii PRxx2, centrala CPR32-SE oferuje jedynie funkcje globalne (globalny APB i strefy alarmowe), natomiast w przypadku kontrolerów serii PRxx1 oferuje dodatkowo bufor zdarzeń i zegar czasu rzeczywistego, gdyż kontrolery tej serii w odróżnieniu od serii PRxx2 nie są w nie wyposażone.

Z kolei centrala CPR32-NET zapewnia te same funkcjonalności co CPR32-SE i dodatkowo umożliwia integrację z centralami alarmowymi serii INTEGRA (SATEL) oraz zamkami bezprzewodowymi systemu APERIO (ASSA ABLOY), pełni rolę interfejsu komunikacyjnego Ethernet-RS485, jak również umożliwia obsługę bufora zdarzeń na zewnętrznej karcie pamięci (30 mln zdarzeń), pozwala na synchronizację czasu z zewnętrznym serwerem NTP i zapewnia szyfrowanie komunikacji na bazie standardu AES128 CBC.

Do wyświetlania ustawień centrali CPR służy przycisk **Centrala**. Jeśli podsystem nie jest w nią wyposażony, przycisk ten jest nieaktywny. Kliknięcie przycisku spowoduje wyświetlenie okna dialogowego zawierającego ustawienia centrali działającej w podsystemie (rysunek 3.58).



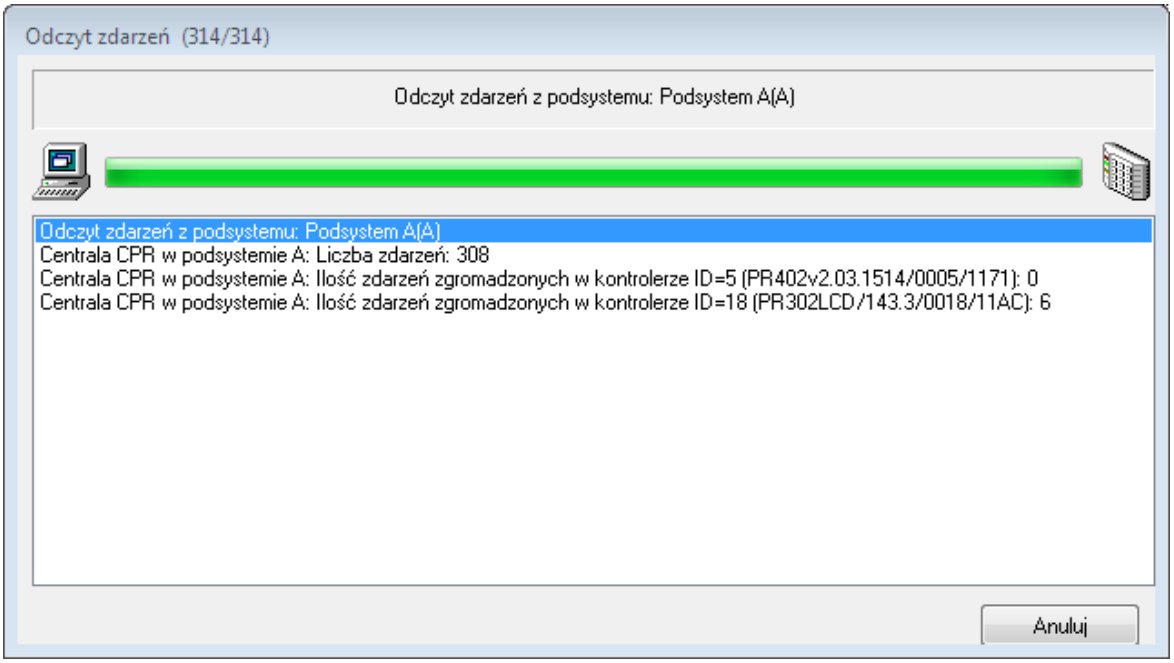
Rysunek 3.58. *Ustawienia centrali CPR32-SE i CPR32-NET*

Użytkownik może obejrzeć bieżące ustawienia i kliknąć **OK** lub wybrać przycisk **Prześlij/Konfiguruj** w celu wysłania ustawień z programu PR Master do centrali.

3.2.8.6. Przesyłanie ustawień do kontrolerów i centrali

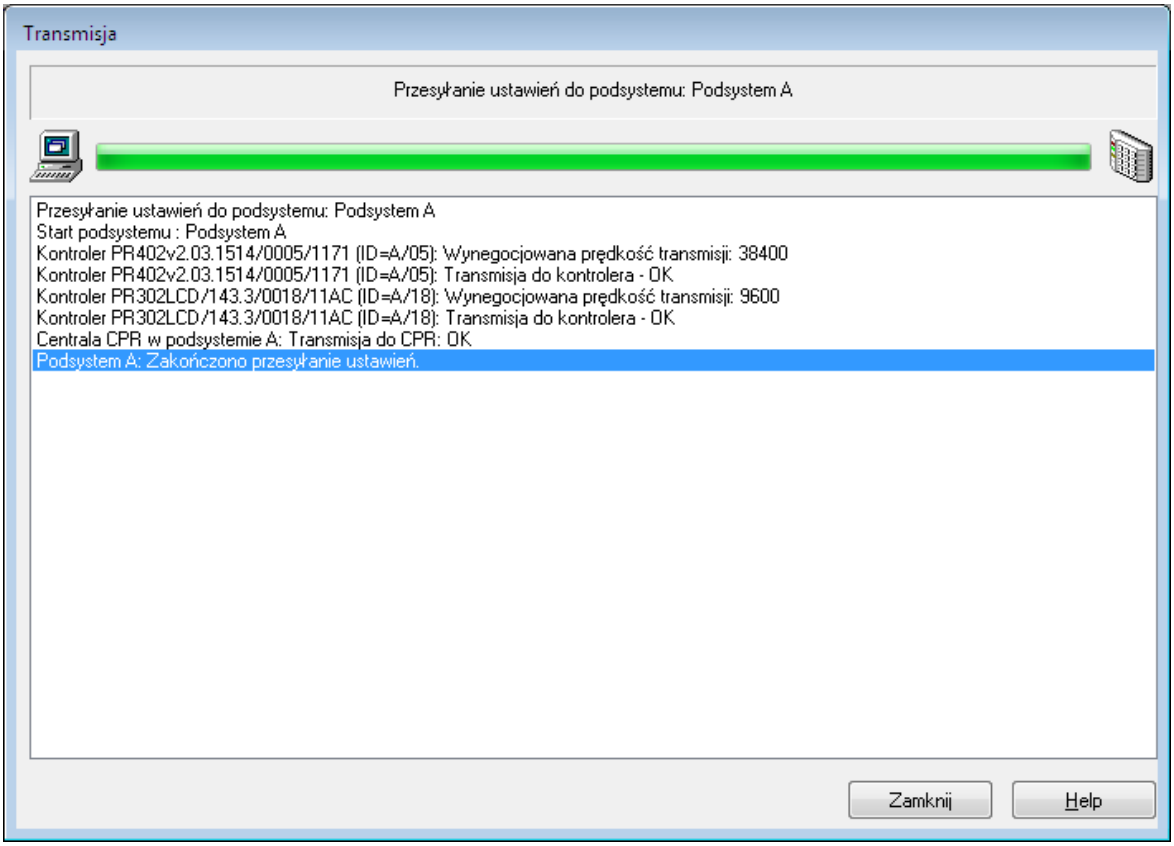
Przycisk **Prześlij** w oknie kartoteki podsystemów służy do przesyłania ustawień do wszystkich kontrolerów oraz centrali CPR we wskazanym podsystemie. W przypadku, gdy podsystem zawiera wiele kontrolerów, operacja ta może być długotrwała, dlatego należy wykonywać ją jak najrzadziej — po wprowadzeniu wszystkich niezbędnych zmian.

Operację przesyłania ustawień do kontrolerów inicjuje kliknięcie przycisku **Prześlij**. Jeśli w tym momencie w kontrolerach lub w centrali są zgromadzone jakieś zdarzenia, to zostaną one pobrane do bazy danych programu PR Master. Podczas ściągania zdarzeń, system wyświetli okno informacyjne zawierające dane o postępach operacji odczytu (rysunek 3.59)



Rysunek 3.59. *Odczyt zdarzeń z podsystemu przed operacją przesyłania ustawień*

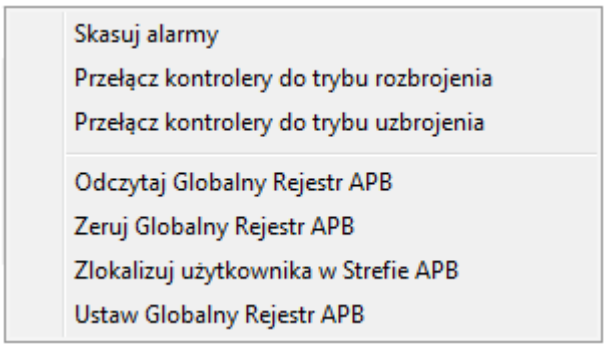
Po wyświetleniu komunikatu o zakończeniu odczytu zdarzeń system przechodzi do operacji przesyłania danych do urządzeń w podsystemie (rysunek 3.60).



Rysunek 3.60. *Przesyłanie ustawień do podsystemu — okno postępu operacji*

3.2.8.7. Wykonywanie komend dla podsystemu

Przycisk **Komendy** w oknie kartoteki podsystemów wyświetla menu komend(rysunek 3.61), które pozwala na wykonywanie komend dla podsystemu.



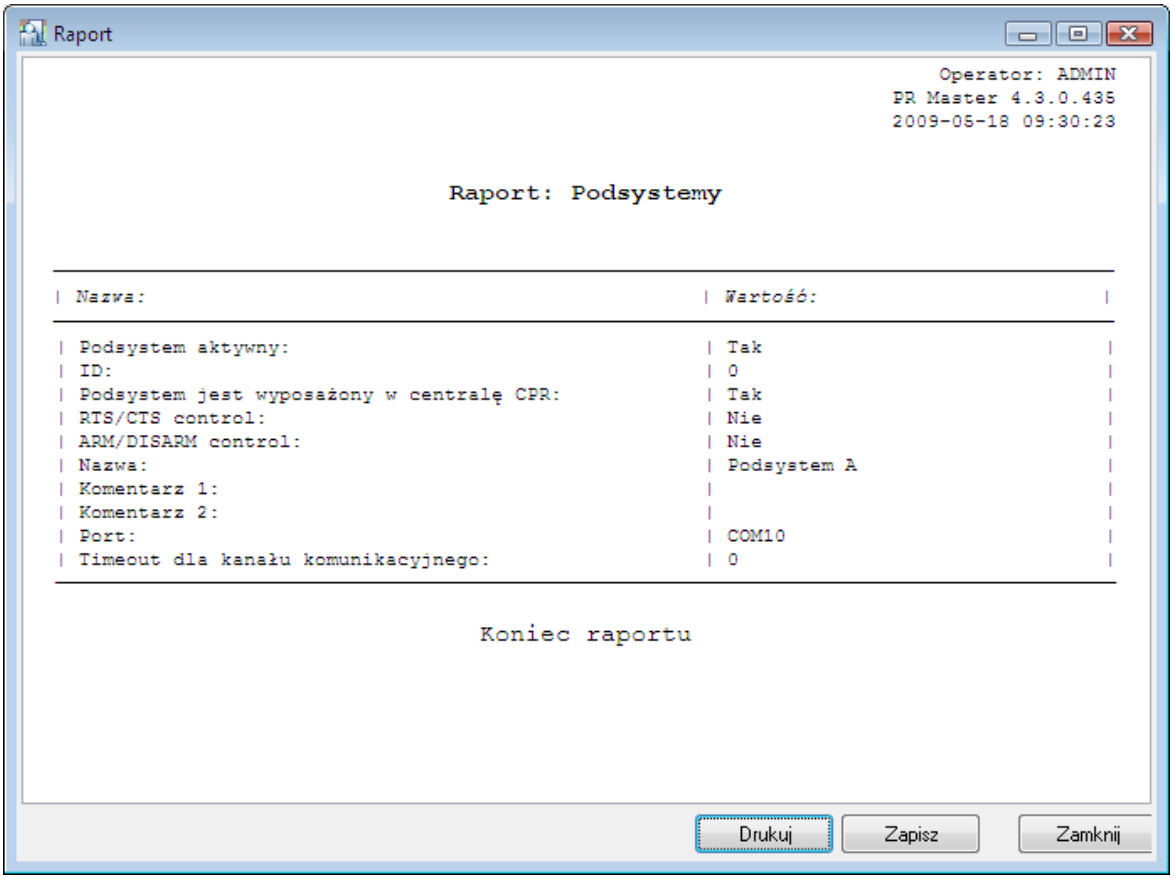
Rysunek 3.61. *Menu Komendy w oknie kartoteki podsystemów*

Menu pozwala na wykonywanie następujących operacji:

- **Skasuj alarmy** — kasowanie wszystkich alarmów na wszystkich kontrolerach w podsystemie. Opcja ta jest przydatna w sytuacji, gdy nie chcemy czekać domyślnych 3 minut, zanim stan alarmu zniknie samoczynnie oraz chcemy wykonać tę operację jednocześnie dla wszystkich kontrolerów w podsystemie.
- **Przełącz kontrolery do trybu rozbrojenia** — przełącza wszystkie kontrolery w podsystemie do trybu rozbrojenie.
- **Przełącz kontrolery do trybu uzbrojenia** — przełącza wszystkie kontrolery w podsystemie do trybu uzbrojenie.
- **Odczytaj Globalny Rejestr APB** — funkcja odczytuje bieżący globalny Rejestr APB w podsystemie. Jest to lista użytkowników wraz z informacją o tym, w jakiej strefie APB aktualnie się zalogowali.
- **Zeruj Globalny Rejestr APB** — funkcja zeruje bieżący globalny rejestr APB w podsystemie. Bezpośrednio po zerowaniu każdy z użytkowników systemu ma w globalnym rejestrze APB status nieokreślony (nie można stwierdzić, czy ostatnio zalogował się na wejściu, czy na wyjściu). Od tego momentu system zaczyna stosować zasady APB.
- **Zlokalizuj użytkownika w strefie APB** — funkcja pozwala na wyszukanie, w jakiej strefie APB w danym momencie znajduje się wskazany użytkownik.
- **Ustaw Globalny Rejestr APB** — funkcja pozwala na ręczne przyporządkowanie wskazanego użytkownika do strefy APB. Po wyborze polecenia wyświetla się okno dialogowe, w którym można wskazać użytkownika oraz wybrać dla niego strefę APB. Można też wyzerować status APB wskazanego użytkownika poprzez wybranie zamiast strefy APB pozycji **Zeruj status APB**.

3.2.8.8. Generowanie raportu Podsystemy

Przycisk **Raport** w oknie kartoteki podsystemów generuje sumaryczny raport dotyczący podsystemów zdefiniowanych w systemie RACS 4. Przykładowy raport pokazano na rysunku 3.62.



Rysunek 3.62. *Raport „Podsystemy'*

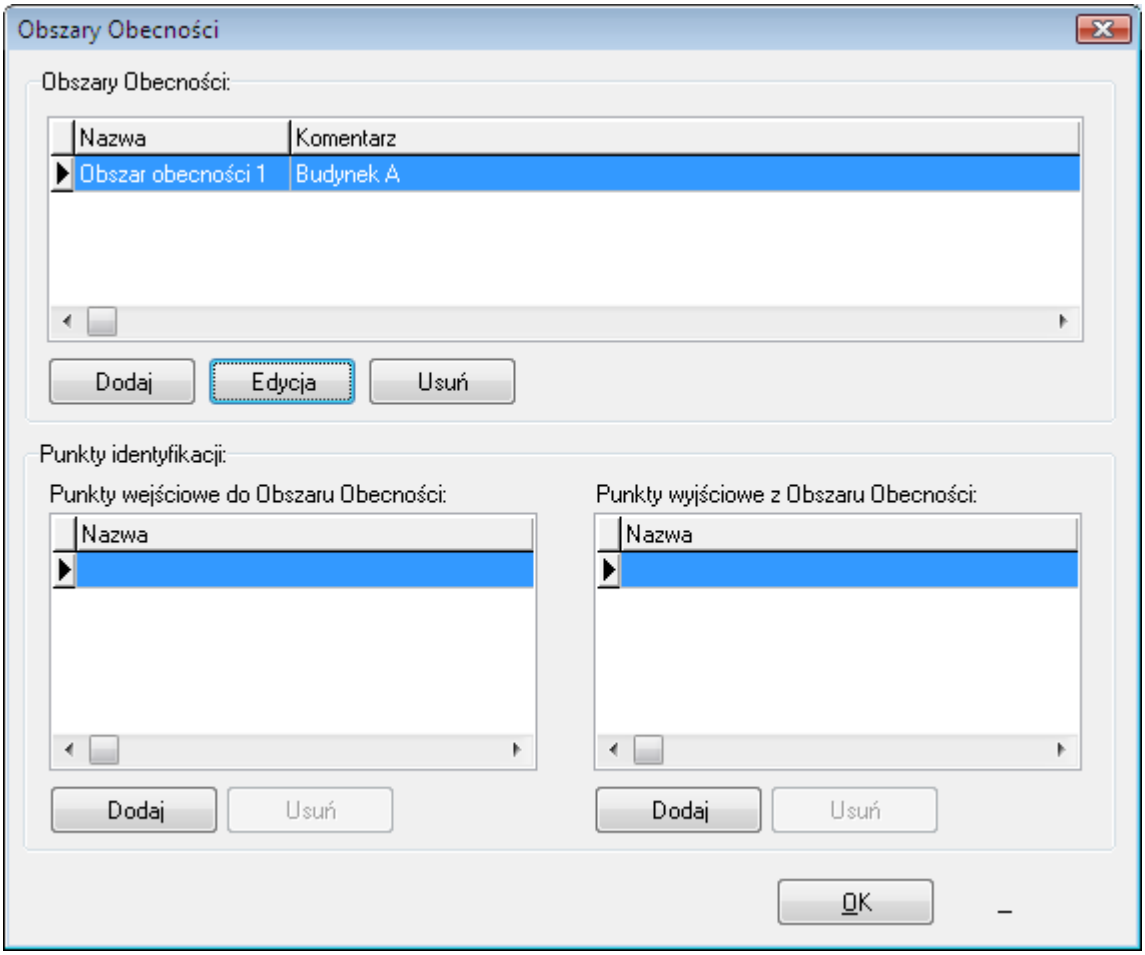
3.2.9. Polecenie Obszary obecności

Obszary obecności to jeden z mechanizmów systemu RACS 4 pozwalający na kontrolowanie miejsca przebywania użytkownika w obiekcie. Obszar obecności należy rozumieć jako fragment obszaru kontrolowanego przez system kontroli dostępu, do którego można wejść poprzez wskazaną grupę punktów identyfikacyjnych oraz wyjść przez odrębną grupę punktów identyfikacyjnych.

Obszary obecności definiuje się w celu sporządzania raportów obecności (**Raporty**/**Obecności**). Raport obecności pokazuje godzinę wejścia/wyjścia użytkownika do/z obszaru oraz łączny czas jego przebywania w obszarze.

W odróżnieniu od rejestracji czasu pracy (RCP), raporty obecności użytkownika systemu nie bazują na deklaracji trybów rejestracji RCP, lecz jedynie na zdefiniowaniu, które urządzenie czytające jest odpowiedzialne za wejście, a które za wyjście z obszaru. Na podstawie raportu obecności można wyliczyć czas przebywania pracownika we wskazanym obszarze (np. hali produkcyjnej).

Wybranie polecenia **Obszary obecności** powoduje otwarcie okna dialogowego **Obszary obecności** (rysunek 3.63)



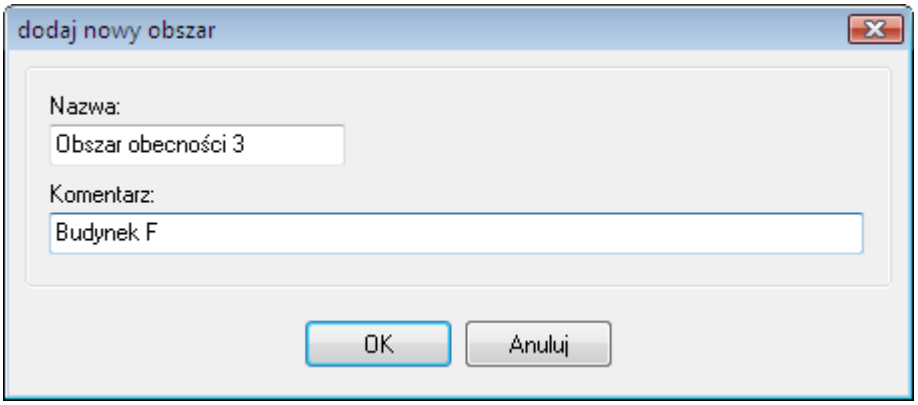
Rysunek 3.63. *Kartoteka obszarów obecności*

Okno pozwala na wykonywanie następujących operacji:

- dodawanie nowego obszaru obecności,
- modyfikowanie istniejącego obszaru obecności,
- usuwanie obszaru obecności,
- dodawanie/usuwanie punktów wejściowych do obszaru obecności,
- dodawanie/usuwanie punktów wyjściowych z obszaru obecności.

3.2.9.1. Dodawanie nowego obszaru obecności

Aby dodać nowy obszar obecności, należy kliknąć przycisk **Dodaj** znajdujący się pod listą obszarów obecności zdefiniowanych w systemie. Wyświetli się okno dialogowe **dodaj nowy obszar** (rysunek 3.64) Należy w nim nadać nazwę obszarowi obecności, wprowadzić opisowy komentarz i kliknąć **OK**.

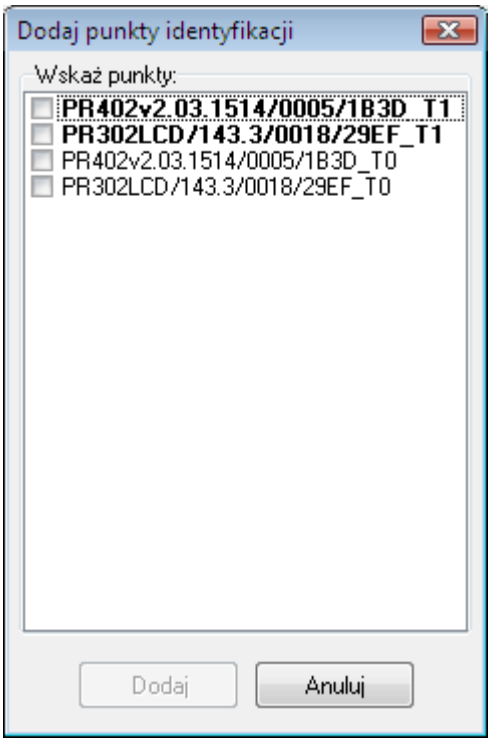


Rysunek 3.64. *Dodawanie nowego obszaru obecności*

Dodawanie/usuwanie punktów wejściowych i wyjściowych do/z obszaru obecności

Bezpośrednio po zdefiniowaniu obszar obecności jest pusty — tzn. nie ma zdefiniowanych punktów wejściowych, ani wyjściowych do (z) obszaru. Dopiero po zdefiniowaniu punktów identyfikacyjnych kontrolujących wejścia i wyjścia, obszar obecności nabiera właściwego sensu (tzn. umożliwia kontrolę przebywania w nim użytkowników).

Aby dodać nowy punkt wejściowy do obszaru obecności, należy kliknąć przycisk **Dodaj** umieszczony pod listą **Punkty wejściowe do Obszaru Obecności**. Wyświetli się okno dialogowe **Dodaj punkty identyfikacji** (rysunek 3.65).



Rysunek 3.63. *Dodawanie punktów wejściowych do obszaru obecności*

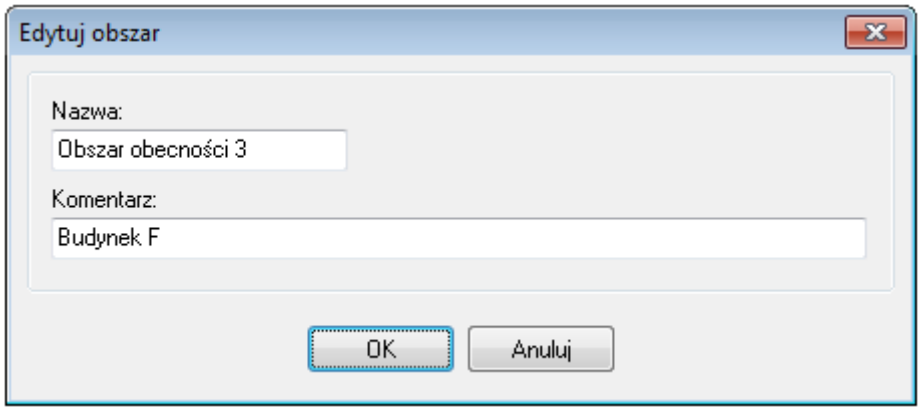
Na liście znajdują się wszystkie punkty identyfikacyjne występujące w systemie, które dotąd nie zostały przyporządkowane jako punkty wejściowe do wskazanego obszaru obecności. Terminale T1 wszystkich kontrolerów w systemie są wyświetlone pogrubioną czcionką. Dodanie punktu wejściowego do obszaru obecności sprowadza się do zaznaczenia pola wyboru obok punktu identyfikacyjnego i kliknięcia przycisku **Dodaj**.

Analogicznie dodaje się punkty wyjściowe z obszaru obecności. W tym przypadku należy skorzystać z przycisku **Dodaj** znajdującego się pod listą **Punkty wyjściowe z Obszaru Obecności**. Wyświetli się okno dialogowe podobne do tego, które pokazano na rysunku 3.65. Różnica polega na tym, że lista nie zawiera punktów identyfikacyjnych wybranych wcześniej jako punkty wejściowe do danego obszaru.

W celu usunięcia punktu wejściowego/wyjściowego do/z obszaru obecności, należy użyć przycisku **Usuń** znajdującego się pod właściwą listą. Program usunie wskazany punkt identyfikacyjny bez wyświetlania dalszych ostrzeżeń.

3.2.9.2. Modyfikowanie istniejącego obszaru obecności

Aby zmienić nazwę lub komentarz związane ze zdefiniowanym obszarem obecności, należy zaznaczyć obszar, którego mają dotyczyć zmiany, a następnie kliknąć przycisk **Edycja** znajdujący się pod listą obszarów obecności. Wyświetli się okno dialogowe **Edytuj obszar** (rysunek 3.66). Można w nim zmienić nazwę lub opisowy komentarz związane z obszarem obecności.



Rysunek 3.66. *Dodawanie nowego obszaru obecności*

3.2.9.3. Usuwanie istniejącego obszaru obecności

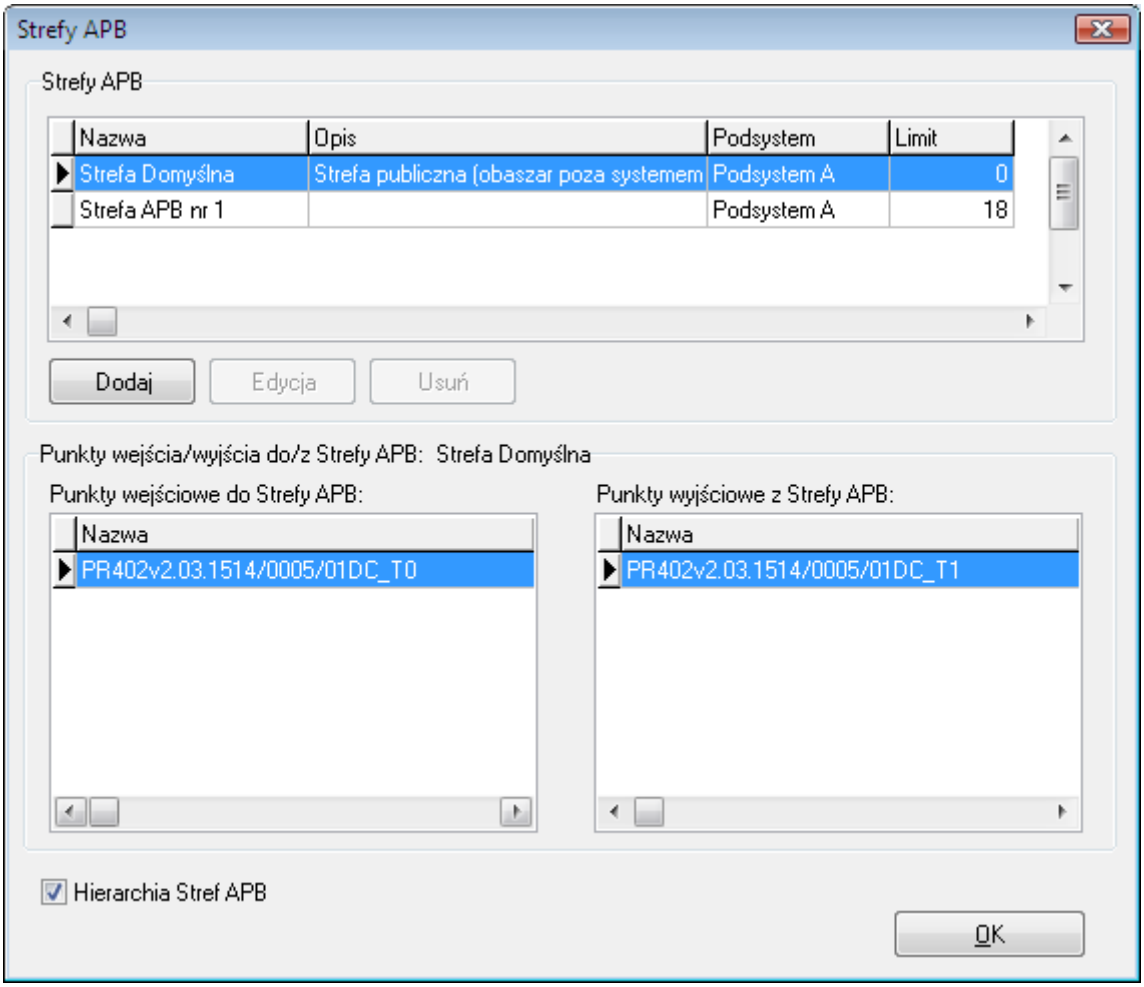
Aby usunąć zdefiniowany obszar obecności, należy kliknąć przycisk **Usuń** znajdujący się pod listą obszarów obecności. System usunie wskazany obszar obecności wraz z przypisanymi do niego punktami identyfikacyjnymi.

Należy zachować ostrożność przy używaniu przycisku **Usuń**, ponieważ system przed usunięciem obszaru obecności nie wyświetla żadnych ostrzeżeń. W związku z tym, trzeba pamiętać o wykonywaniu kopii zapasowych, ponieważ mogą one uchronić użytkownika przed koniecznością wprowadzania danych od nowa na wypadek, gdyby zostały usunięte przypadkowo.

3.2.10. Polecenie Strefy APB

Funkcja Anti-Passback służy do zapobiegania ponownemu użyciu identyfikatora użytkownika na wejściu, jeśli wcześniej nie został on użyty na wyjściu. Inaczej mówiąc, użytkownik nie może dwa razy wejść do strefy APB, jeśli wcześniej z niej nie wyszedł. Funkcja ta ma na celu uniemożliwienie podania karty innej osobie, by ta mogła jej użyć do otwarcia drzwi. Więcej dodatkowych informacji na temat konfiguracji APB podano w instrukcji **Opis funkcjonalny kontrolerów serii PRxx2**.

Wybranie polecenia menu **System**/**Strefy APB** spowoduje wyświetlenie kartoteki stref APB (rysunek 3.67)

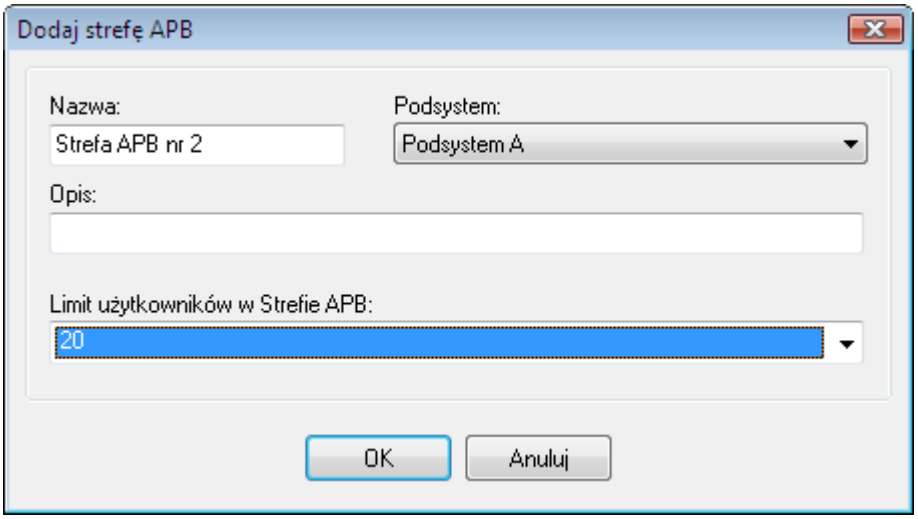


Rysunek 3.67. *Kartoteka stref APB*

Z poziomu tego okna użytkownik może dodać nową strefę APB (przycisk **Dodaj**), usunąć wcześniej zdefiniowaną strefę (przycisk **Usuń**), zmodyfikować właściwości wskazanej strefy (przycisk **Edycja**).

3.2.10.1. Dodawanie nowej strefy APB

Aby dodać nową strefę APB, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Dodaj strefę APB** (rysunek 3.68). Można w nim nadać strefie nazwę, wprowadzić opisowy komentarz oraz określić limit użytkowników przebywających we wskazanej strefie.



Rysunek 3.68. *Dodawanie nowej strefy APB*

Po zdefiniowaniu strefy APB, lista punktów identyfikacji, które do niej należą jest pusta. Strefa APB jest zdefiniowana w sposób kompletny dopiero wtedy, gdy przypiszemy do niej czytniki (terminale). Robi się to z poziomu okien właściwości kontrolerów (patrz **punkt 3.2.10.3**).

3.2.10.2. Usuwanie strefy APB

Aby usunąć strefę APB należy kliknąć przycisk **Usuń** w oknie dialogowym **Strefy APB**. Po usunięciu strefy APB, system automatycznie anuluje przypisanie punktów identyfikacyjnych, które wcześniej do niej należały do tej strefy (ustawienie **Brak**).

Należy zachować ostrożność przy używaniu przycisku **Usuń**, ponieważ system przed usunięciem strefy APB nie wyświetla żadnych ostrzeżeń i od razu trwale usuwa wskazaną strefę. Należy bezwzględnie pamiętać o wykonywaniu kopii zapasowych. W przypadku przypadkowego usunięcia strefy APB, można odzyskać ją z kopii zapasowej.

3.2.10.3. Przypisywanie punktów identyfikacyjnych do strefy APB

Aby przypisać punkt identyfikacyjny do strefy APB, należy otworzyć okno właściwości kontrolera. Najpierw należy załączyć funkcję Anti-Passback (zakładka **Zaawansowane**). Następnie można wskazać strefę APB, do której należy dany terminal (robi się to w zakładkach poszczególnych terminali). Ustawienie stref APB jest poprawne tylko wtedy, gdy do właściwych stref zostaną przypisane oba terminale kontrolera.

3.2.11. Polecenie Strefy Alarmowe

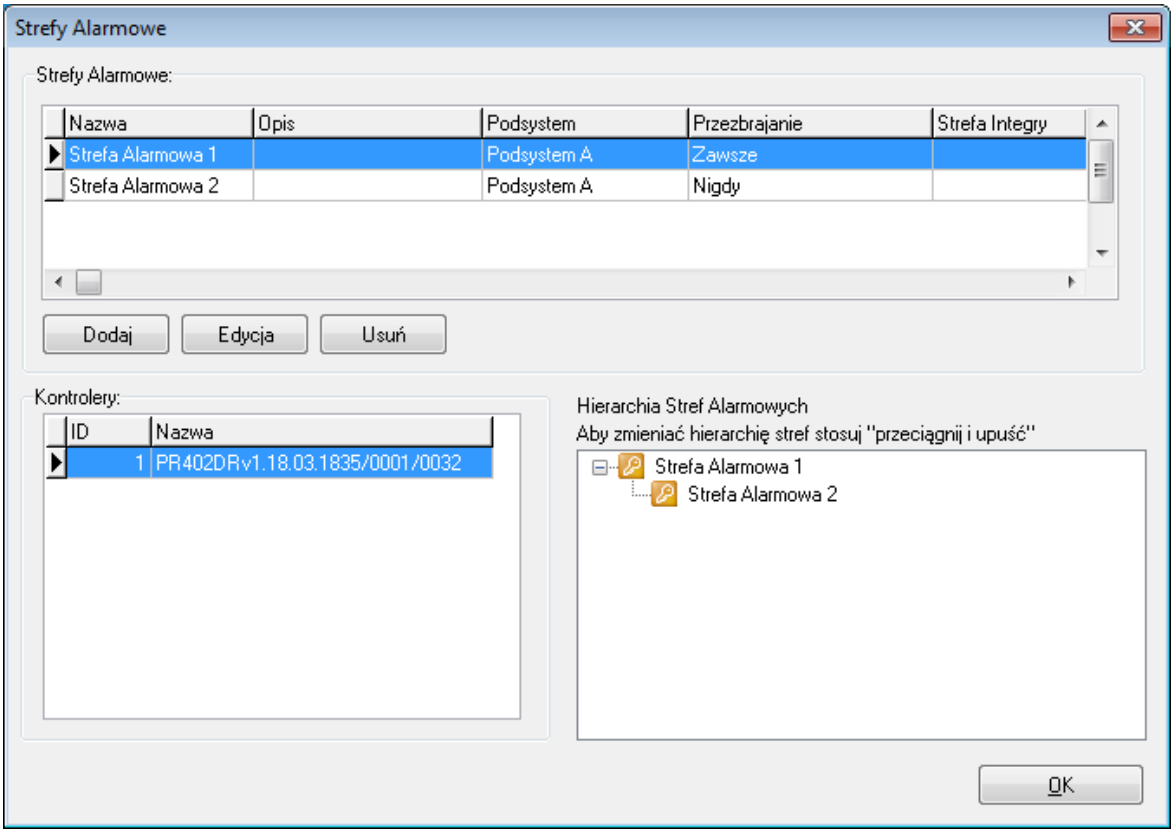
Strefa alarmowa pozwala na zdefiniowanie grupy kontrolerów, które będą przezbrajane według ustalonego harmonogramu. Dodatkowo istnieje możliwość stworzenia hierarchii stref alarmowych. Dzięki temu będą one przezbrajane w określonym porządku. Więcej dodatkowych informacji na temat konfiguracji Stref alarmowych podano w instrukcji **Opis funkcjonalny kontrolerów serii PRxx2**.

Jeśli zdefiniuje się hierarchię między strefami, to może między nimi zachodzić relacja podrzędności lub nadrzędności. Obowiązują następujące zasady uzbrajania/rozbrajania stref alarmowych w hierarchii:

- Uzbrojenie strefy nadrzędnej powoduje uzbrojenie wszystkich jej stref podrzędnych.

- Rozbrojenie strefy nadrzędnej nie ma wpływu na stan uzbrojenia stref podrzędnych.
- Uzbrojenie strefy podrzędnej nie powoduje uzbrojenia strefy nadrzędnej.
- Rozbrojenie strefy podrzędnej nie powoduje rozbrojenia strefy nadrzędnej.

Wybranie polecenia menu **System**/**Strefy Alarmowe** spowoduje wyświetlenie kartoteki stref alarmowych zdefiniowanych w systemie (rysunek 3.69)

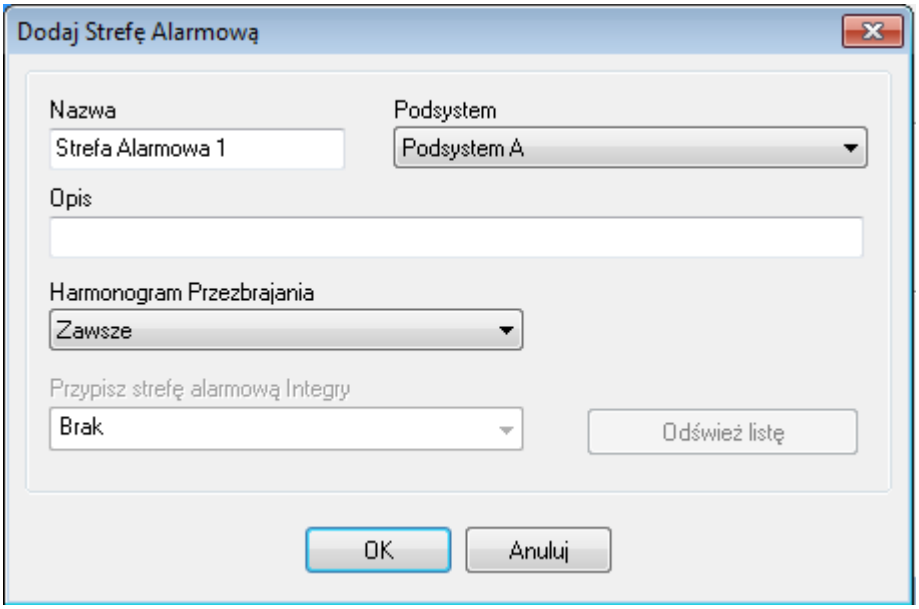


Rysunek 3.69. *Kartoteka stref alarmowych*

Z poziomu tego okna użytkownik może dodać nową strefę alarmową (przycisk **Dodaj**), usunąć wcześniej zdefiniowaną strefę (przycisk **Usuń**), zmodyfikować właściwości wskazanej strefy (przycisk **Edycja**) oraz zmodyfikować hierarchię stref alarmowych.

3.2.11.1. Dodawanie nowej strefy alarmowej

Aby dodać nową strefę alarmową, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Dodaj strefę alarmową** (rysunek 3.70). Można w nim nadać strefie nazwę, wprowadzić opisowy komentarz oraz określić harmonogram uzbrajania kontrolerów należących do strefy. Dodatkowo możliwe jest powiązanie strefy alarmowej systemu RACS 4 ze strefą alarmową systemu alarmowego INTEGRA firmy SATEL o ile taka integracja wymagająca zastosowania centrali CPR32-NET jest stosowana. Więcej informacji na temat integracji podano w dedykowanej instrukcji dostępnej na **www.roger.pl**.



Rysunek 3.70. *Dodawanie nowej strefy alarmowej*

Po zdefiniowaniu strefy alarmowej, lista kontrolerów, które do niej należą jest pusta. Strefa alarmowa będzie zdefiniowana w sposób kompletny dopiero wtedy, gdy przypiszemy do niej kontrolery. Robi się to z poziomu okien właściwości kontrolerów (patrz **punkt 3.2.11.3**).

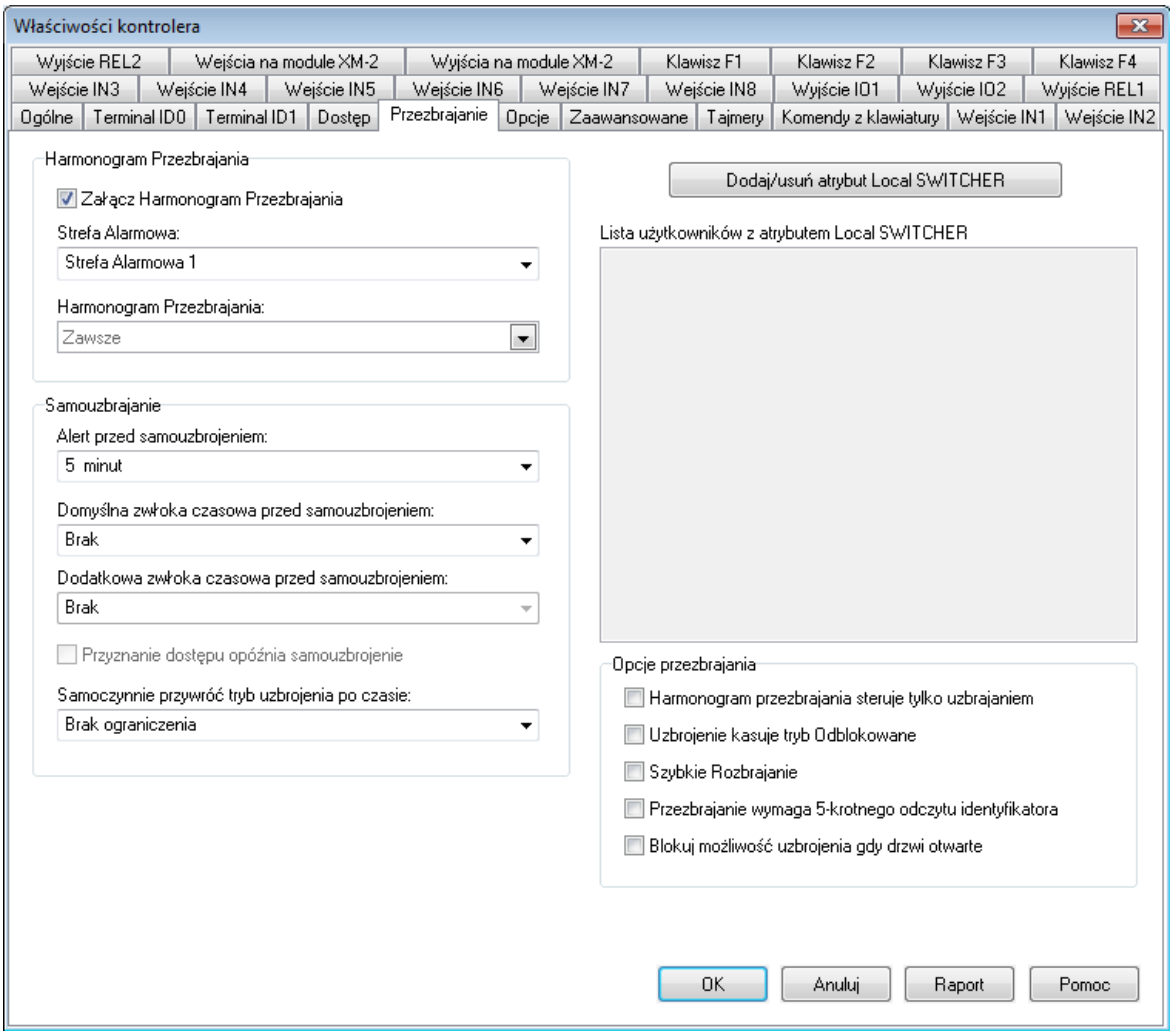
3.2.11.2. Usuwanie strefy alarmowej

Aby usunąć strefę alarmową należy kliknąć przycisk **Usuń** w oknie dialogowym **Strefy Alarmowe**. Po usunięciu strefy alarmowej, system automatycznie anuluje przypisanie do tej strefy kontrolerów, które wcześniej do niej należały (ustawienie **Brak**).

Należy zachować ostrożność przy używaniu przycisku **Usuń**, ponieważ system przed usunięciem strefy alarmowej nie wyświetla żadnych ostrzeżeń i od razu trwale usuwa wskazaną strefę. Należy bezwzględnie pamiętać o wykonywaniu kopii zapasowych. W przypadku przypadkowego usunięcia strefy alarmowej, można odzyskać ją z kopii zapasowej.

3.2.11.3. Przypisywanie kontrolerów do strefy alarmowej

Aby przypisać kontroler do strefy alarmowej, należy otworzyć okno właściwości kontrolera. W zakładce **Przezbrajanie** należy wskazać strefę alarmową, do której należy dany kontroler (rysunek 3.71).



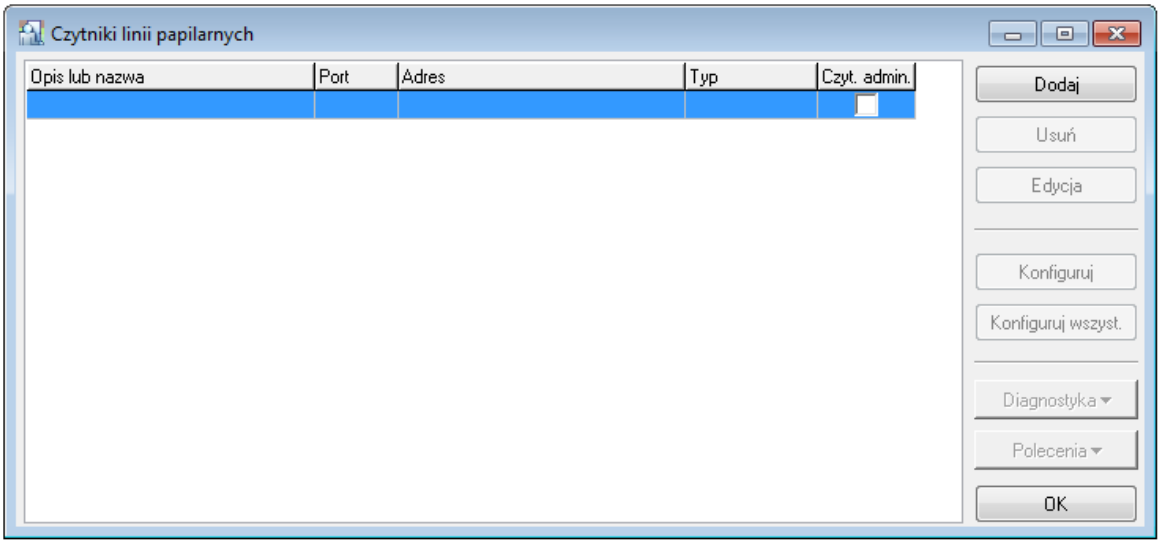
Rysunek 3.71. *Przypisywanie kontrolera do strefy alarmowej*

Po zatwierdzeniu zmian, należy przesłać konfigurację do kontrolera. Przy kolejnym otwarciu kartoteki stref alarmowych, wskazany kontroler wyświetli się na liście kontrolerów należących do strefy.

3.2.12. Polecenie Czytniki linii papilarnych

W systemie RACS 4 można stosować zarówno nowsze czytniki linii papilarnych RFT1000 jak i starsze nieoferowane już w sprzedaży czytniki F7, F8, F10, F11. Czytniki RFT1000 zaleca się podłączać do kontrolerów po magistrali RACS CLK/DTA tak jak czytniki kart serii PRT.

Polecenie menu **System/Czytniki linii papilarnych** służy do zarządzania czytnikami zainstalowanymi w systemie. Wybranie tego polecenia spowoduje wyświetlenie kartoteki czytników linii papilarnych (rysunek 3.72). Więcej informacji na temat instalacji i konfiguracji czytników RFT1000 podano w dedykowanej instrukcji dostępnej na stronie **www.roger.pl**.



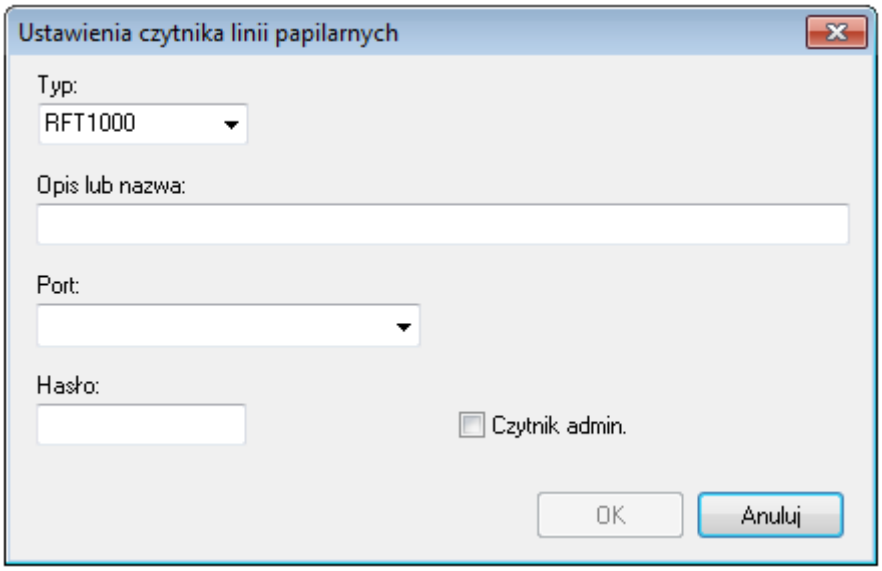
Rysunek 3.72. *Kartoteka czytników linii papilarnych*

Z poziomu tego okna można wykonać następujące operacje:

- dodawać czytniki linii papilarnych,
- usuwać czytniki linii papilarnych,
- modyfikować ustawienia czytników linii papilarnych,
- konfigurować wskazany czytnik linii papilarnych,
- konfigurować wszystkie czytniki linii papilarnych występujące w systemie,
- wykonywać operacje diagnostyczne,
- przesyłać polecenia do wskazanego czytnika.

3.2.12.1. Dodawanie czytników linii papilarnych

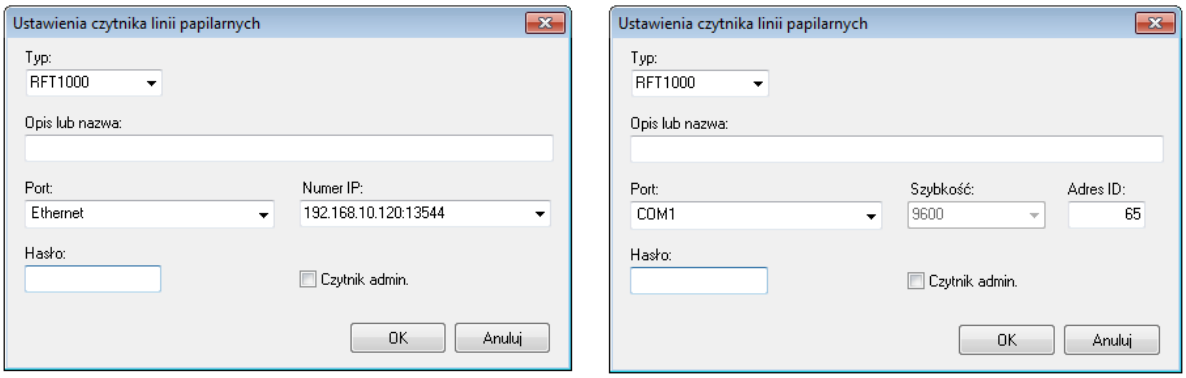
Aby dodać nowy czytnik linii papilarnych, należy kliknąć przycisk **Dodaj**. Wyświetli się okno **Ustawienia czytnika linii papilarnych** (rysunek 3.73).



Rysunek 3.73. *Dodawanie nowego czytnika linii papilarnych*

Należy w nim wybrać typ czytnika (pole **Typ**), podać nazwę czytnika linii papilarnych (pole **Opis lub nazwa**), określić port, za pośrednictwem którego czytnik jest podłączony do systemu (pole **Port**) i opcjonalnie określić hasło dostępu do czytnika (pole **Hasło**).

Czytniki RFT1000 mogą być podłączone do komputera z programem PR Master za pośrednictwem portu Ethernet lub RS-485. Dla obu rodzajów komunikacji konieczne jest skonfigurowanie dalszych parametrów tj. odpowiednio adresu IP i portu lub adresu ID (rysunek 3.74).



Rysunek 3.74. *Dodawanie nowego czytnika linii papilarnych*

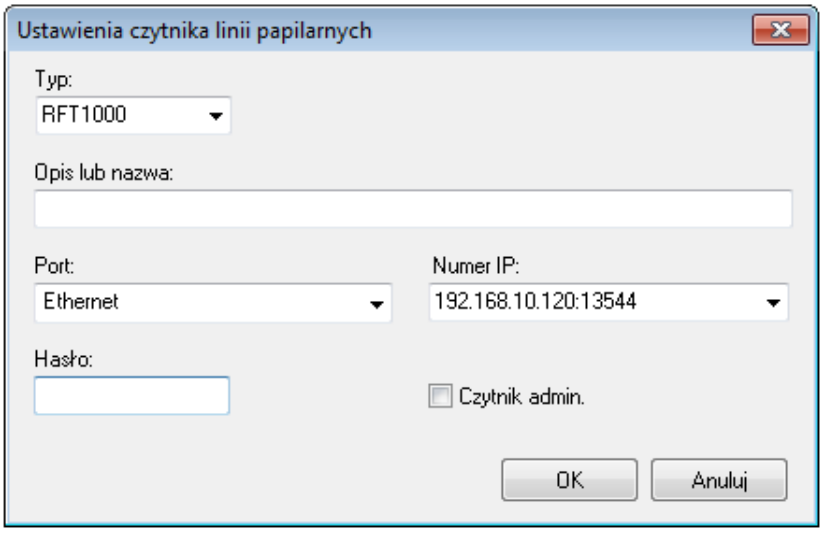
Po dodaniu czytnika linii papilarnych, pojawi się on na liście zainstalowanych czytników linii papilarnych w systemie (rysunek 3.72). Jeśli lista nie jest pusta, aktywne stają się dodatkowe dwa przyciski: **Usuń** i **Właściwości**. Pozwalają one odpowiednio na usuwanie czytnika z systemu lub na zmianę jego konfiguracji.

3.2.12.2. Usuwanie czytników linii papilarnych

Aby usunąć czytnik linii papilarnych z systemu, należy kliknąć przycisk **Usuń**. Przed usunięciem czytnika system wyświetli pytanie o potwierdzenie zamiaru usunięcia. Jeśli użytkownik odpowie twierdząco, czytnik zostanie usunięty z systemu.

3.2.12.3. Przeglądanie (modyfikowanie) właściwości czytników linii papilarnych

Przycisk **Edycja** wyświetla okno ustawień wskazanego czytnika. W ten sposób można zmodyfikować nazwę czytnika, zmienić port a także wprowadzić opcjonalne hasło (rysunek 3.75).



Rysunek 3.75. *Modyfikowanie właściwości czytnika linii papilarnych*

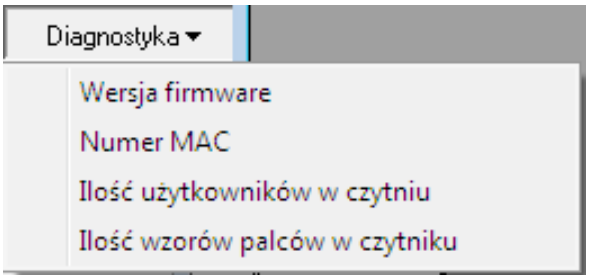
3.2.12.4. Konfigurowanie wskazanego czytnika linii papilarnych lub wszystkich czytników w systemie

Po wprowadzeniu zmian konfiguracyjnych w oknie ustawień czytnika linii papilarnych, należy je do niego przesłać. Dopiero po przesłaniu, zmiany zaczną obowiązywać w systemie kontroli dostępu. W celu przesłania konfiguracji, należy wskazać czytnik linii papilarnych na liście i kliknąć przycisk **Konfiguruj**. Program PR Master skomunikuje się ze wskazanym czytnikiem linii papilarnych i zapisze w nim jego ustawienia. Jeśli operacja przebiegnie pomyślnie, system wyświetli odpowiedni komunikat. Komunikat wyświetli się także wtedy, gdy wystąpią problemy komunikacyjne.

Można również skonfigurować wszystkie czytniki linii papilarnych zainstalowane w systemie. W tym celu należy kliknąć przycisk **Konfiguruj wszyst.** .

3.2.12.6. Wykonywanie operacji diagnostycznych

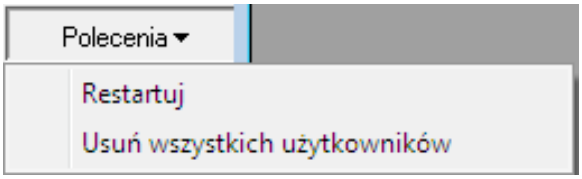
Przycisk **Diagnostyka** daje dostęp do menu operacji diagnostycznych (rysunek 3.76). Z tego menu można wykonać szereg operacji mających na celu weryfikację poprawności działania czytnika linii papilarnych. Można odczytać wersję oprogramowania firmware, numer MAC, liczbę użytkowników zdefiniowanych w czytniku oraz liczbę wzorów odcisków palców.



Rysunek 3.76. *Menu operacji diagnostycznych*

3.2.12.7. Przesyłanie poleceń do wskazanego czytnika

Przycisk **Polecenia** daje dostęp do menu poleceń dostępnych dla wybranego czytnika. W ten sposób można zrestartować urządzenie lub usunąć z niego wszystkich użytkowników. Menu Polecenia pokazano na rysunku 3.77.

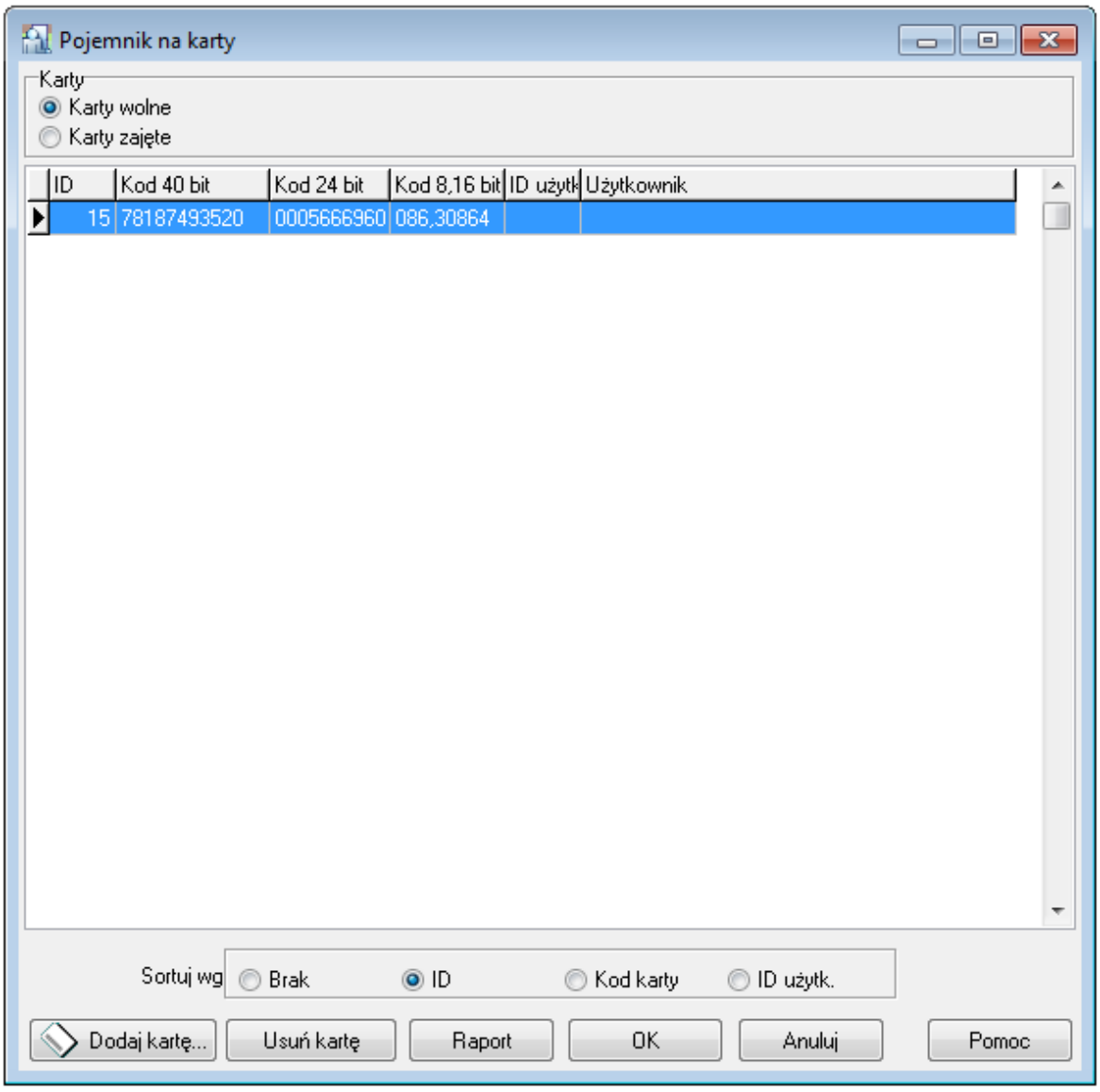


Rysunek 3.77. *Menu Polecenia pozwala na przesyłanie komend do wskazanego czytnika linii papilarnych*

3.2.13. Polecenie Pojemnik na karty

Polecenie **Pojemnik na karty** otwiera kartotekę kart zbliżeniowych zarejestrowanych w systemie. Jest to narzędzie, które ułatwia zarządzanie kartami w systemie RACS 4. Dzięki niemu można jednorazowo wczytać zbiór kart do systemu, a następnie przydzielać je użytkownikom. W ten sposób operacja definiowania użytkownika nie wymaga dostępu do czytnika kart.

Wybranie polecenia powoduje wyświetlenie okna kartoteki kart (rysunek 3.78).



Rysunek 3.78. *Kartoteka kart zbliżeniowych zarejestrowanych w systemie*

Z poziomu tego okna użytkownik może wykonać następujące operacje:

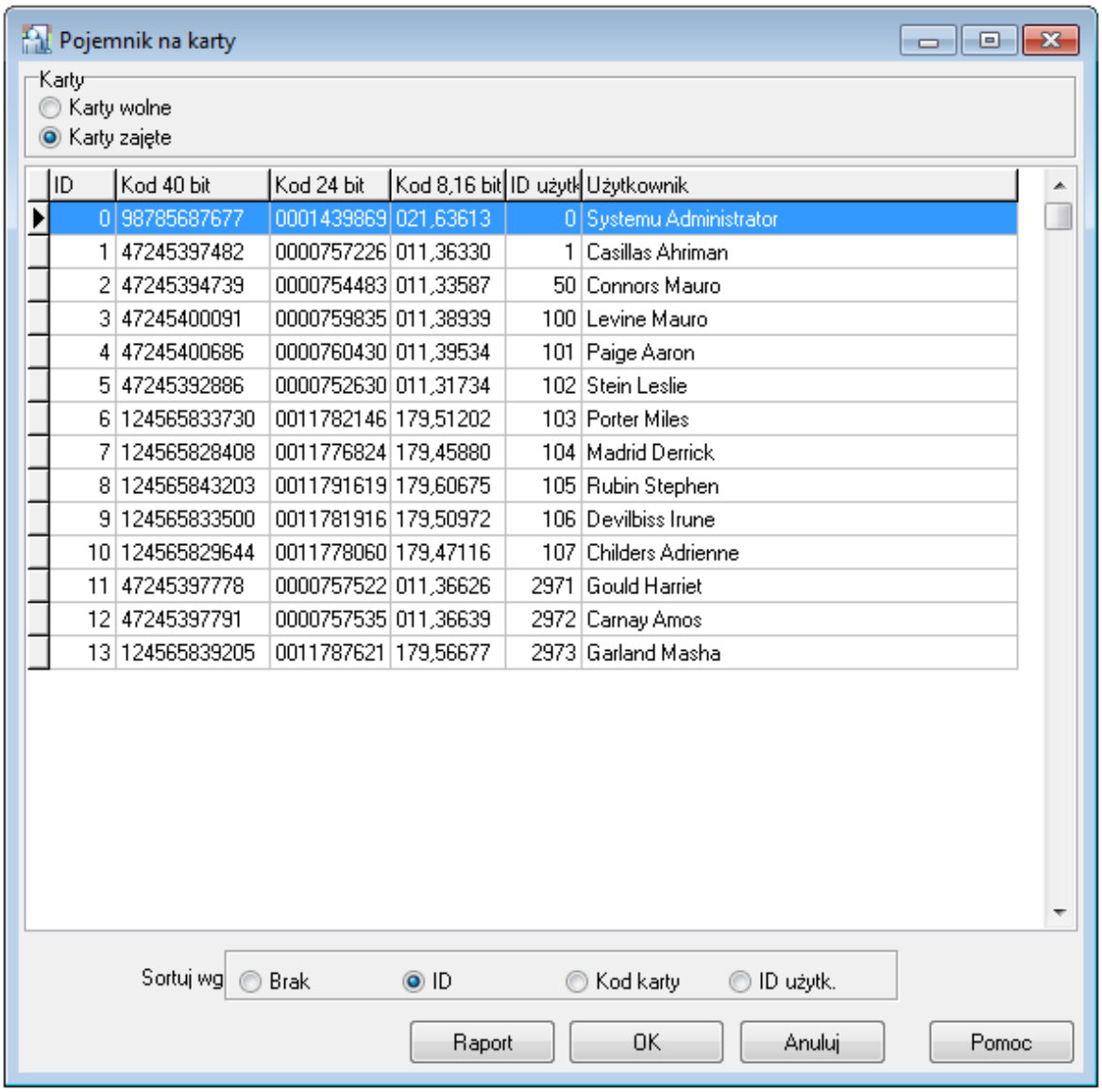
- wyświetlić listę nieprzydzielonych kart w systemie,
- wyświetlić listę przydzielonych kart w systemie,
- dodać kartę do pojemnika,
- posortować listę kart wg wskazanego kryterium,
- wydrukować raport dotyczący kart zbliżeniowych zarejestrowanych w systemie.

Wyświetlenie listy nieprzydzielonych kart w systemie

Aby wyświetlić listę nieprzydzielonych kart w systemie, należy kliknąć przełącznik **Karty wolne** w górnej części okna. System automatycznie wyświetli listę kart znajdujących się w pojemniku, które nie zostały przydzielone do żadnego użytkownika.

Wyświetlenie listy kart zarejestrowanych w systemie, które zostały przydzielone użytkownikom

Aby wyświetlić listę kart zarejestrowanych w systemie przydzielonych użytkownikom, należy kliknąć przełącznik **Karty zajęte** w górnej części okna. System automatycznie wyświetli listę kart przydzielonych użytkownikom (rysunek 3.79).

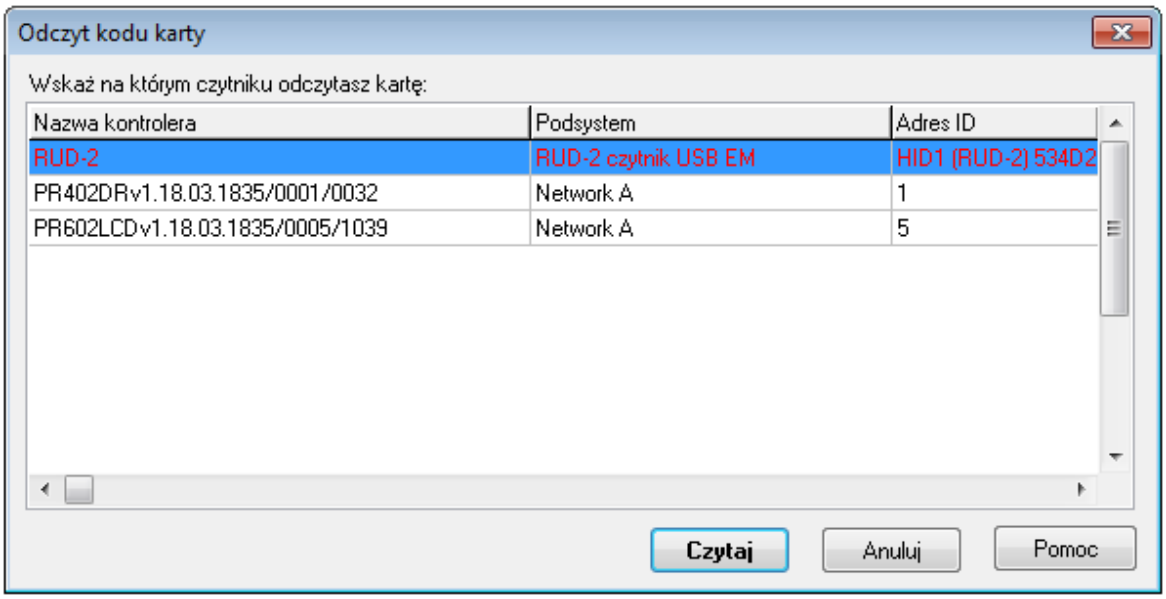


Rysunek 3.79. *Lista kart w systemie przydzielonych użytkownikom*

Dodawanie karty do pojemnika

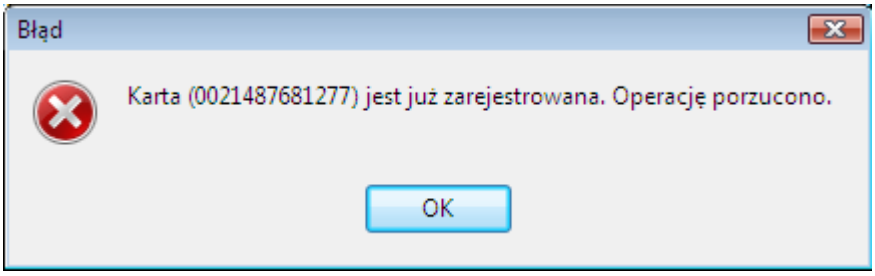
Aby dodać nową kartę do pojemnika, należy najpierw zaznaczyć przełącznik **Karty wolne**. W tym momencie program wyświetli listę nieprzydzielonych kart zarejestrowanych w systemie, a w oknie pojawi się przycisk **Dodaj kartę...**.

Operację dodawania nowej karty inicjujemy poprzez kliknięcie przycisku **Dodaj kartę...**. W odpowiedzi wyświetli się okno dialogowe **Odczyt kodu karty** (rysunek 3.80), w którym należy wskazać czytnik używany do odczytania karty.



Rysunek 3.80. *Odczyt karty dodawanej do pojemnika*

Najpierw należy wskazać czytnik, na którym będziemy odczytywali kartę, a następnie kliknąć przycisk **Czytaj**. Następnie należy odczytać kartę na wskazanym czytniku. Operację odczytania można powtórzyć dla kolejnych kart. System będzie je automatycznie umieszczał na liście. Jeśli któraś z wczytanych kart była już wcześniej zarejestrowana w systemie, system wyświetli ostrzeżenie (rysunek 3.81).



Rysunek 3.81. *Komunikat informując o tym, że karta została wcześniej zarejestrowana w systemie*

Operację wczytywania kart należy przerwać za pomocą przycisku **Anuluj**.

Usuwanie karty z pojemnika

Aby usunąć kartę z pojemnika, należy kliknąć przycisk **Usuń kartę**. System wyświetli pytanie o potwierdzenie zamiaru usunięcia karty. Udzielenie odpowiedzi **Tak** na to pytanie spowoduje usunięcie karty z listy zarejestrowanych kart.

Z pojemnika można usuwać tylko te karty, które nie zostały przydzielone do żadnego użytkownika. W związku z tym, jeśli jest włączony przełącznik Karta zajęta, to przycisk **Usuń kartę** jest niedostępny.

Sortowanie listy kart według wskazanego kryterium

Listę kart w pojemniku można posortować według wskazanego kryterium:

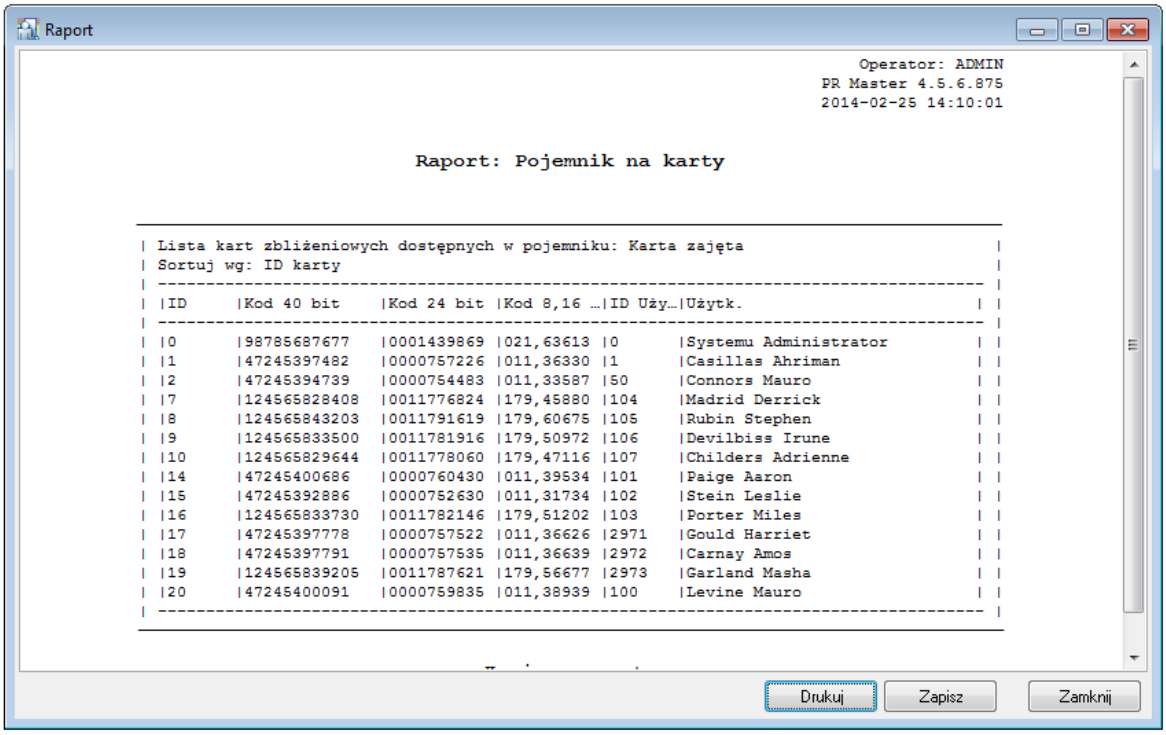
- wg ID karty,
- wg kodu karty,

- wg ID użytkownika.

Do wyboru sposobu sortowania służy przełącznik **Sortuj wg**. Aby posortować karty wg danego kryterium należy zaznaczyć odpowiednią wartość przełącznika.

Drukowanie raportu dotyczącego kart zarejestrowanych w systemie

Program PR Master umożliwia również sporządzenie drukowanego raportu dotyczącego kart zbliżeniowych zarejestrowanych w systemie. Mechanizm ten pozwala na stworzenie listy zarówno tych kart, które jeszcze nie zostały przydzielone żadnemu użytkownikowi, jak i tych, które już przyporządkowano użytkownikom. Aby stworzyć taki raport, należy kliknąć przycisk **Raport** w oknie kartoteki kart zbliżeniowych. Przykładową postać raportu dla kart zajętych pokazano na rysunku 3.82.

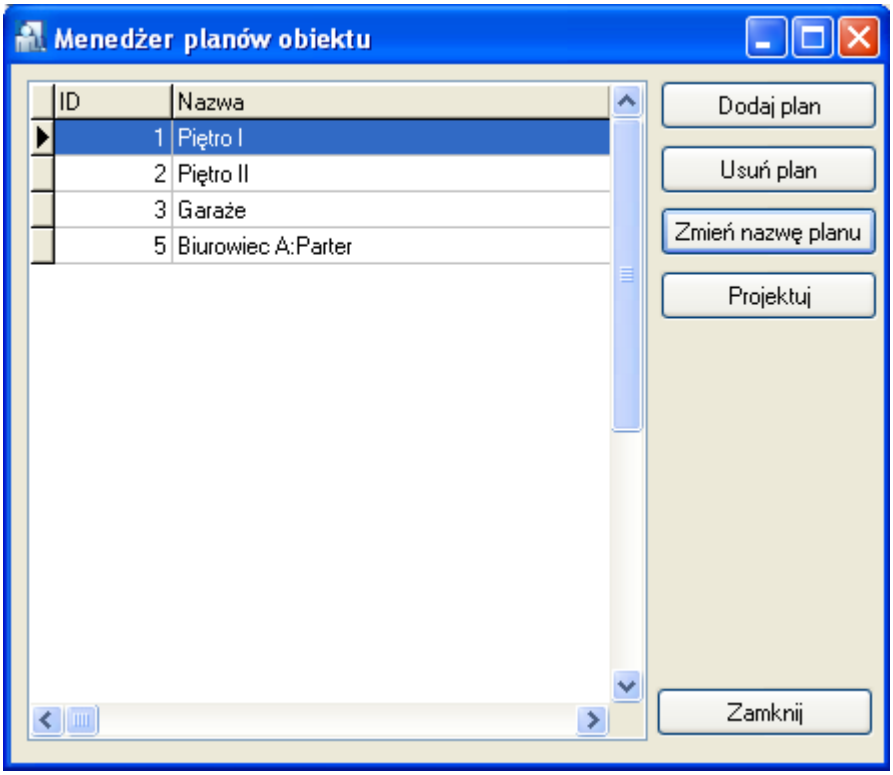


Rysunek 3.82. *Raport z listy kart zbliżeniowych przydzielonych użytkownikom systemu*

3.2.14. Polecenie Plany obiektu

Polecenie **Plany obiektu** otwiera kartotekę planów obiektu zarejestrowanych w systemie. Plan obiektu to graficzna mapa (np. podkład budowlany), na którym naniesiono ikony wybranych kontrolerów. Zdefiniowane plany obiektu można później wykorzystać w trybie monitorowania za pośrednictwem polecenia menu **Widok**/**Mapa obiektu** (patrz **punkt 4.1.14**). W systemie RACS 4 można zdefiniować do 20 osobnych planów obiektu.

Wybór polecenia **Plany obiektu** powoduje wyświetlenie okna kartoteki planów obiektu (rysunek 3.83)



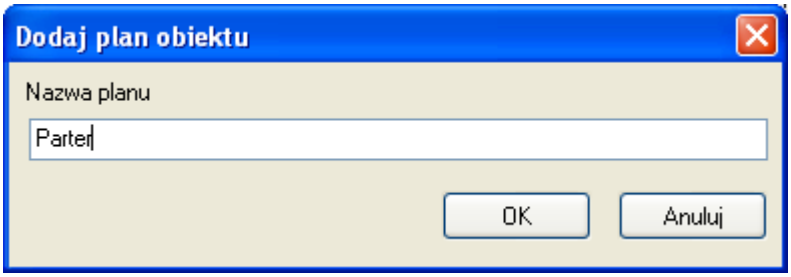
Rysunek 3.83. *Kartoteka planów obiektu*

Z poziomu tego okna użytkownik może wykonać następujące operacje:

- dodać nowy plan obiektu — przycisk **Dodaj plan**,
- usunąć zdefiniowany wcześniej plan obiektu — przycisk **Usuń plan**,
- zmienić nazwę istniejącego planu obiektu — przycisk **Zmień nazwę planu**,
- zaprojektować rozmieszczenie ikon na planie i określić plik z podkładem graficznym — przycisk **Projektuj**.

3.2.14.1. Dodawanie planu obiektu

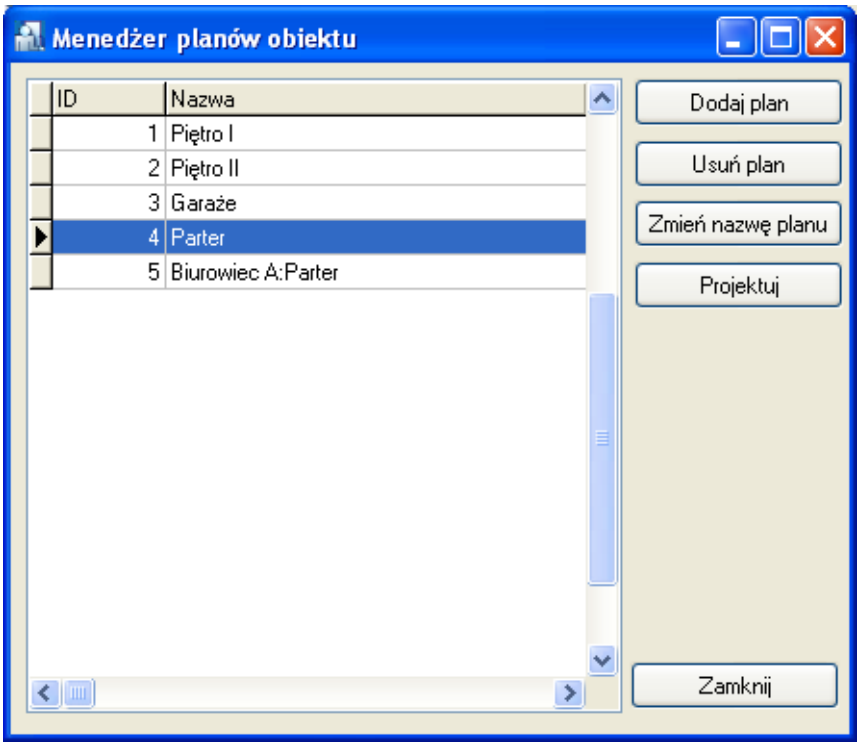
Aby dodać nowy plan obiektu, należy kliknąć przycisk **Dodaj plan**. Wyświetli się okno **Dodaj plan obiektu** (rysunek 3.84).



Rysunek 3.84. *Dodawanie nowego planu obiektu*

Należy w nim podać nazwę, za pomocą której będziemy identyfikować plan obiektu. Nazwa powinna jednoznacznie wskazywać, o jaki plan obiektu nam chodzi. Po wpisaniu nazwy w polu

Nazwa planu klikamy przycisk **OK**. Spowoduje to dodanie planu do kartoteki dostępnych planów na pierwszej wolnej pozycji (rysunek 3.85).



Rysunek 3.85. *Nowy plan — Parter — pojawił się na pozycji nr 4*

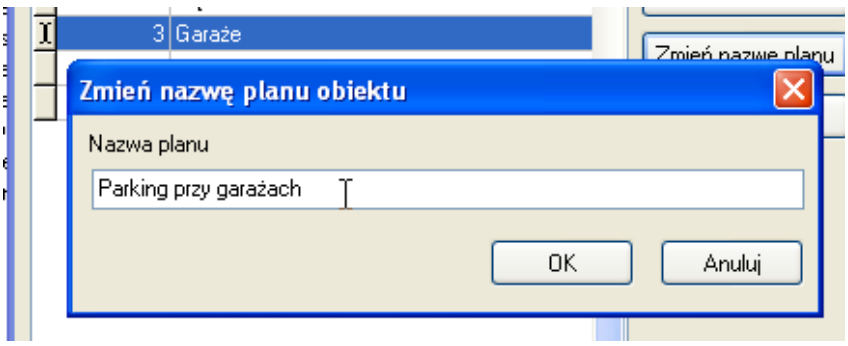
3.2.14.2. Usuwanie planu obiektu

Aby usunąć plan obiektu, należy kliknąć przycisk **Usuń plan**. Wyświetli się okno **Potwierdź** z pytaniem o potwierdzenie zamiaru usunięcia planu. Kliknięcie **Tak** spowoduje, że wskazany plan zostanie trwale usunięty z bazy danych.

Aby zapobiec przypadkowemu usunięciu planu obiektu z systemu, warto zadbać o częste wykonywanie kopii zapasowej bazy danych. Więcej informacji na ten temat można znaleźć w **punkcie 2.3.2**.

3.2.14.3. Zmiana nazwy planu obiektu

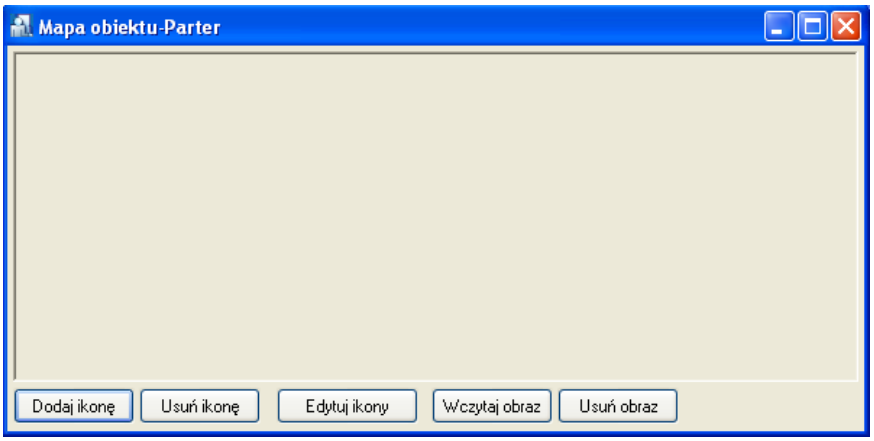
Aby zmienić nazwę planu obiektu, należy kliknąć przycisk **Zmień nazwę planu**. Wyświetli się okno dialogowe **Zmień nazwę planu obiektu** (rysunek 3.86). Należy wprowadzić w nim nową nazwę planu, a następnie kliknąć **OK**.



Rysunek 3.86. *Zmienianie nazwy planu obiektu*

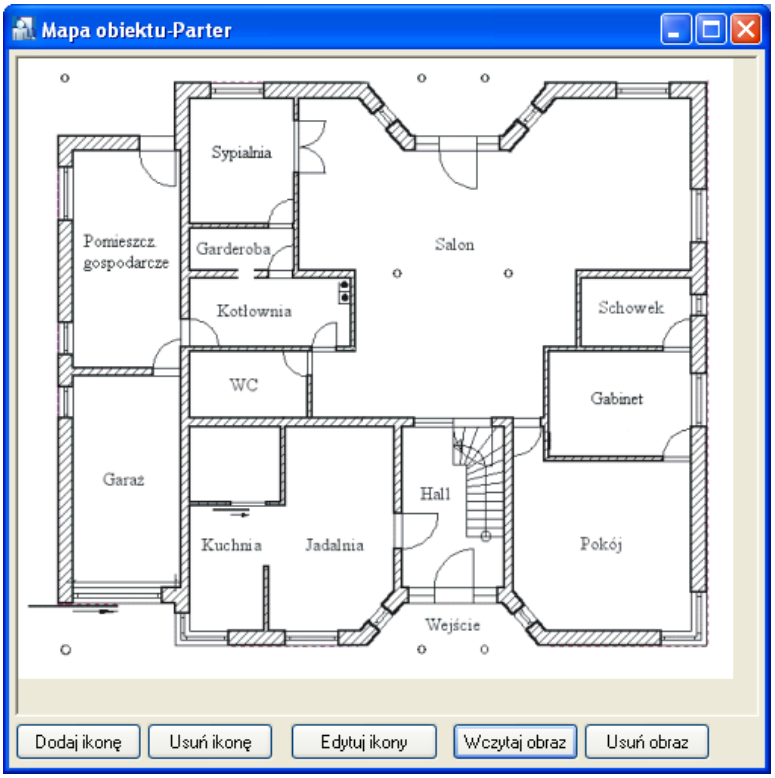
3.2.14.4. Projektowanie planu obiektu

Aby zaprojektować plan obiektu, należy wskazać go w kartotece planów, po czym kliknąć przycisk **Projektuj**. Wyświetli się okno projektowania obiektu. Jeśli jest to nowy plan, okno będzie puste — podobne do pokazanego na rysunku 3.87.



Rysunek 3.87. *Projektowanie planu obiektu — ekran początkowy*

Projektowanie planu obiektu, należy rozpocząć od wczytania odpowiedniego podkładu graficznego. może to być, na przykład, podkład budowlany, rzut piętra lub plan obiektu, w którym zainstalowano kontrolery. Aby wczytać plan, należy kliknąć przycisk **Wczytaj obraz** i wybrać plik z podkładem graficznym (*.jpg, *.bmp). Następnie należy odpowiednio dostosować rozmiar okna do wymiarów pliku graficznego. Po wykonaniu tych czynności, okno projektowania planu może mieć postać podobną do pokazanej na rysunku 3.88.

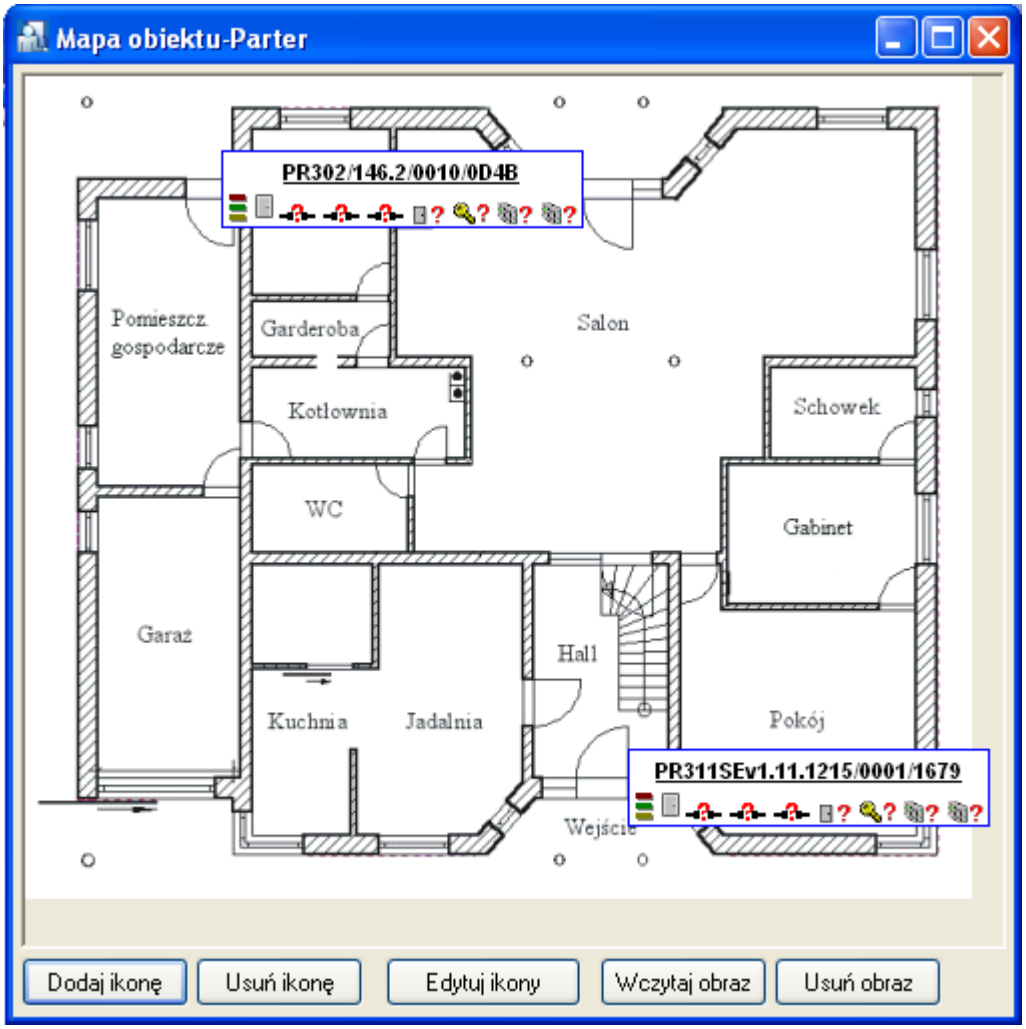


Rysunek 3.88. *Projektowanie planu obiektu — okno po wczytaniu rzutu piętra*

Teraz należy dodać do planu ikony kontrolerów. Wciśnięcie przycisku **Dodaj ikonę** powoduje wyświetlenie listy dostępnych kontrolerów (tzn. takich, które jeszcze nie zostały dodane do planu).

Na tej liście należy wskazać kontrolery, które mają być dodane do planu (poprzez zaznaczenie odpowiednich pól wyboru), a następnie kliknąć **Wybierz**. Dodane ikony standardowo wyświetlają się w lewym górnym narożniku okna. Należy teraz odpowiednio przeciągnąć je na planie tak, by wskazywały lokalizację instalacji czytnika.

Po rozmieszczeniu ikon na planie, ekran projektowania może wyglądać tak, jak pokazano na rysunku 3.89.



Rysunek 3.89. *Projektowanie planu obiektu — okno po wybraniu i rozmieszczeniu ikon kontrolerów*

Ostatnią czynnością jest dostosowanie sposobu wyświetlania ikon. W zależności od poziomu szczegółowości planu, można dostosować sposób ich wyświetlania do własnych potrzeb.

Edycja ikon

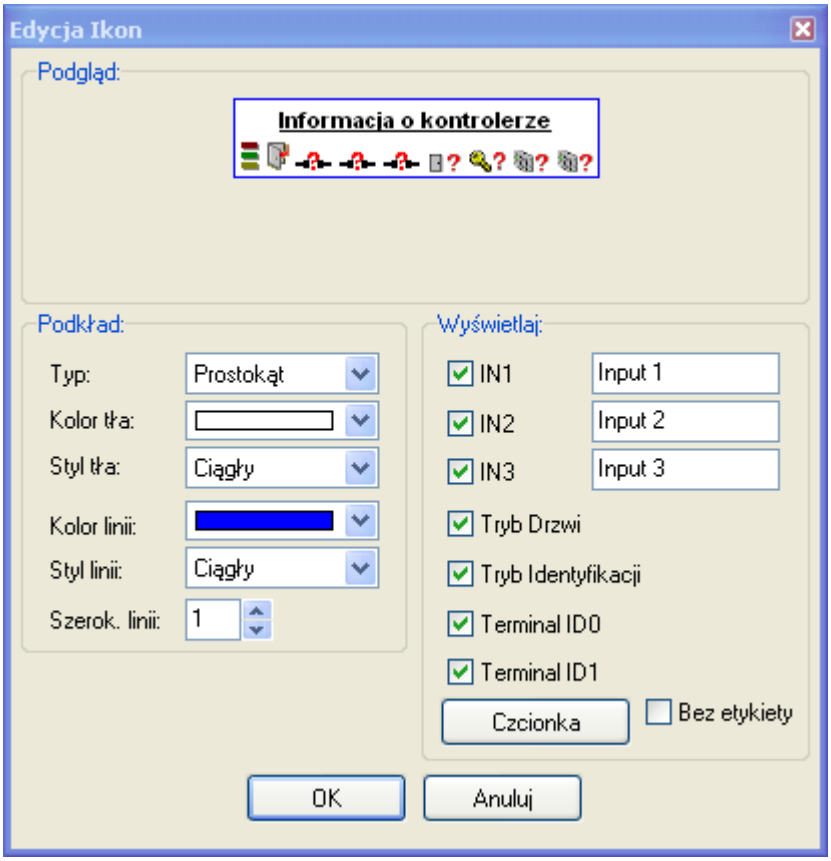
Ikony można edytować na dwa sposoby:

- kliknąć prawym przyciskiem myszy ikonę i wybrać z menu polecenie **Edytuj ikonę**

lub

- kliknąć przycisk **Edytuj ikony**.

Po wyborze polecenia **Edytuj ikony** i wskazaniu kontrolera do modyfikacji, wyświetla się okno dialogowe **Edycja Ikon** (rysunek 3.90).

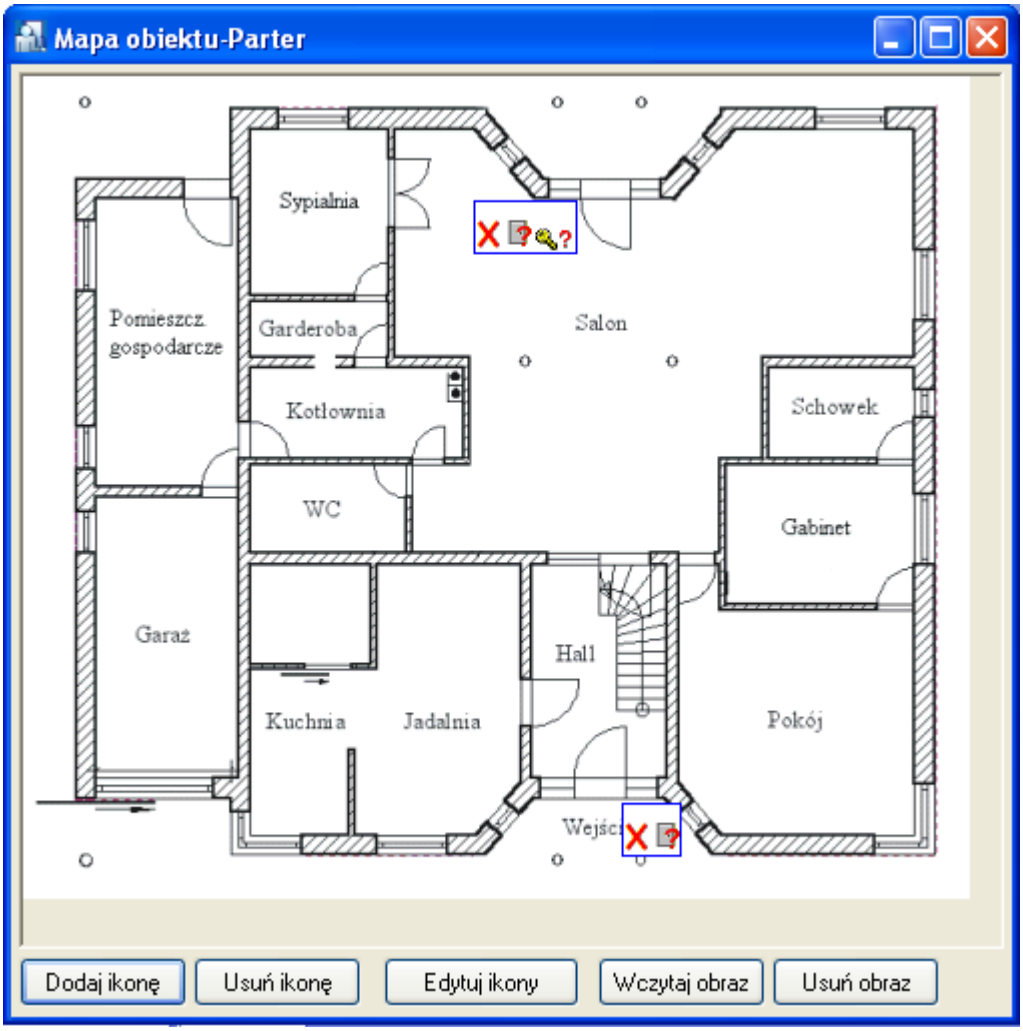


Rysunek 3.90. *Edycja ikon*

Za pomocą tego okna można dostosować sposób wyświetlania ikony na schemacie.

W przypadku, gdy chcemy, aby na planie wyświetlała się tylko minimalna ilość informacji o kontrolerze, możemy wyłączyć pola wyboru reprezentujące poszczególne elementy ikony, a nawet wyłączyć etykietę ikony (zaznaczając opcję **Bez etykiety**). Nazwę samego kontrolera zmienia się w jego właściwościach wybierając dany kontroler w oknie głównym programu PR Master.

Po dostosowaniu wyglądu ikon, gotowy plan może przyjąć postać pokazaną na rysunku 3.91.



Rysunek 3.91. *Projektowanie planu obiektu — okno planu obiektu w finalnej postaci*

Aby zapisać plan, należy zamknąć okno projektowania. Można teraz będzie wykorzystać zdefiniowany plan w trybie monitorowania do obserwacji działania systemu w trybie graficznym (więcej informacji na temat monitorowania w trybie graficznym można znaleźć w **punkcie 4.1.14**).

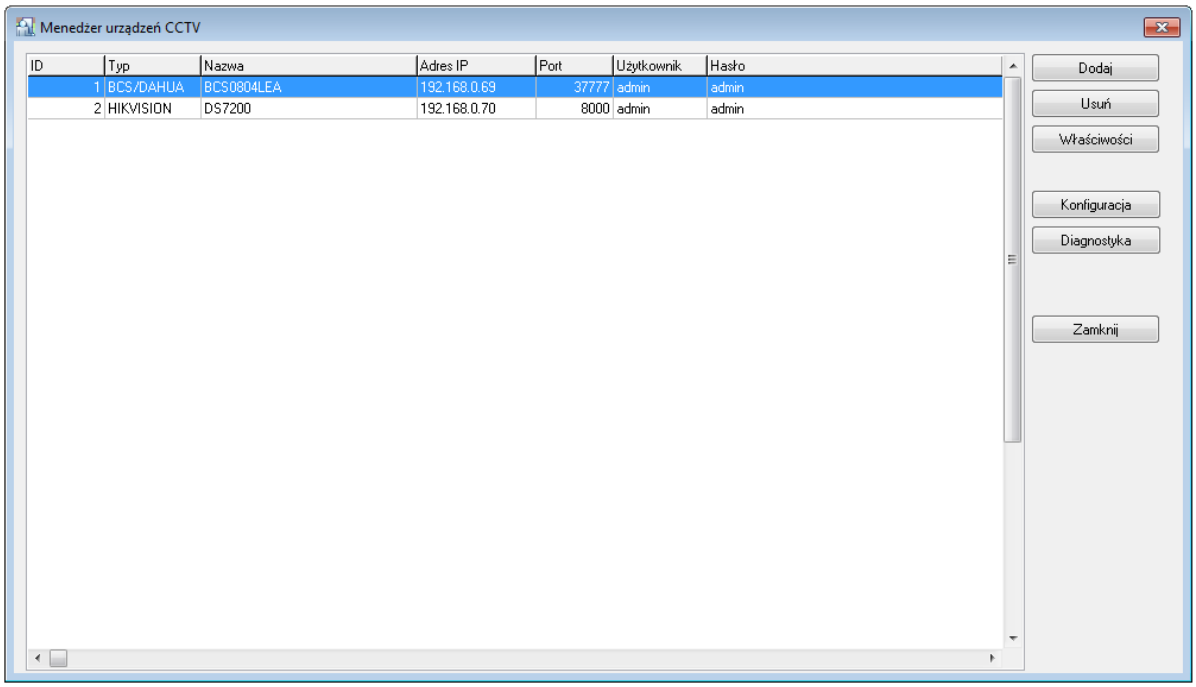
3.2.15. Urządzenia CCTV

Polecenie **Urządzenia CCTV** służy do skonfigurowania integracji systemu RACS 4 z telewizją przemysłową. Aktualnie RACS 4 współpracuje przede wszystkim z rejestratorami takich producentów jak Dahua (BCS) oraz HIK Vision.

W ogólnym ujęciu integracja polega na możliwości powiązania zdarzeń w systemie kontroli dostępu RACS 4 z obrazem zarejestrowanym przez kamery. Integracja została opracowana do zastosowania w sieci lokalnej (LAN) ale praktyczne testy wykazały, że może ona funkcjonować prawidłowo również w sieci rozległej (WAN). Można połączyć więcej niż jeden rejestrator z systemem RACS 4. Dzięki integracji z CCTV, w trybie monitorowania programu PR Master (patrz **punkt 4.5**) można skorzystać z przycisków **Odtwórz nagranie z CCTV** oraz **Podgląd kamer CCTV**, a w oknie rejestru zdarzeń (patrz **punkt 3.3.7.2**) można skorzystać z przycisku **Odtwórz nagranie z CCTV**.

Więcej informacji na temat integracji podano w dedykowanej instrukcji dostępnej na **www.roger.pl**.

Wybór polecenia **Urządzenia CCTV** powoduje wyświetlenie okna Menedżer urządzeń CCTV (rysunek 3.92)



Rysunek 3.92. *Menedżer urządzeń CCTV*

W tym oknie dostępne są następujące przyciski:

- **Dodaj** – umożliwia dodanie rejestratora do listy obsługiwanych urządzeń.
- **Usuń** – umożliwia usunięcie rejestratora z listy obsługiwanych urządzeń.
- **Właściwości** – umożliwia edycję dodanego rejestratora.
- **Konfiguracja** – umożliwia skonfigurowanie danego rejestratora tj. powiązanie jego kanałów (kamer) z kontrolerami (przejściami) oraz typami zdarzeń.
- **Diagnostyka** – test łączności z wybranym rejestratorem polegający na próbie zalogowania się na dany rejestrator.

3.3. MENU RAPORTY

Menu **Raporty** pokazano na rysunku 3.93.

Rysunek 3.93. *Menu Raporty*

Zawiera ono polecenia służące do sporządzania drukowanych raportów dotyczących informacji wprowadzonych do systemu. Większość poleceń znajdujących się w tym menu powoduje wyświetlanie raportów w oknie **Raport**. Użytkownik ma w nim do dyspozycji przycisk **Drukuj**, który pozwala na wydrukowanie raportu na papierze oraz przycisk **Zapisz** pozwalający na zapisanie raportu w pliku **.rtf** lub **.csv**.

3.3.1. Polecenie Grupy

Polecenie **Grupy** powoduje wyświetlenie raportu zawierającego informacje o grupach zdefiniowanych w systemie. Ten sam raport można wygenerować za pomocą przycisku **Raport** w głównym oknie kartoteki grup. Wybranie polecenia **Raport**/**Grupy** spowoduje wyświetlenie raportu **Grupy** w oknie **Raport** (patrz **punkt 3.2.5.4**).

3.3.2. Polecenie Użytkownicy

Polecenie **Użytkownicy** powoduje wyświetlenie raportu zawierającego informacje o użytkownikach wprowadzonych do systemu. Ten sam raport można wygenerować za pomocą przycisku **Raport** w głównym oknie kartoteki użytkowników. Wybranie polecenia **Raport**/**Użytkownicy** spowoduje wyświetlenie raportu **Użytkownicy** w oknie **Raport** (patrz **punkt 3.2.3.5**).

3.3.3. Polecenie Strefy Dostępu

Polecenie **Strefy Dostępu** powoduje wyświetlenie raportu zawierającego informacje o strefach dostępu zdefiniowanych w systemie. Ten sam raport można wygenerować za pomocą przycisku **Raport** w głównym oknie kartoteki stref dostępu. Wybranie polecenia **Raport**/**Strefy Dostępu** spowoduje wyświetlenie raportu **Strefy** w oknie **Raport** (patrz **punkt 3.2.7.4**).

3.3.4. Polecenie Podsystemy

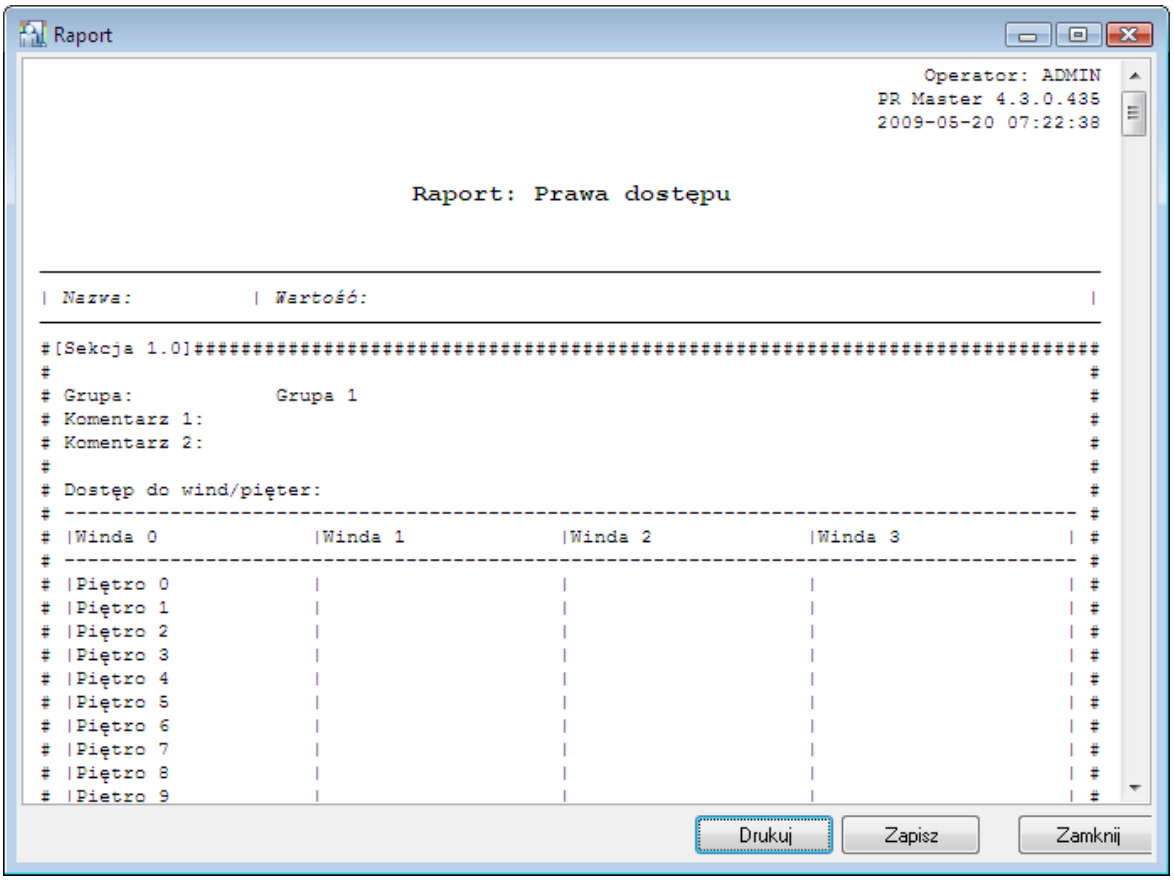
Polecenie **Podsystemy** powoduje wyświetlenie raportu zawierającego informacje o podsystemach zdefiniowanych w systemie KD. Ten sam raport można wygenerować za pomocą przycisku **Raport** w głównym oknie kartoteki podsystemów. Wybranie polecenia **Raport**/**Podsystemy** spowoduje wyświetlenie raportu **Podsystemy** w oknie **Raport** (patrz **punkt 3.2.8.8**).

3.3.5. Polecenie Kontrolery

Polecenie **Kontrolery** powoduje wyświetlenie raportu zawierającego informacje o ustawieniach kontrolerów zainstalowanych w systemie KD. Podobny raport można wygenerować za pomocą przycisku **Raport** w oknie kartoteki kontrolerów wybranego podsystemu. Różnica polega na tym, że w tym przypadku raport obejmuje kontrolery zainstalowane we wszystkich podsystemach. Wybranie polecenia **Raport**/**Kontrolery** spowoduje wyświetlenie raportu **Kontrolery** w oknie **Raport** (patrz **punkt 3.2.8.4**).

3.3.6. Polecenie Prawa dostępu

Wybranie polecenia **Raport**/**Prawa dostępu** spowoduje wyświetlenie raportu **Prawa dostępu** w oknie **Raport** (rysunek 3.94). Raport ten zawiera sumaryczne zestawienie wszystkich grup użytkowników i ich praw dostępu.

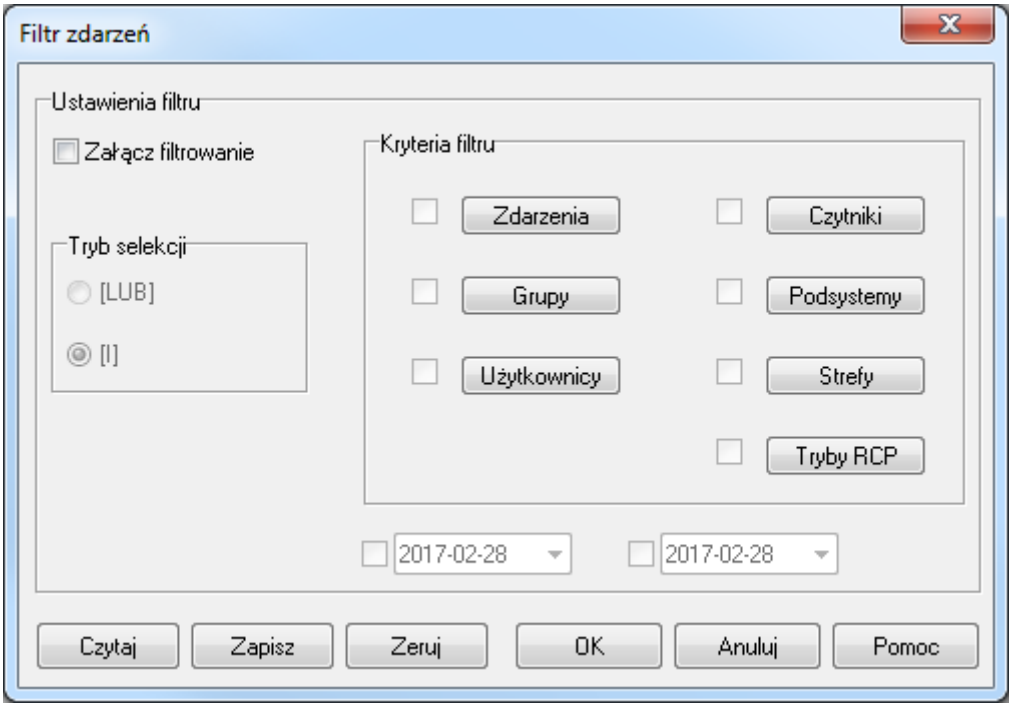


Rysunek 3.94. *Raport „Prawa dostępu”*

3.3.7. Polecenie Zdarzenia

Polecenie **Zdarzenia** pozwala na sporządzanie szczegółowych raportów zdarzeń, raportów RCP oraz raportów specjalnych.

Wybranie polecenia powoduje, że system przystępuje do ściągnięcia zdarzeń z systemu do bazy danych. Następnie wyświetla się okno dialogowe **Filtr zdarzeń** (rysunek 3.95).



Rysunek 3.95. *Ustawienia filtrowania raportu zdarzeń*

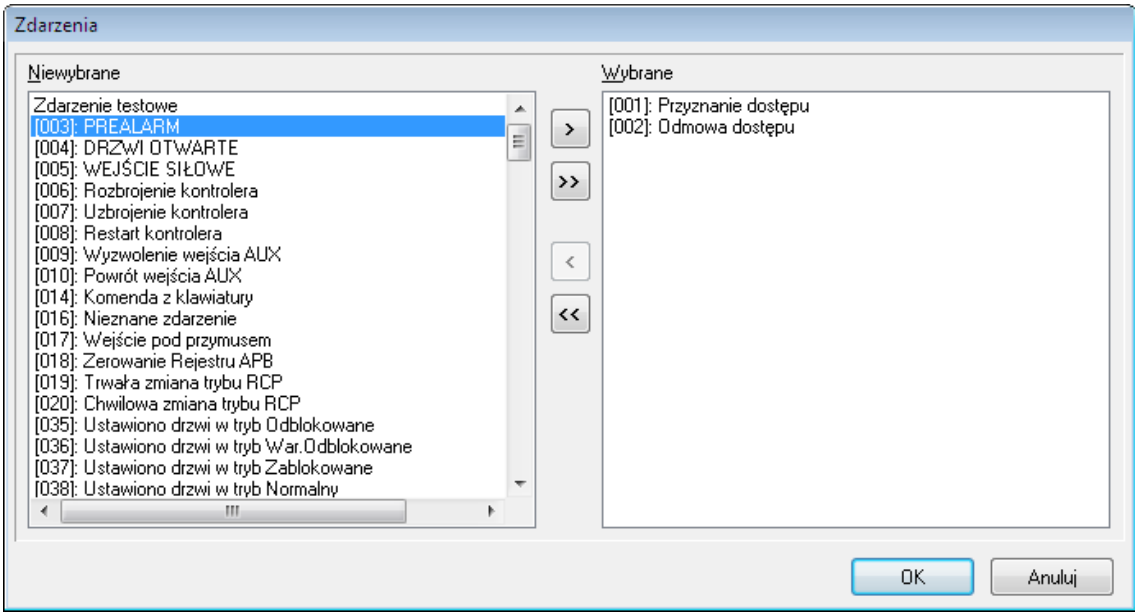
Za pomocą tego okna dialogowego można ustawić dowolny filtr zdarzeń. Dzięki temu można, na przykład, wyświetlić tylko zdarzenia **Przyznanie dostępu** dotyczące użytkownika Jan Kowalski w podanym przedziale czasowym. Zdefiniowany filtr można zapisać w pliku, co umożliwia późniejsze szybkie załadowanie pożądanego zbioru warunków.

Domyślnie maksymalna ilość przetwarzanych i wyświetlanych zdarzeń w historii to 300 000. Możliwe jest zwiększenie ilości zdarzeń podlegających przetwarzaniu poprzez uruchomienie programu PR Master z parametrem /EVLIMIT=x gdzie x oznacza ilość przetwarzanych zdarzeń. Maksymalna możliwa wartość parametru zależy od mocy obliczeniowej komputera i praktyczne testy wykazały, że nie powinna przekraczać wartości 1 000 000. Parametr nie zwiększa maksymalnej ilości zdarzeń wyświetlanych w historii zdarzeń ale pozwala za pomocą filtrowania dotrzeć do szerszego zakresu zdarzeń.

3.3.7.1. Definiowanie filtru

Aby zdefiniować filtr, należy przede wszystkim zaznaczyć pole wyboru **Załącz filtrowanie**. Spowoduje to uaktywnienie kontrolek definiowania filtrów. Filtr definiuje się poprzez wybór trybu selekcji (**[I]** albo **[LUB]**) oraz wskazanie warunków dla wybranych pól rejestru zdarzeń. Warunki można definiować dla siedmiu parametrów: rodzajów zdarzeń, grup, użytkowników, czytników, podsystemów, stref i trybów RCP. Parametrom tym odpowiadają przyciski w obszarze **Kryteria filtru**. Aby sformułować warunek dla danego parametru, należy zaznaczyć pole wyboru znajdujące się obok właściwego przycisku. Następnie należy kliknąć przycisk i sformułować warunek.

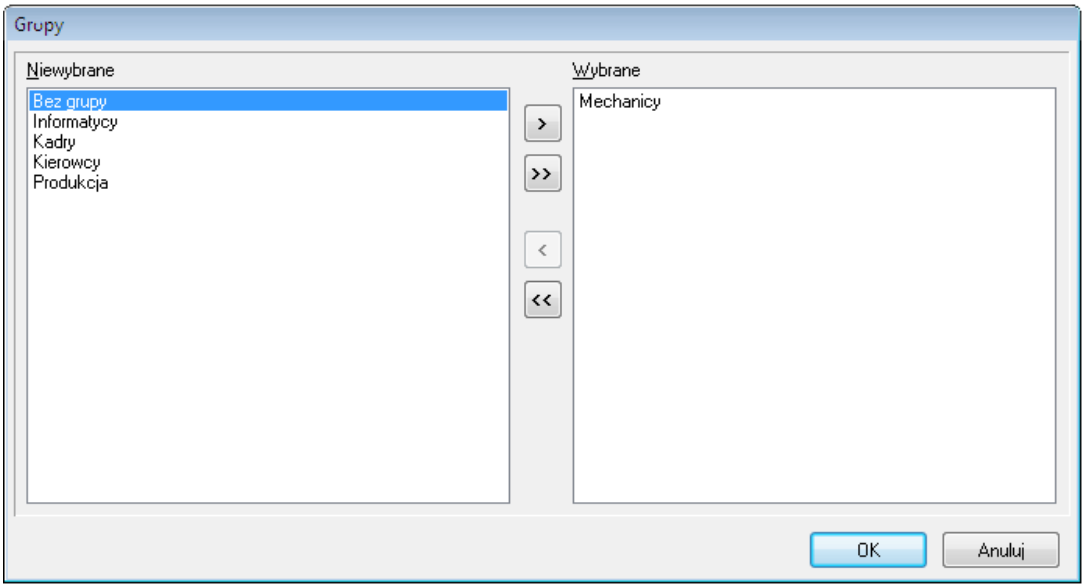
Załóżmy, że chcemy by w raporcie zdarzeń znalazły się tylko zdarzenia **Przyznanie dostępu** i **Odmowa dostępu** dla użytkowników z grupy **Mechanicy**. Aby zdefiniować taki filtr zaznaczamy tryb selekcji **[I]**, oraz pola wyboru obok przycisków **Zdarzenia** i **Grupy**. Następnie klikamy przycisk **Zdarzenia**. Spowoduje to wyświetlenie okna dialogowego **Zdarzenia** (rysunek 3.96).



Rysunek 3.96. *Ustawienie warunku filtrowania zdarzeń — rodzaj zdarzeń*

Z lewej strony okna wyświetla się lista zdarzeń, których nie wybrano, a zatem tych, które nie pojawią się w raporcie. Dwukrotne kliknięcie zdarzenia na tej liście spowoduje przeniesienie danego zdarzenia na listę **Wybrane**. Można również zaznaczyć określone zdarzenie i kliknąć przycisk . Kliknięcie przycisku spowoduje przeniesienie na listę **Wybrane** wszystkich zdarzeń znajdujących się po lewej stronie. Na podobnej zasadzie usuwa się wybrane zdarzenia. Dwukrotne kliknięcie zdarzenia na liście **Wybrane** spowoduje przeniesienie go na listę **Niewybrane**. Można również zaznaczyć określone zdarzenie i kliknąć przycisk . Kliknięcie przycisku spowoduje przeniesienie na listę **Niewybrane** wszystkich zdarzeń znajdujących się aktualnie na liście po prawej stronie.

Wracając do naszego przykładu, aby ustawić pożądany filtr, należy dwukrotnie kliknąć pozycje odpowiadające zdarzeniom **Przyznanie dostępu** oraz **Odmowa dostępu** i kliknąć **OK**. Okno wyboru zdarzeń zamknie się i powrócimy do okna **Filtr zdarzeń**. Teraz klikamy przycisk **Grupy.** Spowoduje to wyświetlenie okna dialogowego **Grupy** (rysunek 3.97).

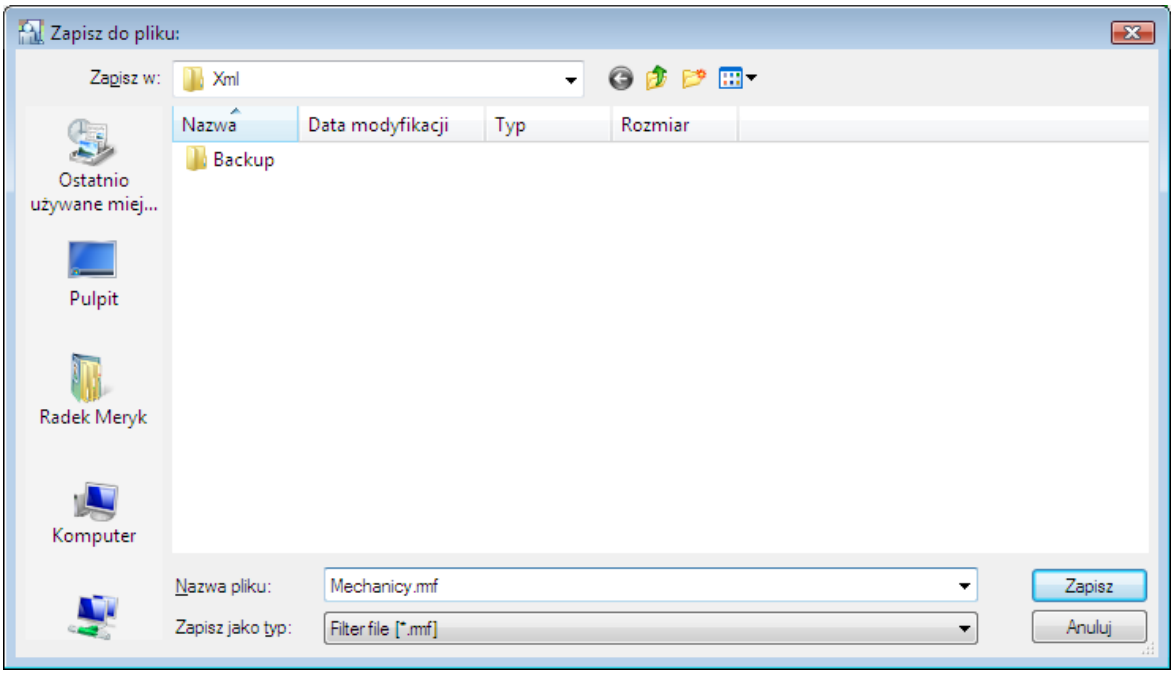


Rysunek 3.97. *Ustawienie warunku filtrowania zdarzeń — grupy*

Wybieramy grupę **Mechanicy** i klikamy **OK**.

Właśnie zdefiniowaliśmy filtr. W raporcie zdarzeń znajdą się wszystkie zdarzenia **Przyznanie dostępu** i **Odmowa dostępu** dla użytkowników z grupy **Mechanicy**. W podobny sposób można sformułować warunki filtrowania dla użytkowników, czytników, podsystemów, stref i trybów RCP.

Tak zdefiniowany filtr możemy zapisać do pliku. W tym celu należy kliknąć przycisk **Zapisz** w oknie dialogowym **Filtr zdarzeń**. Następnie należy wskazać lokalizację, w której ma być zapisany plik z warunkami filtrowania (rozszerzenie **.rmf**) — rysunek 3.98.



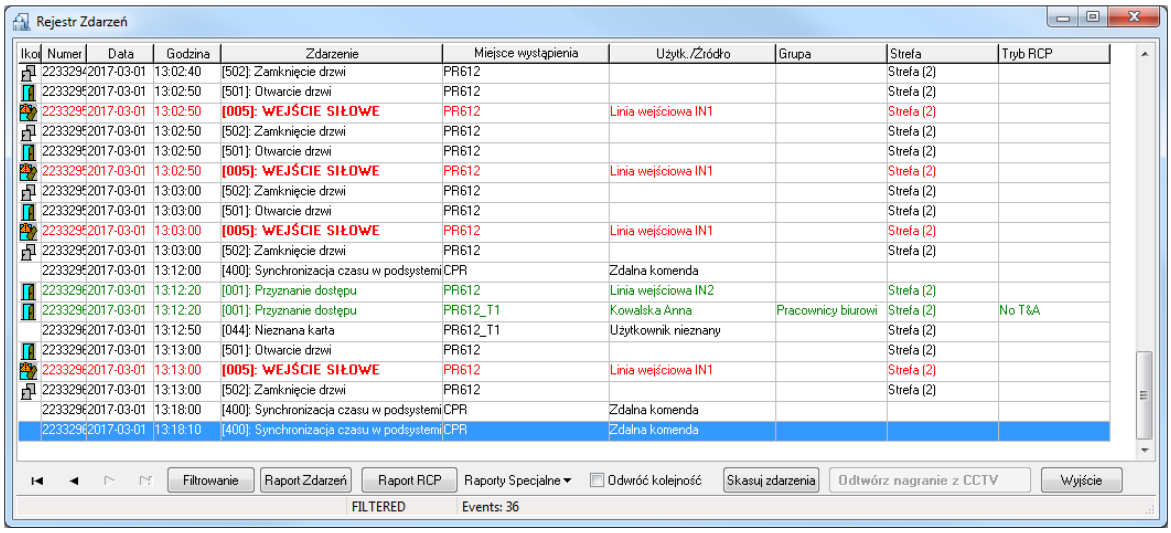
Rysunek 3.98. *Zapisywanie warunku filtrowania w pliku*

Przycisk **Zeruj** pozwala na wyczyszczenie dotychczas zdefiniowanego filtru. W tym momencie możemy zacząć ręczne definiowanie filtra od początku lub wczytać wcześniej zdefiniowany filtr z pliku. Ten drugi sposób jest możliwy za pośrednictwem przycisku **Czytaj**. Jego kliknięcie spowoduje wyświetlenie okna wyboru pliku **.rmf**. Aby wczytać filtr, wybieramy plik z filtrem i klikamy **Otwórz**.

Poniżej obszaru **Kryteria filtrowania** w oknie **Ustawienia filtru** znajdują się dwa pola dat. Lewe określa początkowy zakres dat, a prawe końcowy zakres dat, dla których ma być wygenerowany raport zdarzeń. Polom dat, podobnie jak przyciskom w obszarze **Kryteria filtru**, również towarzyszą pola wyboru. Aby sformułować warunek dla początku okresu, należy zaznaczyć pole wyboru obok lewego pola daty i wprowadzić datę początku okresu, dla którego będzie generowany raport zdarzeń. Podobnie, aby sformułować warunek dla końca okresu, należy zaznaczyć pole wyboru obok prawego pola daty i wprowadzić datę końca okresu, dla którego będzie generowany raport zdarzeń.

3.3.7.2. Wyświetlanie rejestru zdarzeń

Po zakończeniu definiowania filtra, należy kliknąć **OK** w oknie dialogowym **Filtr zdarzeń**. Spowoduje to wyświetlenie okna **Rejestr zdarzeń** (rysunek 3.99).



Rysunek 3.99. *Rejestr zdarzeń*

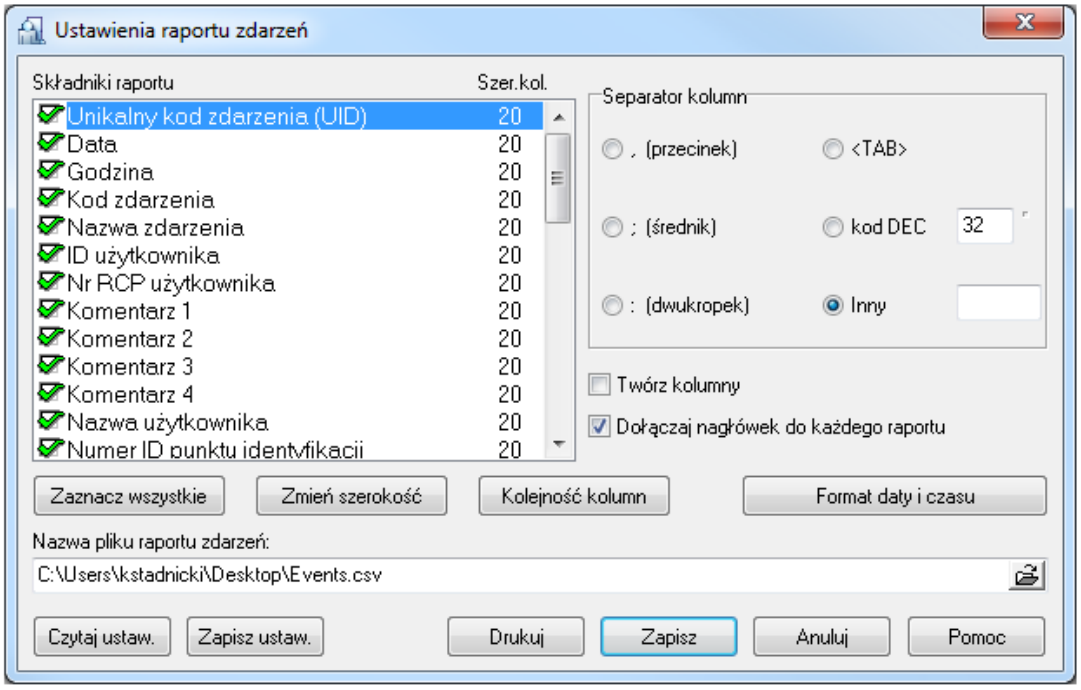
Okno to pozwala na ostateczne przeglądanie/redagowanie listy zdarzeń przed wydrukowaniem raportu zdarzeń. Z tego poziomu można również wydrukować raport RCP lub raporty specjalne.

Przyciski ⏮ ◀ ▶ ⏭ w lewej części paska poleceń pozwalają na poruszanie się po rejestrze zdarzeń. Pozwalają one przejść na początek rejestru zdarzeń, przejść o jedno zdarzenie w górę, przejść o jedno zdarzenie w dół, przejść na koniec rejestru zdarzeń.

Przycisk **Filtrowanie** powoduje ponowne wyświetlenie okna **Filtr zdarzeń**. Można w ten sposób zaktualizować filtr, który został zdefiniowany wcześniej.

Drukowanie raportu zdarzeń

Kliknięcie przycisku **Raport zdarzeń** powoduje wyświetlenie okna dialogowego **Ustawienia raportu zdarzeń** (rysunek 3.100).

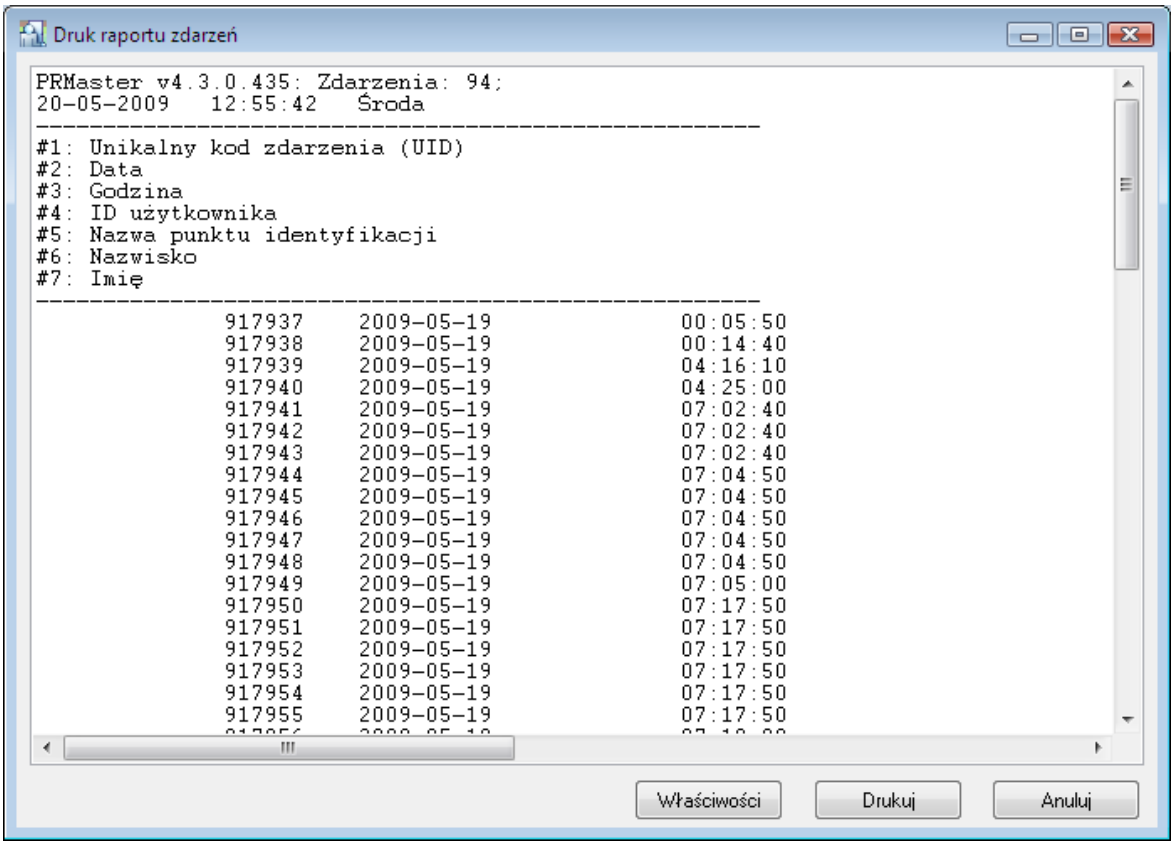


Rysunek 3.100. *Ustawienia raportu zdarzeń*

Za pomocą tego okna dialogowego można dokładnie skonfigurować wydruk raportu zdarzeń. Użytkownik może zaznaczyć kolumny, które mają pojawić się w raporcie, określić ich szerokość, zmienić kolejność kolumn oraz ustalić format daty i czasu.

Ustawienia raportu zdarzeń można zapisać do pliku (przycisk **Zapisz ustaw.**), a później je z niego zaimportować (przycisk **Czytaj ustaw.**).

Po wprowadzeniu wszystkich ustawień, można kliknąć przycisk **Drukuj**, który spowoduje wyświetlenie raportu w oknie **Druk raportu zdarzeń** (rysunek 3.101).

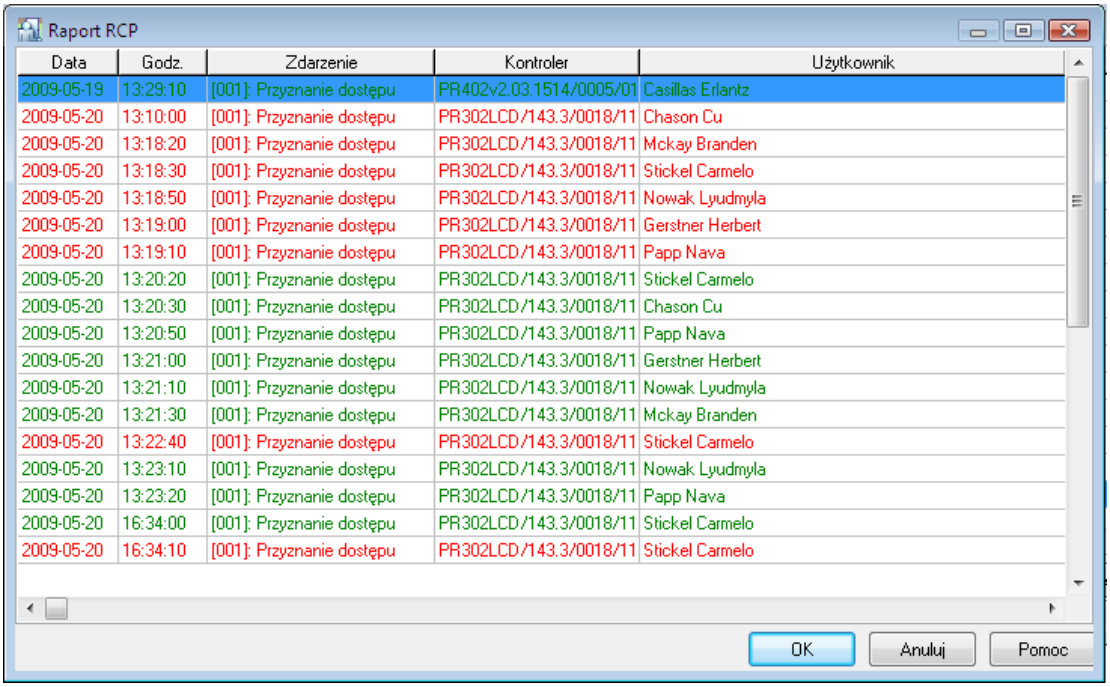


Rysunek 3.101. *Drukowanie raportu zdarzeń*

Aby skierować wydruk na drukarkę, należy kliknąć przycisk **Drukuj**. Wcześniej można wybrać drukarkę i ustawić jej opcje za pomocą przycisku **Właściwości**.

Generowanie raportu RCP

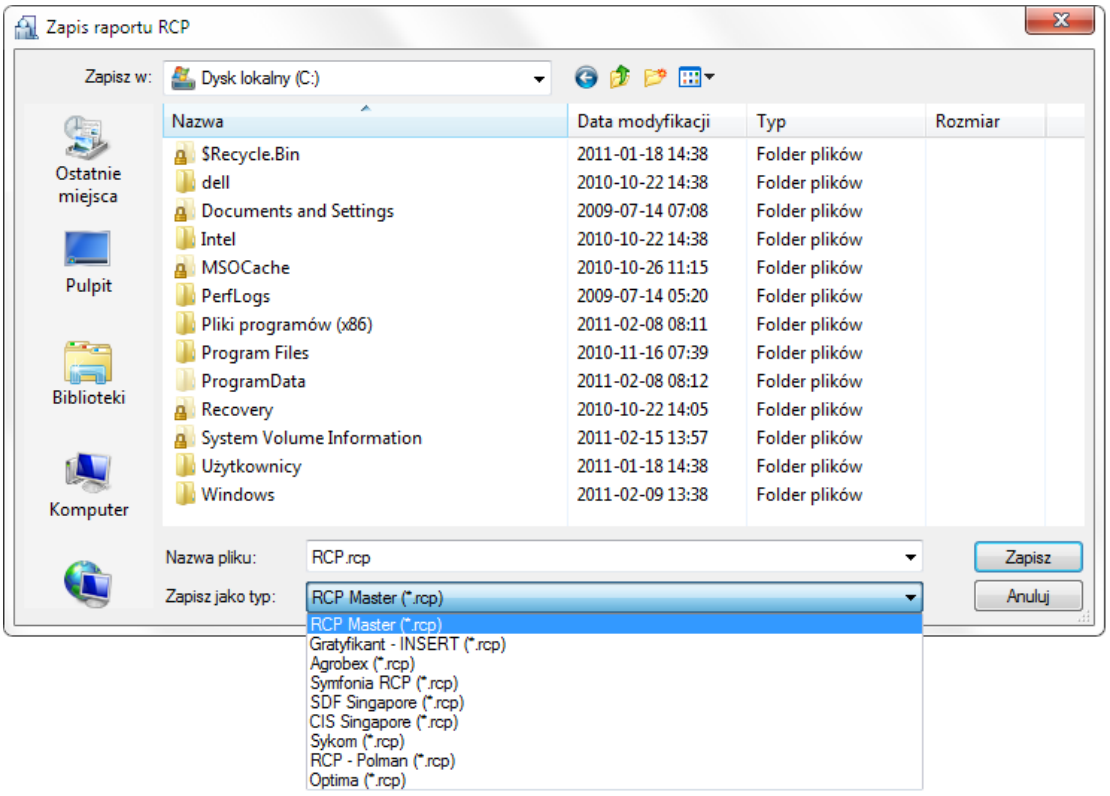
Kliknięcie przycisku **Raport RCP** powoduje wyświetlenie okna dialogowego **Raport RCP** (rysunek 3.102).



Rysunek 3.102. *Generowanie raportu RCP*

W zależności od trybu RCP poszczególne zdarzenia są określone różnymi kolorami. Na przykład, wszystkie wejścia są oznaczone kolorem czerwonym, wyjścia kolorem zielonym, a wyjścia służbowe kolorem niebieskim.

Kliknięcie przycisku **OK** umożliwia zapisanie raportu RCP w wielu różnych formatach (rysunek 3.103).



Rysunek 3.103. *Zapis raportu RCP w wybranym formacie*

Dzięki możliwości zapisu raportu RCP w formatach innych aplikacji, program PR Master może wymieniać dane z zewnętrznymi aplikacjami służącymi do rozliczania czasu pracy.

Program PR Master od wersji 4.5.18 umożliwia bardziej dopasowaną współpracę z programem Symfonia RCP z wykorzystaniem Trybów RCP. Wzajemne zależności pomiędzy Trybami RCP obu programów przedstawiono w poniższej tabeli. Niektóre Tryby RCP Symfonii wymagają zdefiniowania odpowiedników przez administratora systemu po stronie PR Mastera. Tryby RCP można definiować za pomocą polecenia Tryby RCP (patrz **punkt** 3.5.5)

Tryb RCP (PRM)	Parametr 1 (PRM)	Parametr 2 (PRM)	Tryb RCP (Symfonia)	Kod (Symfonia)
Niepredefiniowany	Wejście	Inne	Wejście zwykłe	11
Niepredefiniowany	Wyjście	Inne	Wyjście zwykłe	01
Niepredefiniowany	Wejście	Służb.	Wej. służbowe	12
WYJ. SŁUŻB.	Wyjście	Służb.	Wyj. służbowe	02
WEJŚCIE	Wejście	Pryw.	Wej. prywatne	10
WYJŚCIE	Wyjście	Pryw.	Wyj. prywatne	00

Raporty specjalne

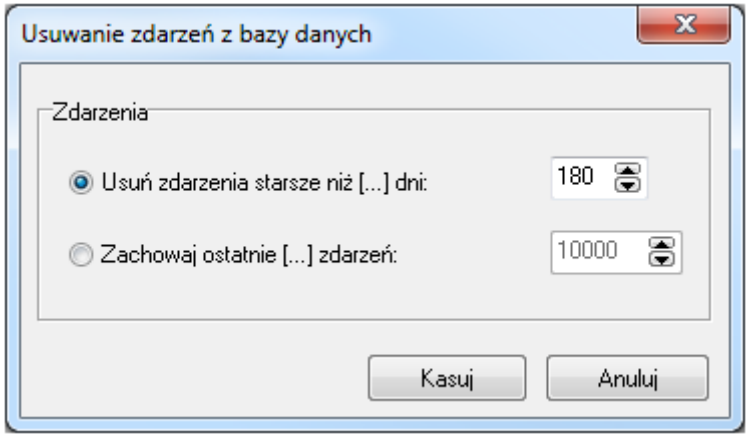
Menu **Raporty specjalne** zostało stworzone w celu definiowania raportów wykonywanych na specjalne zamówienie użytkowników systemu. Na przykład, raport **Raport typu 1** pozwala na wyświetlenie osób, które zalogowały się na wskazanym czytniku. W związku z bardzo indywidualnym charakterem raportów specjalnych, ich szczegółowe omawianie wykracza poza zakres niniejszego dokumentu.

Odwracanie kolejności zdarzeń

Standardowo zdarzenia w oknie **Rejestr zdarzeń** wyświetlają się w porządku od najstarszego do najmłodszego. Aby odwrócić tę kolejność należy zaznaczyć pole wyboru **Odwróć kolejność**.

Usuwanie zdarzeń z bazy danych

W oknie **Rejestr zdarzeń** można również usunąć stare zdarzenia z bazy danych. Do tego celu służy przycisk **Skasuj zdarzenia**. Kliknięcie tego przycisku spowoduje wyświetlenie okna dialogowego **Usuwanie zdarzeń z bazy danych** (rysunek 3.104).



Rysunek 3.104. *Usuwanie zdarzeń z bazy danych*

Za jego pomocą można usunąć z bazy danych zdarzenia starsze od określonej liczby dni (opcja **Usuń zdarzenia starsze niż [...] dni**) lub określić liczbę zdarzeń, które mają pozostać w bazie danych po wykonaniu operacji usuwania (opcja **Zachowaj ostatnie [...] zdarzeń**).

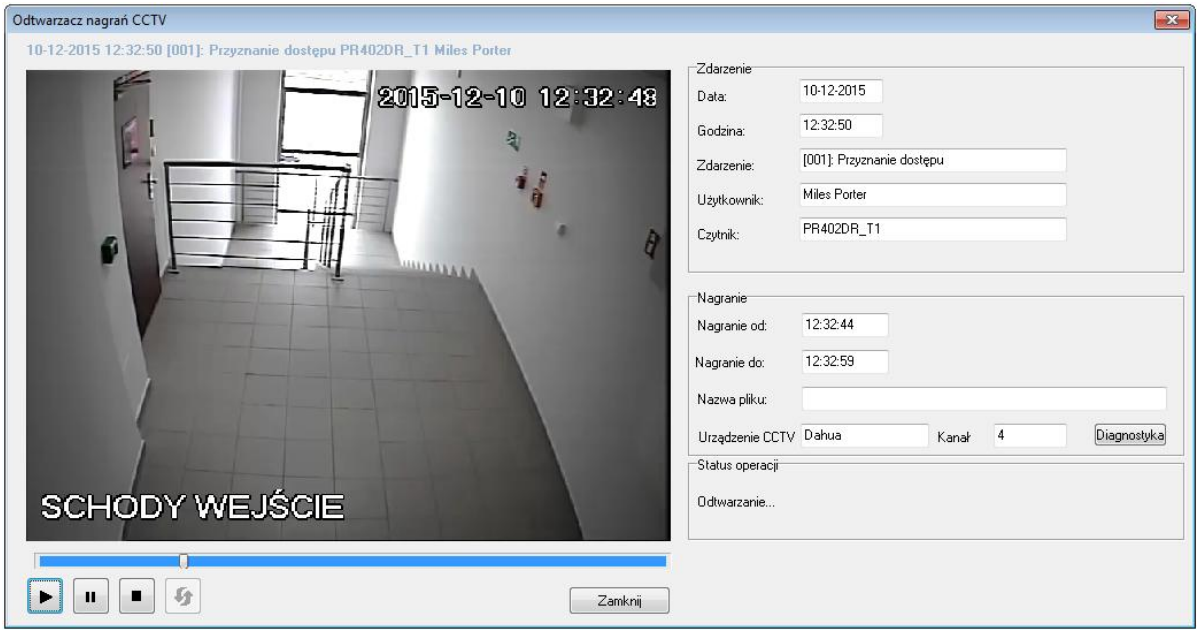
Po zaznaczeniu właściwych opcji należy kliknąć przycisk **Kasuj**, co spowoduje usunięcie zdarzeń z bazy danych.

Zamknięcie rejestru zdarzeń

Aby zamknąć okno rejestru zdarzeń i przejść do głównego okna programu PR Master, należy kliknąć przycisk **Wyjście**.

Odtwórz nagranie z CCTV

Jeżeli skonfigurowana została integracja systemu RACS 4 z obsługiwanymi rejestratorami zgodnie z dedykowaną instrukcją dostępną na stronie **www.roger.pl** to dla określonych zdarzeń możliwe jest odtworzenie filmików zarejestrowanych przez określone kamery w ramach zdefiniowanego przejścia. Do tego celu służy przycisk **Odtwórz nagranie z CCTV**, po użyciu którego wyświetlane jest okno pokazane na rysunku 3.105. Ten przycisk jest dostępny również w trybie monitorowania (patrz **punkt 4.5.1**). W otwartym oknie możliwe jest odtworzenie filmiku, zmiana jego przedziału czasowego jak również uzyskanie informacji na temat jego statusu. W przypadku karty rejestratora GV600/4 możliwe jest również wygenerowanie zdjęcia ze stopklatki poprzez kliknięcie prawym przyciskiem myszki obrazu i wybranie odpowiedniej opcji.

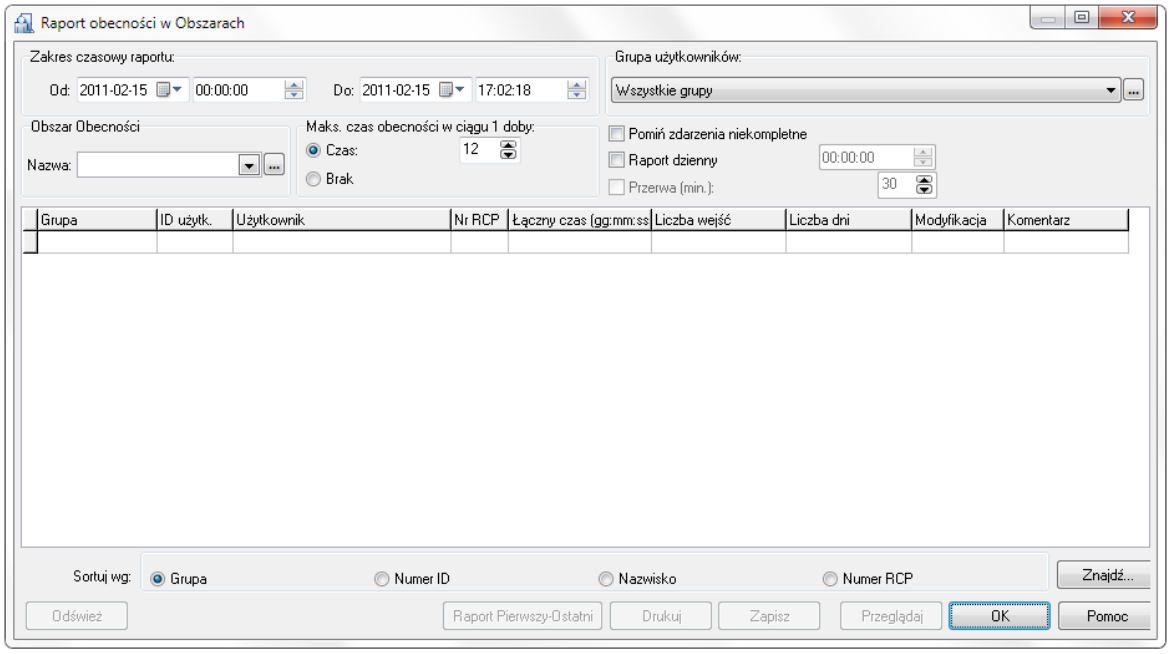


Rysunek 3.105. *Odtwarzacz nagrań z CCTV*

3.3.8. Polecenie Obecności

Polecenie **Obecności** pozwala na wygenerowanie raportu obecności osób w zdefiniowanych obszarach obecności. Za pomocą tego polecenia można dowiedzieć się, na przykład, przez jaki czas w zdefiniowanym obszarze przebywały osoby ze wskazanej grupy. Można też sporządzić raport Pierwszy-Ostatni, który pokazuje, kto pierwszy wchodził i ostatni wychodził do(ze) wskazanego obszaru w wybranym zakresie dat. Korzystanie z Raportów Obecności wymaga skonfigurowania Obszarów Obecności (patrz **punkt 3.2.9**).

Wybranie polecenia **Raporty**/**Obecności** powoduje wyświetlenie okna dialogowego **Raport obecności w obszarach** (rysunek 3.106).



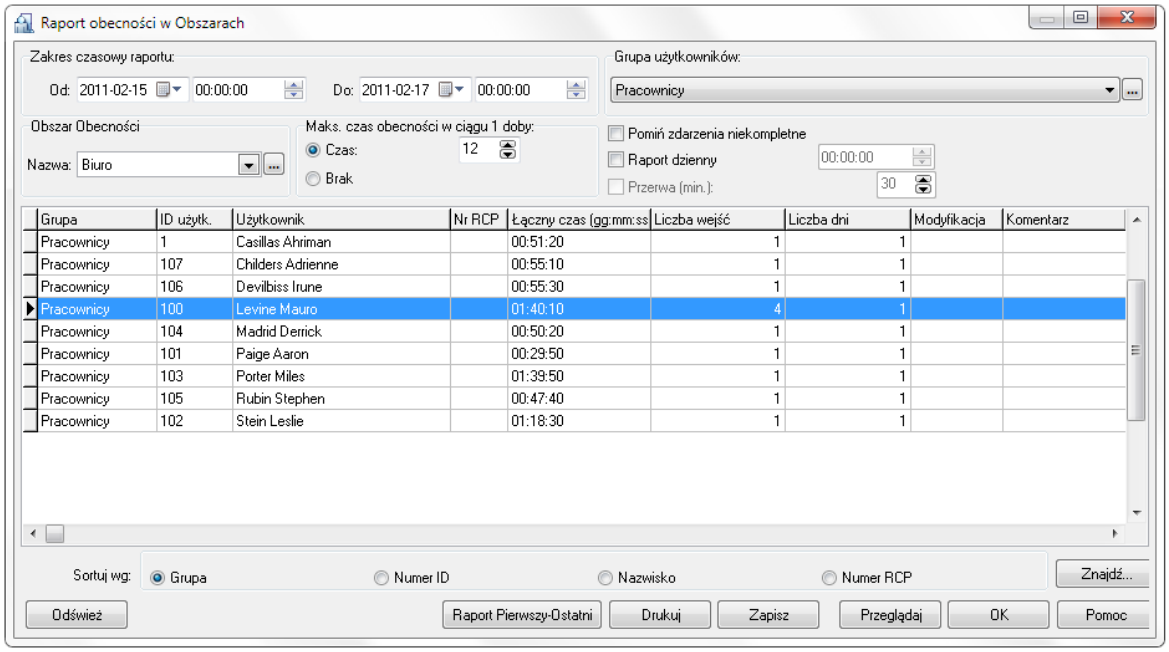
Rysunek 3.106. *Generowanie raportu obecności w obszarach obecności*

Pokazane powyżej okno dialogowe pozwala na:

- określanie zakresu czasowego raportu,
- wskazywanie grupy użytkowników, których ma dotyczyć raport,
- wskazywanie obszaru obecności, którego ma dotyczyć raport,
- określanie maksymalnego czasu obecności w ciągu 1 doby,
- wyszukiwanie pracownika o podanym nazwisku,
- sortowanie rekordów według wskazanego kryterium,
- zapisywanie raportu w pliku,
- drukowanie raportu na drukarce,
- inicjowanie tworzenia raportu Pierwszy-Ostatni.

Po otwarciu okna, lista rekordów obecności jest pusta. Aby ją wygenerować, należy ustawić parametry raportu: zakres czasowy, obszar obecności, maksymalny czas przebywania w obszarze oraz opcjonalnie grupę, której ma dotyczyć raport. Następnie, należy kliknąć przycisk **Odśwież**. Spowoduje to wyświetlenie rekordów obecności w oknie (rysunek 3.107).

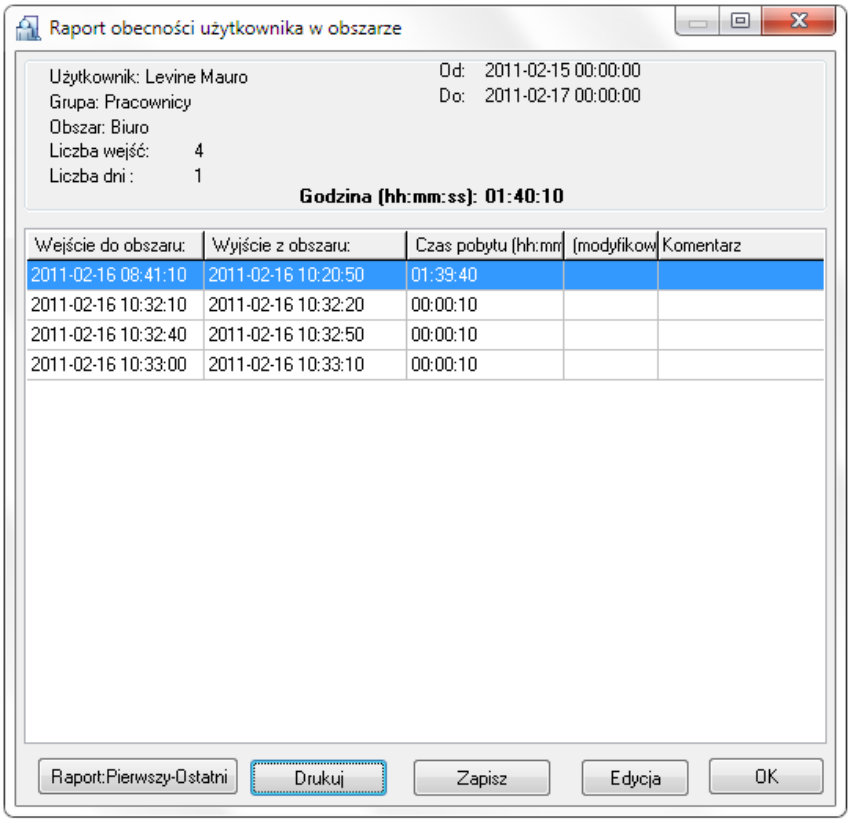
Mechanizmy wewnętrzne stosowane w Raportach Obecności wykorzystują nr ID użytkowników zamiast imion i nazwisk do identyfikacji użytkowników. W związku tym w danym okresie rozliczania/raportowania nie należy zmieniać ani zamieniać nr ID użytkowników. Lepiej to zrobić na koniec takiego okresu (np. na koniec miesiąca). Nie spełnienie tego warunku może skutkować niespójnościami w raporcie.



Rysunek 3.107. *Raport przebywania w obszarze obecności „Biuro" użytkowników z grupy Pracownicy*

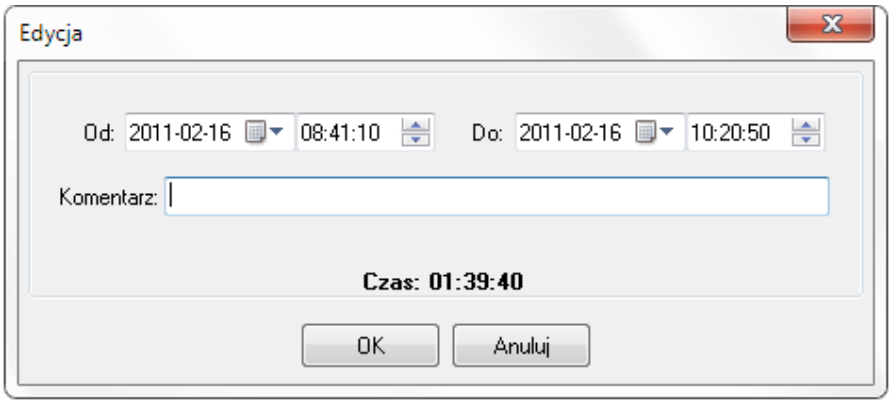
Zaznaczenie pola wyboru **Przerwa** po zaznaczeniu pola wyboru **Raport dzienny** i następnie ustawienie długości trwania przerwy spowoduje, że program automatycznie odliczy przerwę od czasu przebywania użytkownika w określonym obszarze.

Dwukrotne kliknięcie dowolnej pozycji na liście spowoduje wyświetlenie okna dialogowego **Raport obecności użytkownika w obszarze** (rysunek 3.108).



Rysunek 3.108. *Raport obecności wybranego użytkownika we wskazanym obszarze obecności*

W przypadku, gdy rejestr zdarzeń zawiera błędne dane dotyczące danego użytkownika, można je zmodyfikować. W tym celu należy kliknąć dwukrotnie pozycję na liście lub wybrać ją i następnie kliknąć **Edycja**. Spowoduje to wyświetlenie okna dialogowego **Edycja** (rysunek 3.109), które pozwala na skorygowanie błędnego zapisu oraz ewentualne dodanie komentarza.

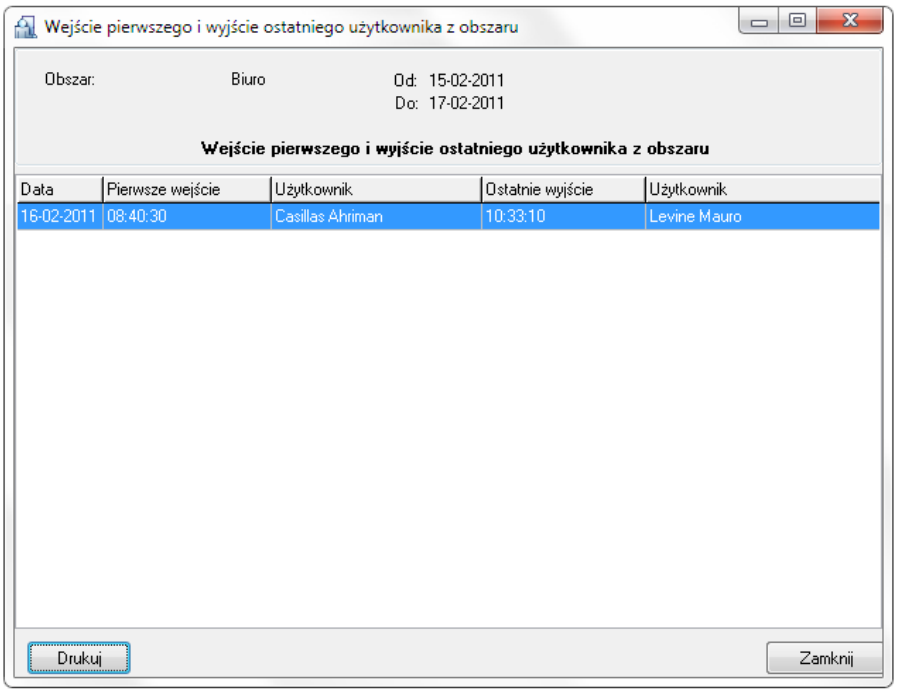


Rysunek 3.109. *Korekta błędnych zapisów oraz dodawanie komentarzy w raporcie obecności*

Po zmodyfikowaniu zapisu i kliknięciu **OK**, zmodyfikowana pozycja jest oznaczona na liście zdarzeń znakiem „V".

Aby wydrukować zdarzenia dotyczące obecności w obszarze określonego pracownika, należy kliknąć **Drukuj**. Przycisk **Zapisz** pozwala na zapis raportu w pliku o formacie **.rtf** lub **.csv**.

Jeśli użytkownik w ciągu dnia kilka razy wchodził i wychodził z obszaru obecności, to program standardowo wskaże wszystkie okresy przebywania użytkownika i zliczy sumaryczny czas. Czasami jednak istotną informacją jest pierwsze wejście i ostatnie wyjście użytkownika z systemu. Do tego celu można wykorzystać przycisk **Raport:Pierwszy-Ostatni** widoczny na rysunku 3.107. Kliknięcie tego przycisku spowoduje wyświetlenie zestawienie pierwszych wejść i ostatnich wyjść wskazanego użytkownika w wybranym zakresie dat (rysunek 3.110).



Rysunek 3.110. *Raport „Pierwsze wejście - ostatnie wyjście" dla wskazanego obszaru w wybranym zakresie dat*

Raport ten można wydrukować, albo zapisać w formacie **.rtf** lub **.csv**.

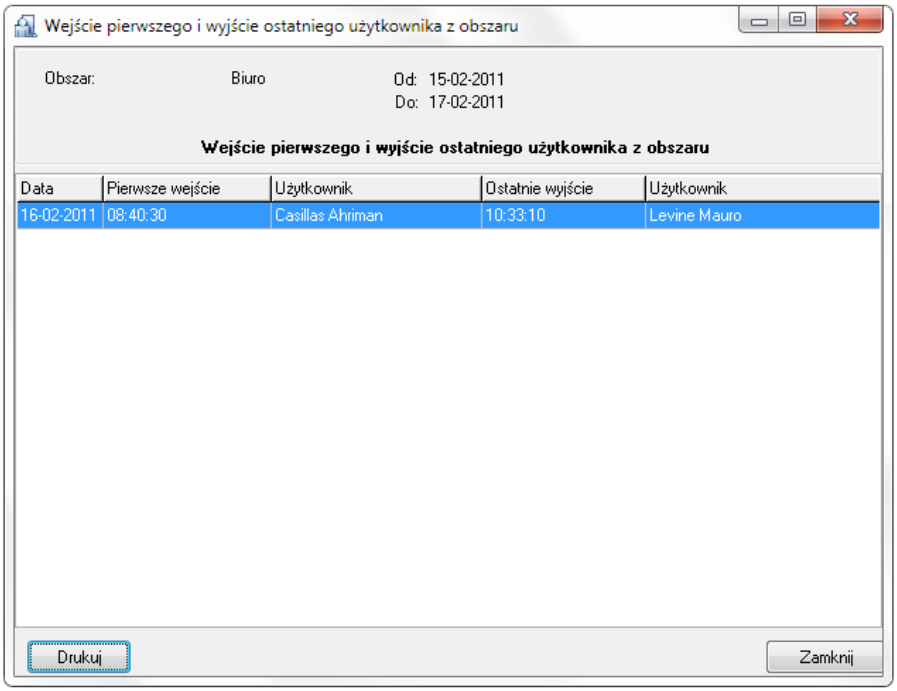
Identyczny raport można uzyskać poprzez zaznaczenie pola wyboru **Raport dzienny** przed odświeżeniem listy rekordów w oknie raportu obecności. Dla wygody dodano jednak przycisk **Raport Pierwszy-Ostatni**, który generuje zestawienie pierwszych wejść i ostatnich wyjść z obszaru niezależnie od tego, czy użytkownik zaznaczył pole wyboru **Raport dzienny**, czy nie.

Przycisk **Raport Pierwszy-Ostatni** występuje również w głównym oknie **Raport obecności w obszarach** (rysunek 3.107). W tym przypadku raport ten generuje zestawienie, w którym znajdują się nazwiska osób, które pierwsze weszły do obszaru i ostatnie wyszły z obszaru dla wskazanego zakresu dat. Raport ten opisano w **punkcie 3.3.8.1**, bezpośrednio poniżej tej ramki.

3.3.8.1. Raport Pierwszy-Ostatni

Czasami istotna jest informacja o tym, kto wchodził do obszaru jako pierwszy oraz kto z niego wychodził jako ostatni. Może to być przydatne, na przykład w sytuacji, kiedy chcemy ustalić, kto otwierał dane pomieszczenie i kto je zamykał.

Do tego celu można wykorzystać przycisk **Raport Pierwszy-Ostatni** występujący w głównym oknie **Raport obecności w obszarach** (rysunek 3.107). Kliknięcie tego przycisku spowoduje wygenerowanie zestawienia z nazwiskami osób, które pierwsze weszły do obszaru i ostatnie z niego wyszły dla wskazanego zakresu dat (rysunek 3.111).

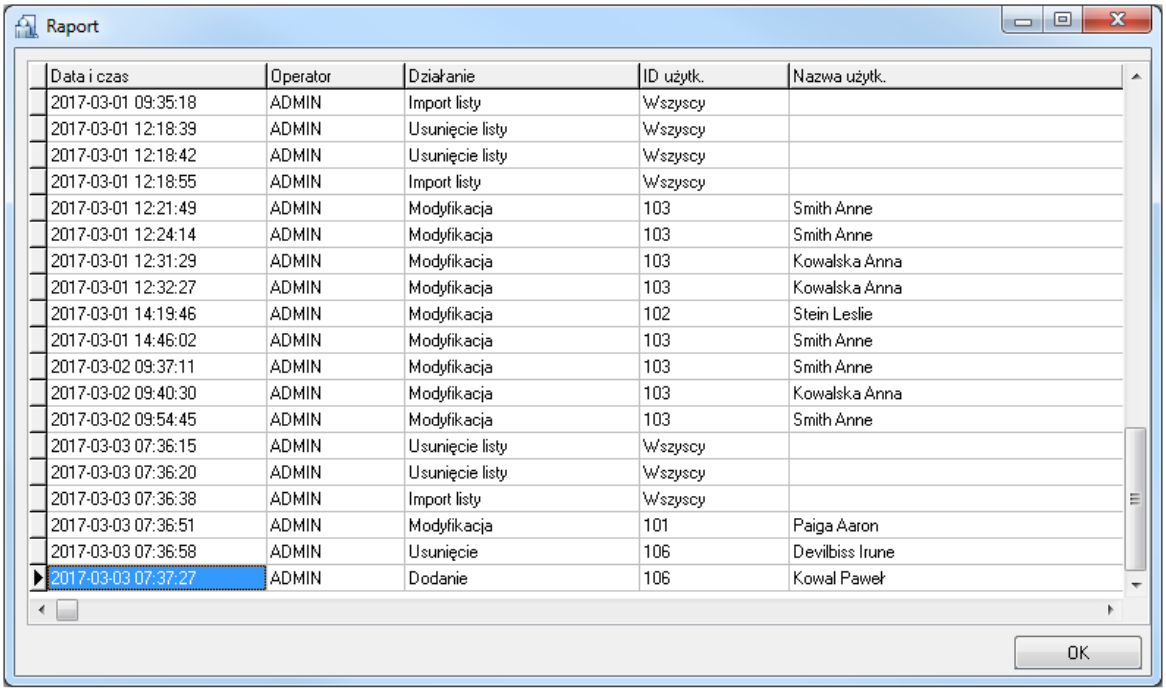


Rysunek 3.111. *Raport „Pierwsze wejście - ostatnie wyjście" dla wskazanego zakresu dat*

Standardowo raport można wydrukować, albo zapisać w formatach **.csv** lub **.rtf**.

3.3.9. Polecenie Modyfikacje użytkowników

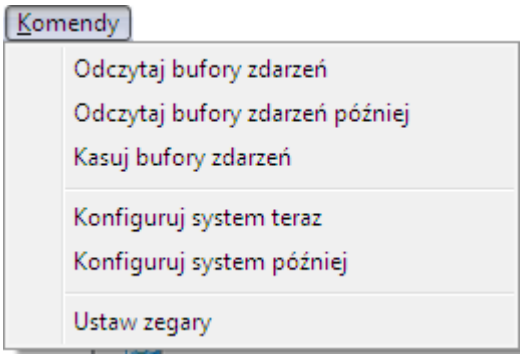
Polecenie **Modyfikacje użytkowników** pozwala na wygenerowanie raportu zawierającego listę zmian wprowadzonych przez danego operatora w zakresie użytkowników systemu. Raport odnotowuje takie działania jak dodanie, usunięcie i modyfikacja użytkownika jak też usunięcie oraz import całej listy użytkowników.



Rysunek 3.112. *Przykładowy raport 'Modyfikacje użytkowników'*

3.4. MENU KOMENDY

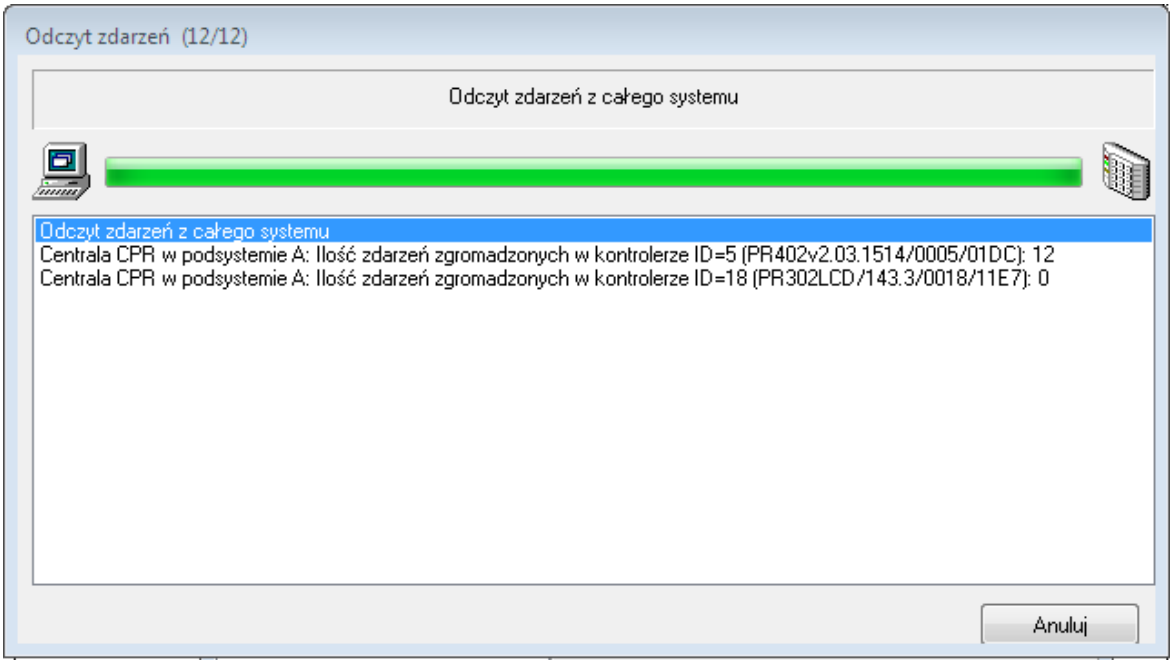
Menu **Komendy** pokazano na rysunku 3.112.



Rysunek 3.112. *Menu Komendy*

3.4.1. Polecenie Odczytaj bufory zdarzeń

W systemie RACS 4 zdarzenia są zapisywane w kontrolerach serii PRxx2 albo centrali CPR. Wybór polecenia **Odczytaj bufory zdarzeń** powoduje przepisanie zawartości buforów zdarzeń do bazy danych programu PR Master. Jeśli program PR Master pracuje w trybie monitorowania, dopisywanie zdarzeń odbywa się na bieżąco. Po wybraniu polecenia, system zapyta **Czy odczytać bufory zdarzeń teraz?**. Twierdząca odpowiedź na to pytanie spowoduje zainicjowanie procesu odczytu zdarzeń (rysunek 3.113).



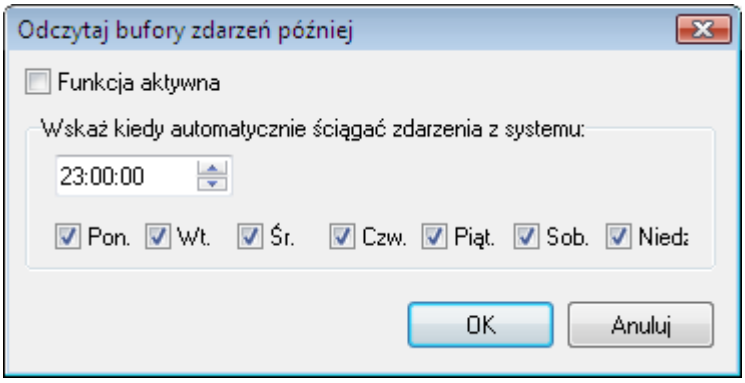
Rysunek 3.113. *Odczyt zdarzeń z systemu*

Po zakończeniu procesu odczytu zdarzeń system wyświetli informację potwierdzającą sukces operacji.

3.4.2. Polecenie Odczytaj bufory zdarzeń później

W przypadku rozbudowanego systemu kontroli dostępu, proces odczytywania zdarzeń może zająć sporo czasu. W związku z tym, aby nie tracić czasu na bierne oczekiwanie, operator może zaplanować tę operację o określonej godzinie we wskazanych dniach tygodnia. Do tego celu służy polecenie **Odczytaj bufory zdarzeń później**.

Wybranie tego polecenia spowoduje wyświetlenie okna dialogowego **Odczytaj bufory zdarzeń później** (rysunek 3.114).



Rysunek 3.114. *Planowanie automatycznego odczytywania zdarzeń z systemu*

W powyższym oknie dialogowym należy zaznaczyć dni tygodnia, w których ma być wykonywane automatyczne ściąganie zdarzeń z systemu oraz wybrać godzinę dla tej operacji.

Aby uaktywnić funkcję należy zaznaczyć pole wyboru **Funkcja aktywna**. W przeciwnym przypadku harmonogram nie będzie realizowany.

3.4.3. Polecenie Kasuj bufory zdarzeń

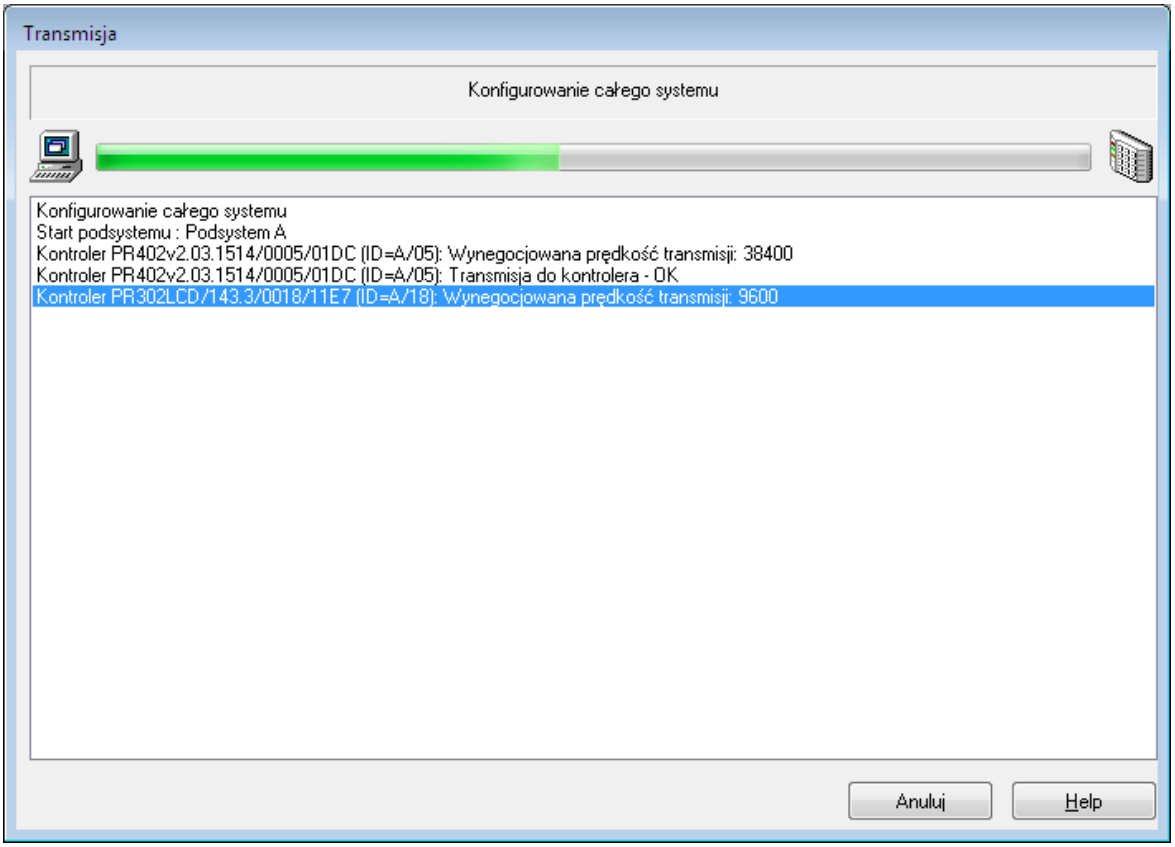
Polecenie **Kasuj bufory zdarzeń** pozwala na usunięcie na żądanie zdarzeń zapisanych w buforach urządzeń we wszystkich podsystemach systemu KD. Wybranie polecenia spowoduje wyświetlenie pytania o potwierdzenie zamiaru wykonania tej operacji. Twierdząca odpowiedź na to pytanie powoduje skasowanie zawartości wszystkich buforów zdarzeń i wyświetlenie informacji o wykonaniu operacji.

3.4.4. Polecenie Konfiguruj system teraz

Polecenie **Konfiguruj system teraz** służy do przesyłania ustawień do wszystkich kontrolerów oraz central CPR we wszystkich podsystemach. W przypadku, gdy system KD jest rozbudowany, operacja ta może być długotrwała, dlatego należy wykonywać ją jak najrzadziej — po wprowadzeniu wszystkich niezbędnych zmian.

Operację konfiguracji systemu inicjuje wybranie komendy **Konfiguruj system teraz**. Jeśli w tym momencie w urządzeniach systemu są zgromadzone jakieś zdarzenia, system przed przesłaniem ustawień spyta o to, co należy z nimi zrobić. Można je skasować lub odczytać do bazy danych. W przypadku decyzji o odczytaniu zdarzeń, system wyświetli okno informacyjne zawierające dane o postępach operacji odczytu.

Po wyświetleniu komunikatu o zakończeniu odczytu zdarzeń system przechodzi do operacji konfigurowania całego systemu (rysunek 3.115).

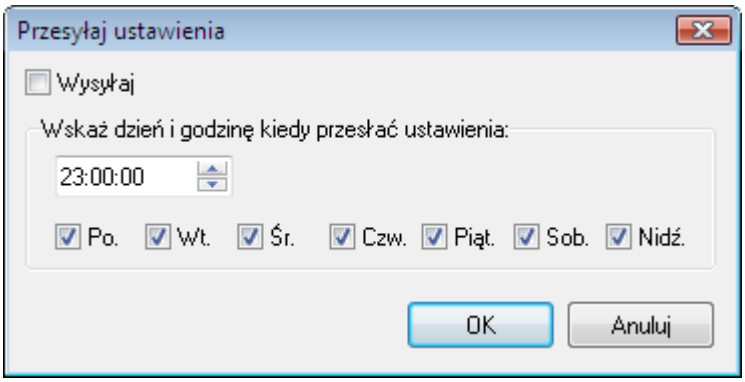


Rysunek 3.115. *Konfigurowanie całego systemu — okno postępu operacji*

3.4.5. Polecenie Konfiguruj system później

Ponieważ operacja konfigurowania całego systemu może zająć dużo czasu, istnieje możliwość zaplanowania tej operacji na określoną godzinę we wskazanych dniach tygodnia. Do tego celu służy polecenie **Konfiguruj system później**.

Wybranie tego polecenia spowoduje wyświetlenie okna dialogowego **Przesyłaj ustawienia** (rysunek 3.116).



Rysunek 3.116. *Planowanie automatycznego konfigurowania całego systemu*

W powyższym oknie dialogowym należy zaznaczyć dni tygodnia, w których ma być wykonywane automatyczne konfigurowanie systemu oraz wybrać godzinę dla tej operacji.

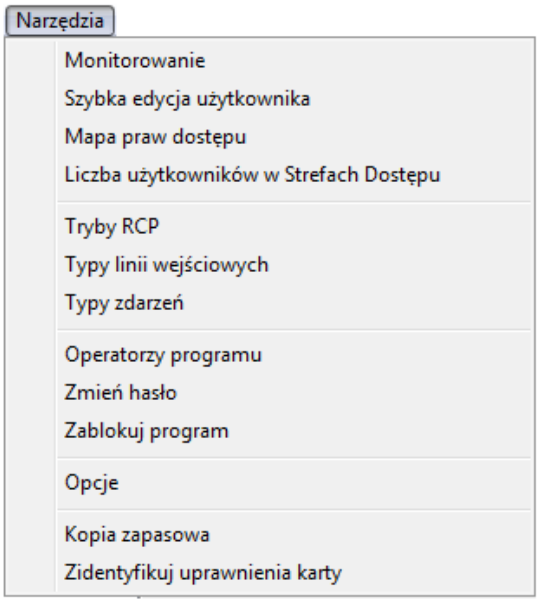
Aby uaktywnić funkcję należy zaznaczyć pole wyboru **Wysyłaj**. W przeciwnym przypadku harmonogram konfigurowania systemu nie będzie realizowany.

3.4.6. Polecenie Ustaw zegary

Polecenie Ustaw zegary pozwala na ustawienie zegarów urządzeń systemu RACS 4 zgodnie z czasem systemowym komputera, na którym jest zainstalowany system PR Master.

3.5. MENU NARZĘDZIA

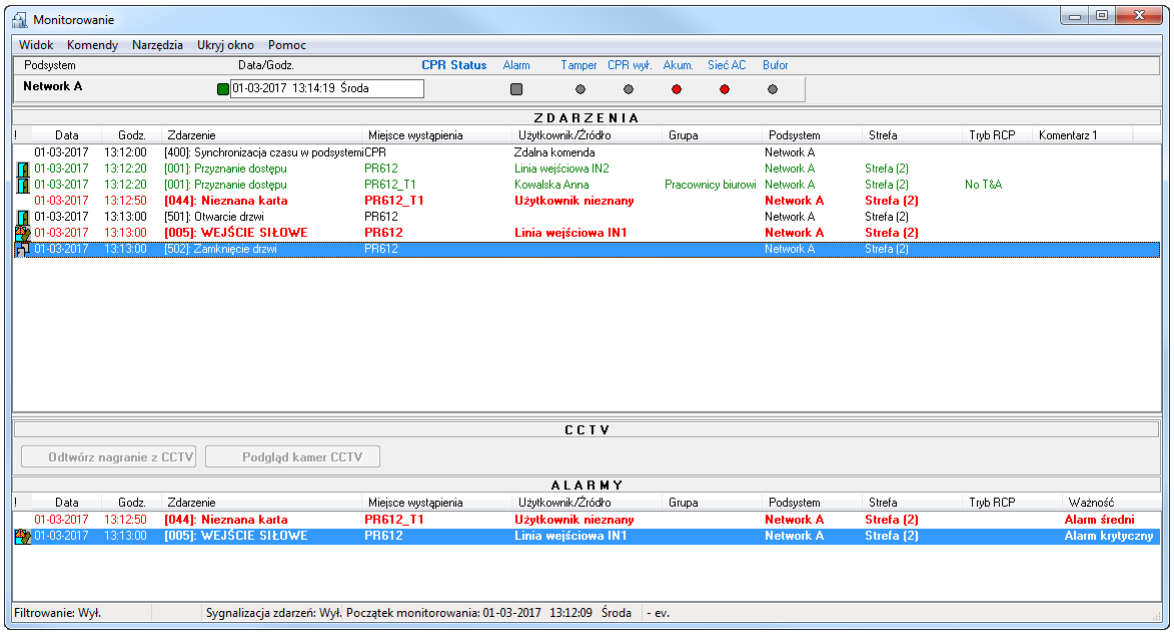
Menu **Narzędzia** pokazano na rysunku 3.117.



Rysunek 3.117. *Menu Narzędzia*

3.5.1. Polecenie Monitorowanie

Monitorowanie włącza tryb pracy programu PR Master umożliwiający obserwację w czasie rzeczywistym zdarzeń zachodzących w systemie RACS 4. Kiedy program PR Master jest w trybie monitorowania, zdarzenia powstałe w systemie są natychmiast dopisywane do bazy danych systemu i dostępne do tworzenia raportów. Wybranie polecenia **Monitorowanie** każdorazowo wymusza odczyt zdarzeń z buforów w całym systemie. Następnie system przechodzi do trybu monitorowania online (rysunek 3.118).



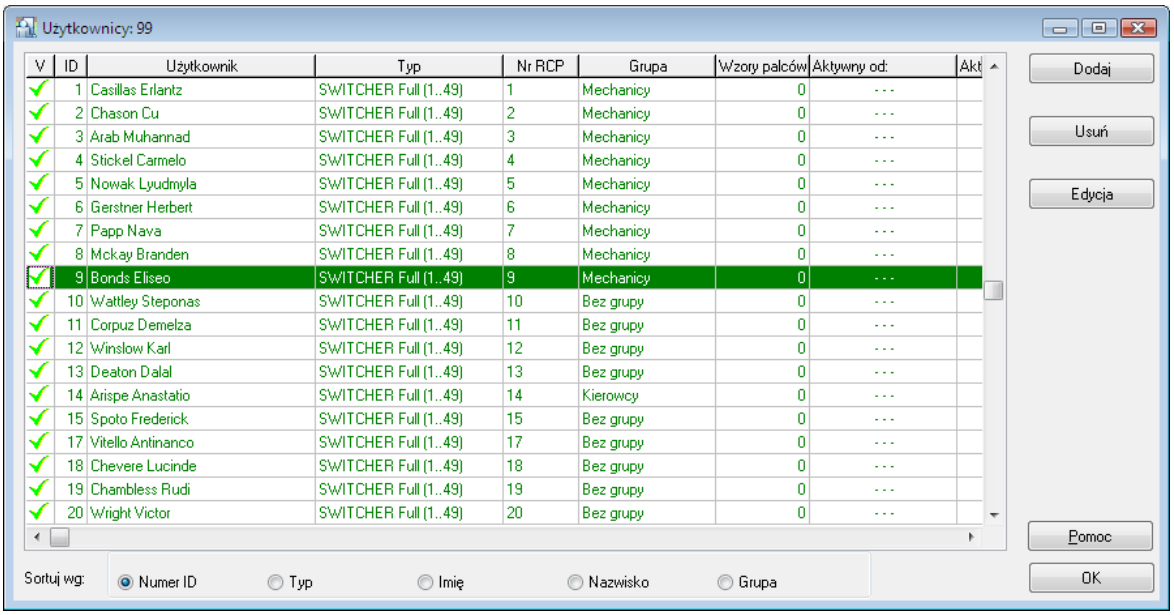
Rysunek 3.118. *Monitorowanie zdarzeń w programie PR Master*

W tym trybie pracy program PR Master posiada osobne, rozbudowane menu. Zostanie ono opisane **w rozdziale 4**.

3.5.2. Polecenie Szybka edycja użytkowników

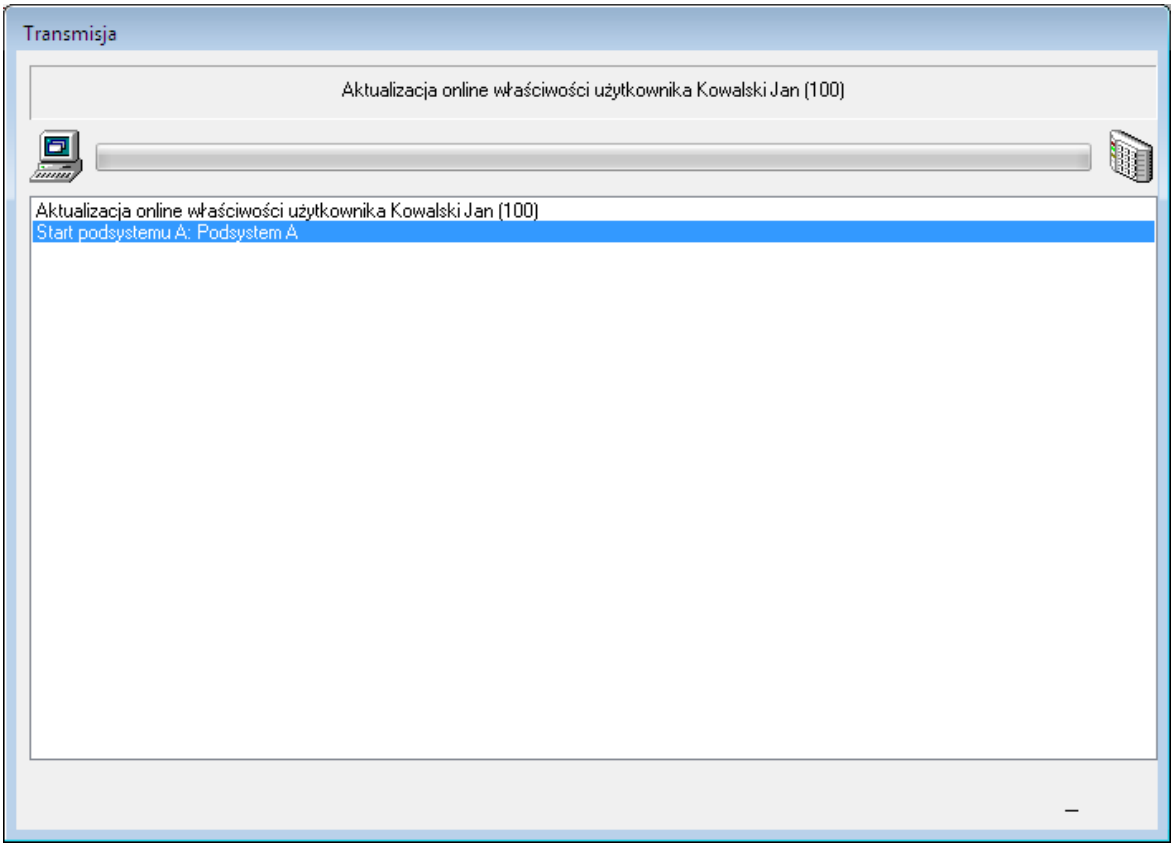
Każdorazowa zmiana właściwości użytkownika — tzn. zmiana przydziału do grupy, wymiana karty zbliżeniowej, czy kodu PIN wymaga przesłania danych do kontrolerów. Ze względu na to, że operacja przesyłania całej konfiguracji do wszystkich kontrolerów w systemie jest czasochłonna, a zmiany wykonywane w konfiguracji są znacznie rzadsze w porównaniu z zadaniami administracji użytkownikami, w systemie istnieje możliwość tzw. szybkiej edycji użytkowników. Operacja ta pozwala na przesłanie do kontrolerów jedynie zmienionych właściwości pojedynczego użytkownika.

Wybranie polecenia powoduje wyświetlenie okrojonej wersji okna kartoteki użytkowników (rysunek 3.119).



Rysunek 3.119. *Szybka edycja użytkowników*

Okno to pozwala na dodawanie, usuwanie i modyfikowanie właściwości użytkowników. W przypadku dodania użytkownika do systemu lub aktualizacji jego właściwości i zatwierdzeniu przyciskiem OK, program automatycznie prześle nowe dane do kontrolerów (rysunek 3.120).



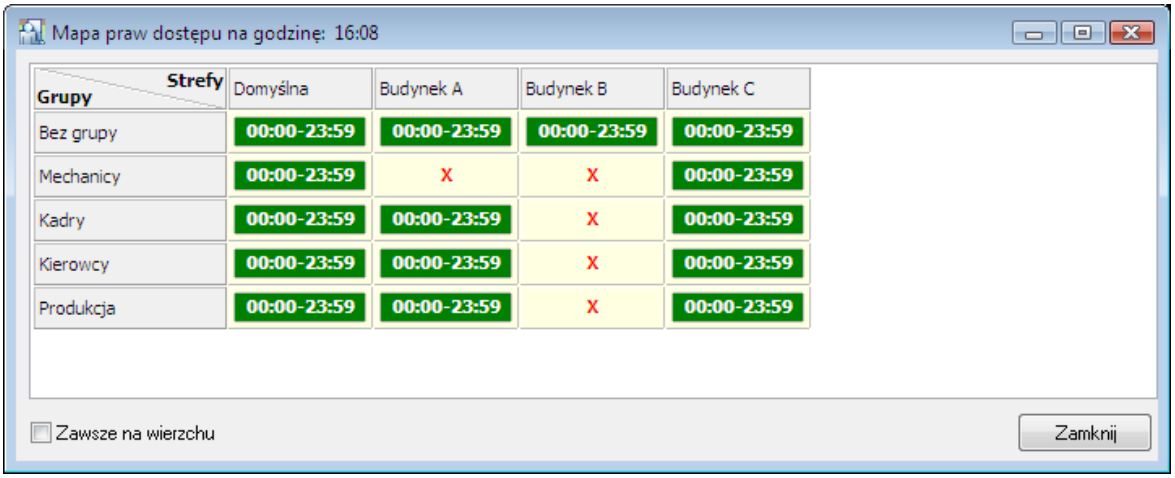
Rysunek 3.120. *Aktualizacja online właściwości użytkownika*

Ze zrozumiałych względów, operacja ta przebiega znacznie szybciej od konfiguracji całego systemu.

Operacja szybkiej edycji użytkownika może być wykonywana tylko pojedynczo. Oznacza to, że nie można zmienić danych kilku użytkowników, a potem przesłać danych całej grupy na raz.

3.5.3. Polecenie Mapa praw dostępu

Polecenie **Mapa praw dostępu** wyświetla bieżący stan uprawnień dostępu. Wybranie polecenia powoduje wyświetlenie okna dialogowego **Mapa praw dostępu na godzinę: xx:xx** (rysunek 3.121).

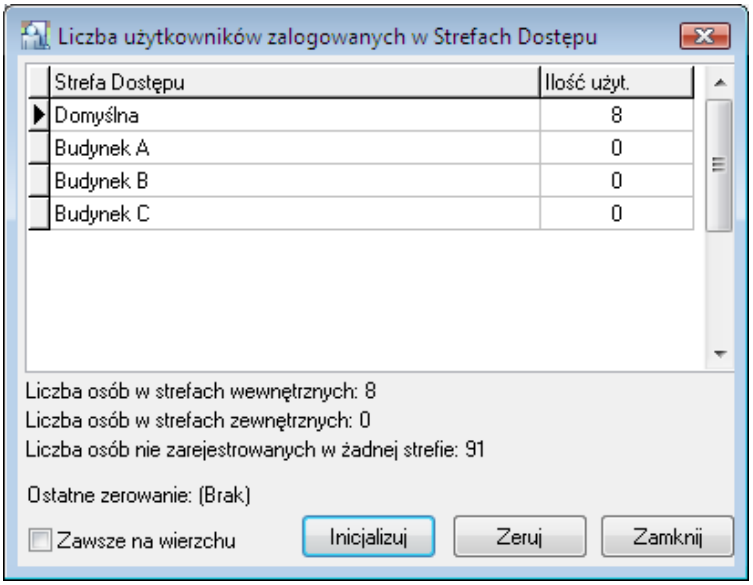


Rysunek 3.121. *Mapa praw dostępu w systemie*

Jeśli w danym momencie określona grupa ma prawa dostępu w określonej strefie, to w tabelce na przecięciu się wiersza grupy i kolumny strefy wyświetla się przedział czasowy, w jakim to uprawnienie występuje. Jeśli natomiast dana grupa nie ma aktualnie uprawnienia w strefie (np. ze względu na ograniczenia harmonogramu czasowego), to na przecięciu się strefy i grupy wyświetla się czerwony symbol **x**.

3.5.4. Polecenie Liczba użytkowników w Strefach Dostępu

Polecenie **Liczba użytkowników w Strefach Dostępu** wyświetla zestawienie stref dostępu wraz z liczbą zalogowanych w nich osób (rysunek 3.122).

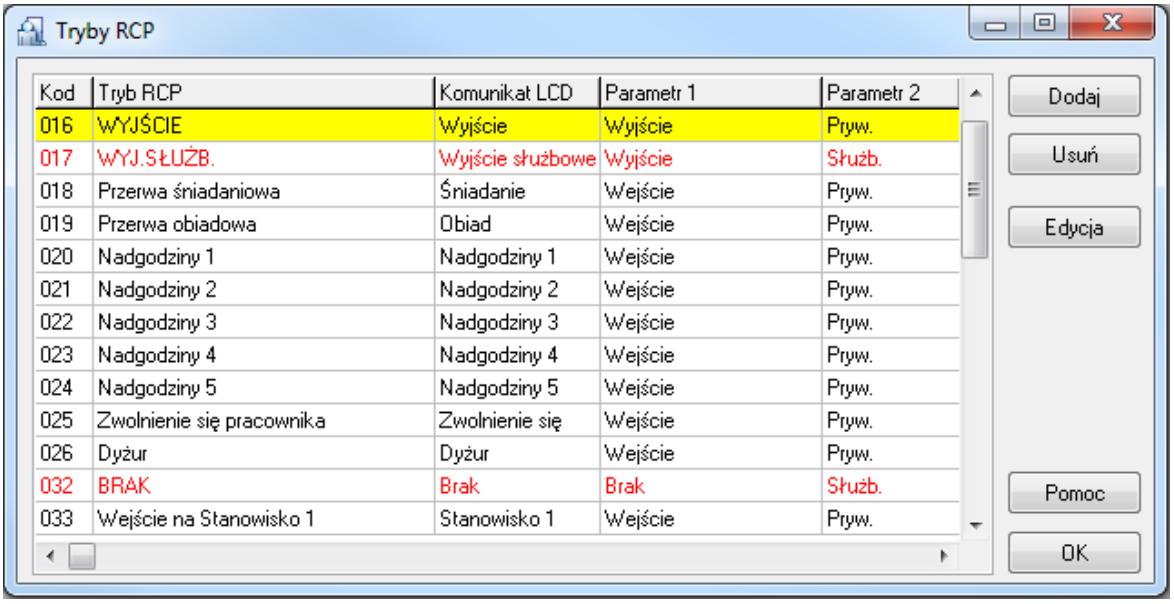


Rysunek 3.122. *Liczba użytkowników zalogowanych w poszczególnych strefach dostępu*

Przycisk **Inicjalizuj** powoduje zainicjowanie tabeli w oparciu o bieżący rejestr zdarzeń systemu RACS 4. Przycisk **Zeruj** powoduje wyzerowanie tabeli. Od momentu wyzerowania, system zaczyna zliczać liczbę osób w strefach dostępu na nowo. Jednak w przypadku ponownego użycia przycisku **Inicjalizuj**, system usuwa informację o zerowaniu.

3.5.5. Polecenie Tryby RCP

Polecenie **Tryby RCP** otwiera kartotekę trybów RCP w systemie RACS 4 (rysunek 3.123).

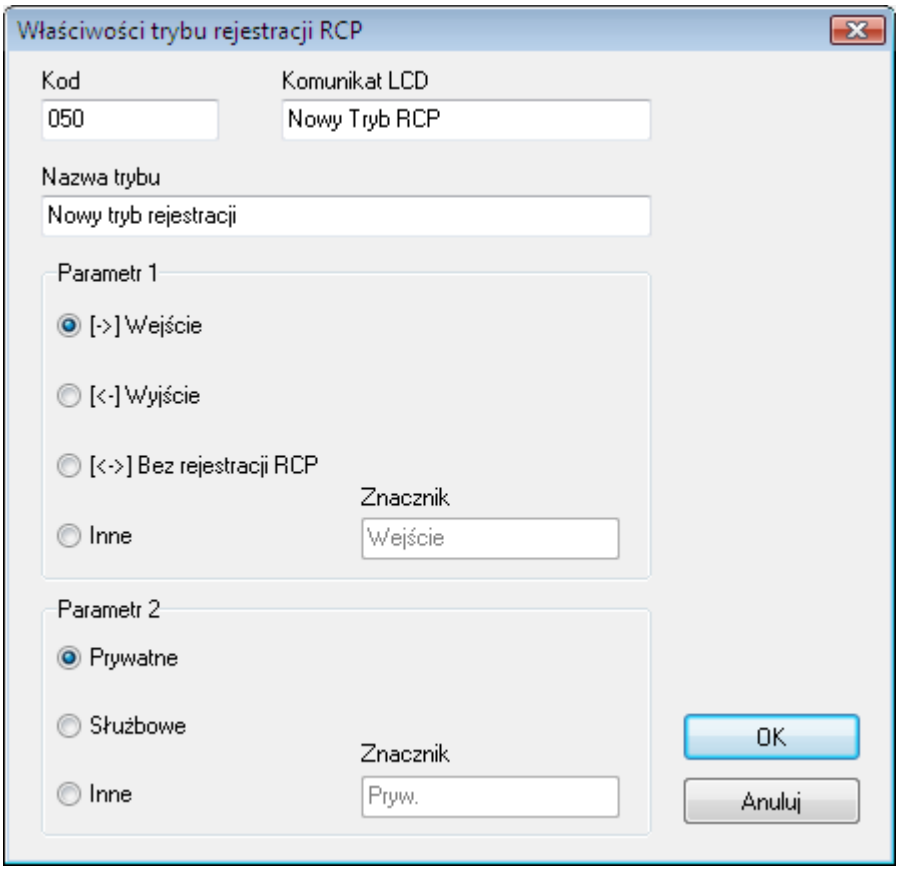


Rysunek 3.123. *Kartoteka trybów RCP*

Za pomocą tej kartoteki można dodać własne tryby rejestracji RCP.

Dodawanie nowego trybu RCP

Aby dodać nowy tryb RCP, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Właściwości trybu rejestracji RCP** (rysunek 3.124).



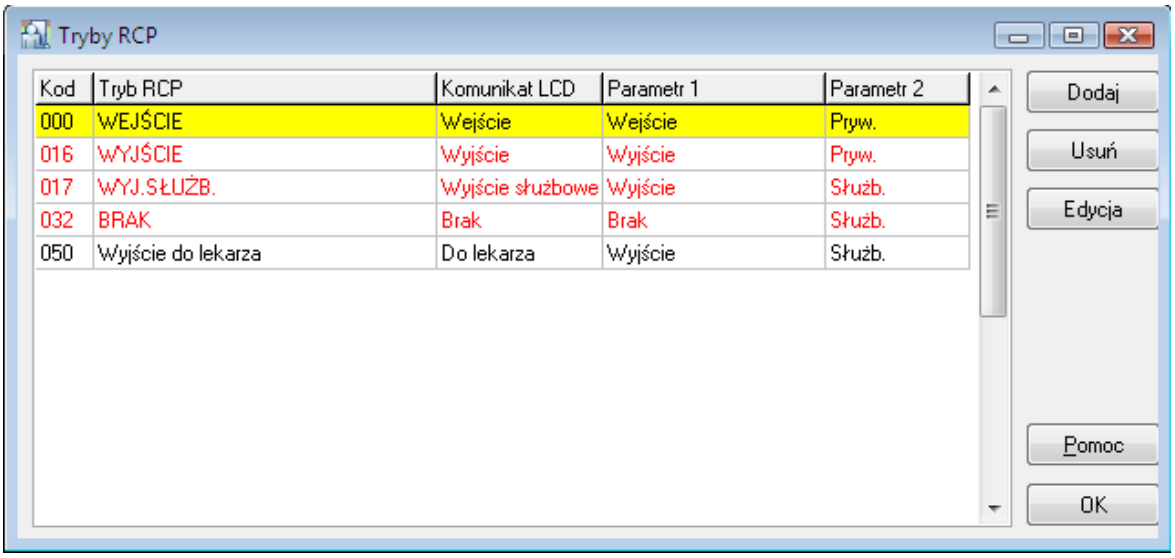
Rysunek 3.124. *Dodawanie nowego trybu rejestracji RCP*

W tym oknie należy podać kod trybu i jego nazwę. Można również określić komunikat LCD dla kontrolerów wyposażonych w wyświetlacz LCD. Następnie należy zdefiniować dwa parametry, które decydują o sposobie interpretowania trybu RCP.

Parametr 1. określa, czy dany tryb rejestracji RCP jest wejściem, wyjściem, czy też trybem bez rejestracji RCP. Można również zaznaczyć opcję **Inne** i określić własny znacznik trybu rejestracji.

Parametr 2 określa, czy dane zdarzenie RCP ma charakter prywatny, służbowy czy inny (określony przez indywidualnie nadany znacznik).

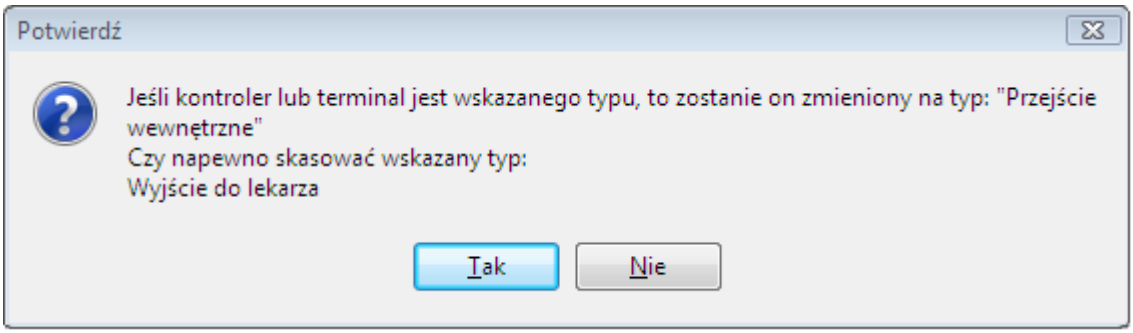
Po zdefiniowaniu wszystkich właściwości trybu rejestracji, należy kliknąć **OK**. Nowy tryb pojawi się w oknie kartoteki trybów RCP (rysunek 3.125). Należy zwrócić uwagę, że tryby RCP zdefiniowane przez użytkownika wyświetlają się w kolorze czarnym, w odróżnieniu od trybów predefiniowanych wyświetlanych na czerwono.



Rysunek 3.125. *Tryb RCP o kodzie 050 został dodany przez użytkownika*

Usuwanie trybu RCP

Tryby RCP, które zostały zdefiniowane przez użytkownika mogą być usunięte. Do tego celu służy przycisk **Usuń** w oknie kartoteki trybów RCP. Jego kliknięcie spowoduje wyświetlenie następującego ostrzeżenia (rysunek 3.126).

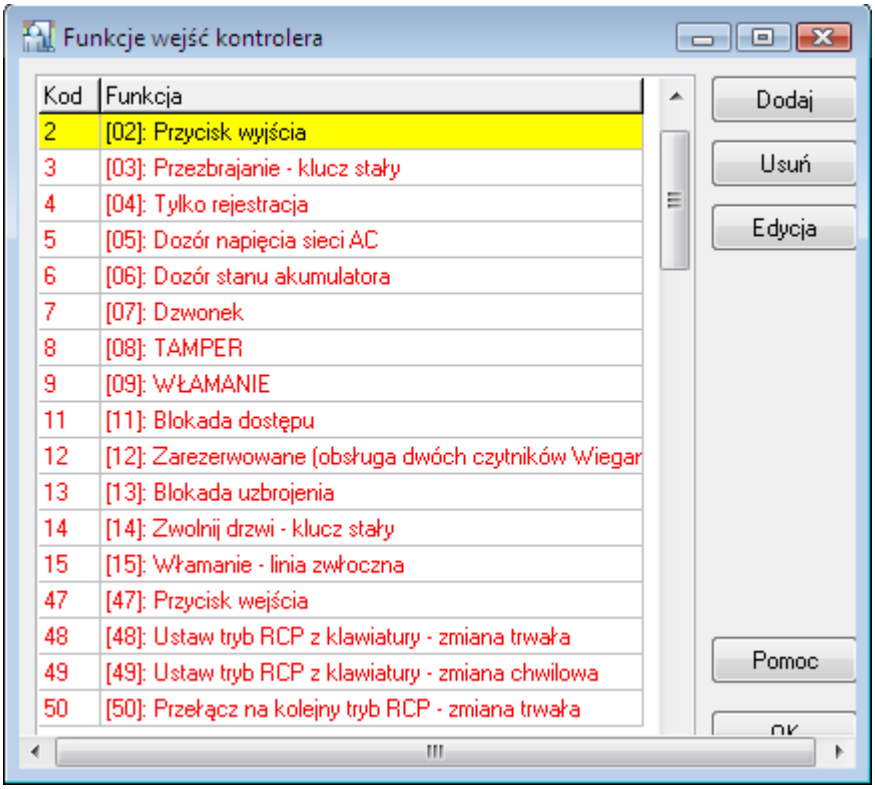


Rysunek 3.126. *Usuwanie trybu RCP zdefiniowanego przez użytkownika*

W przypadku twierdzącej odpowiedzi na to pytanie, tryb RCP zdefiniowany przez użytkownika zostanie usunięty z systemu, natomiast terminale lub kontrolery, które wcześniej rejestrowały ten tryb RCP, odtąd będą rejestrowały w trybie **Przejście wewnętrzne**.

3.5.6. Polecenie Typy linii wejściowych

Polecenie **Typy linii wejściowych** otwiera kartotekę typów linii wejściowych w systemie RACS 4 (rysunek 3.127).

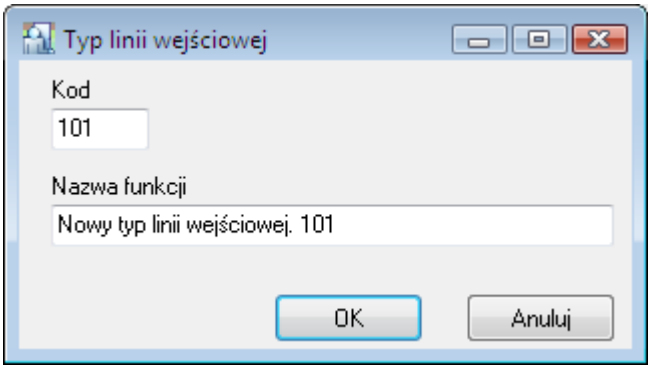


Rysunek 3.127. *Kartoteka typów linii wejściowych w systemie RACS 4*

Za pomocą tej kartoteki można dodać własne typy linii wejściowych. Należy jednak pamiętać, że typy linii wejściowych o kodach z zakresu od 00–100 są predefiniowane i nie można ich usuwać, ani modyfikować. Nowe typy linii wejściowych mogą być wykorzystane w przypadku, gdy kontroler ma informować o stanie innych urządzeń (np. czujnika gazu).

Dodawanie nowego typu linii wejściowej

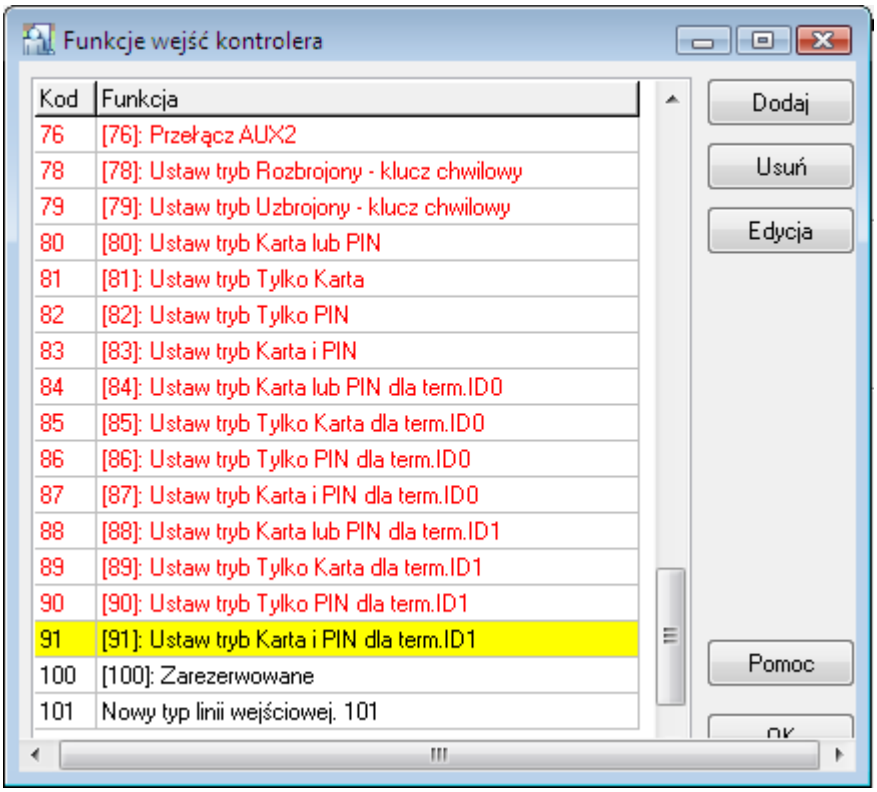
Aby dodać nowy typ linii wejściowej, należy kliknąć przycisk **Dodaj**. Wyświetli się okno dialogowe **Typ linii wejściowej** (rysunek 3.128).



Rysunek 3.128. *Dodawanie nowego typu linii wejściowej*

W tym oknie należy podać kod typu linii wejściowej i jego nazwę a następnie potwierdzić je przyciskiem **OK**. Nowy typ linii wejściowej pojawi się w oknie kartoteki typów linii wejściowej

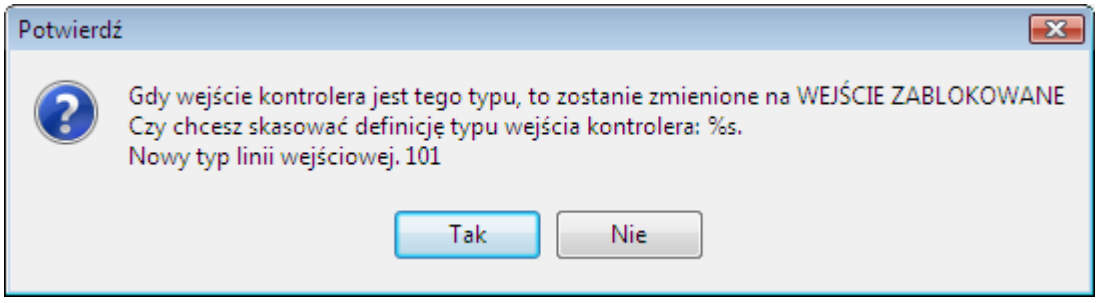
(rysunek 3.129). Należy zwrócić uwagę, że typy linii wejściowych zdefiniowane przez użytkownika wyświetlają się w kolorze czarnym, w odróżnieniu od typów predefiniowanych wyświetlanych na czerwono.



Rysunek 3.129. *Typ linii wejściowej o kodzie 101 został dodany przez użytkownika*

Usuwanie typu linii wejściowej

Typy linii wejściowych, które zostały zdefiniowane przez użytkownika mogą być usunięte. Do tego celu służy przycisk **Usuń** w oknie kartoteki funkcji wejść kontrolerów. Jego kliknięcie spowoduje wyświetlenie następującego ostrzeżenia (rysunek 3.130).

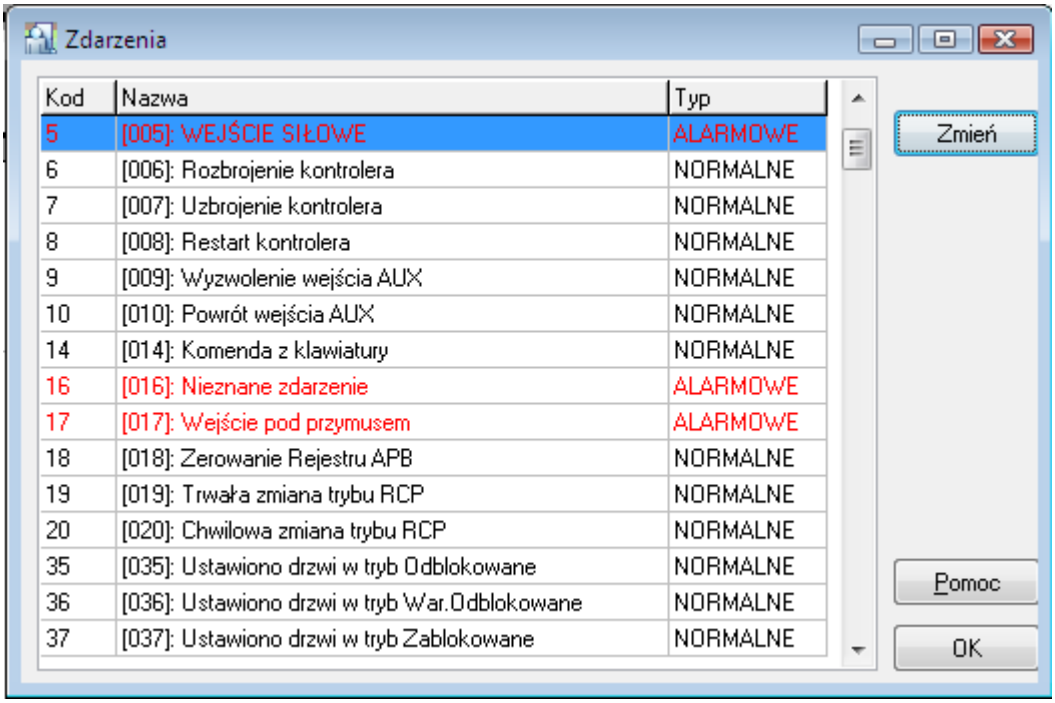


Rysunek 3.130. *Usuwanie typu linii wejściowej zdefiniowanego przez użytkownika*

W przypadku twierdzącej odpowiedzi na to pytanie, typ linii wejściowej zdefiniowany przez użytkownika zostanie usunięty z systemu, natomiast wejścia kontrolera, które wcześniej były tego typu, będą zamienione na typ **WEJŚCIE ZABLOKOWANE**.

3.5.7. Polecenie Typy zdarzeń

Polecenie **Typy zdarzeń** wyświetla listę typów zdarzeń rejestrowanych w systemie RACS 4 (rysunek 3.131).



Rysunek 3.131. *Lista typów zdarzeń w systemie RACS 4*

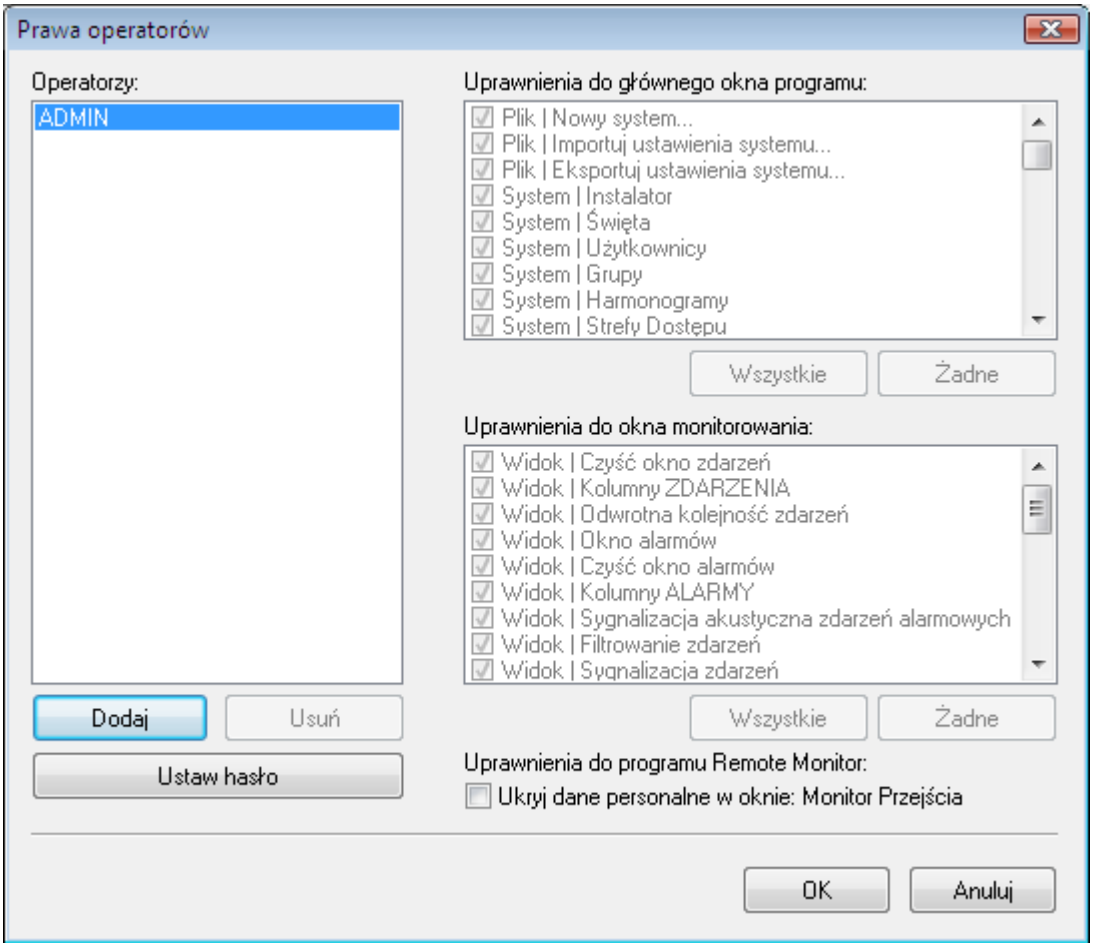
W tym oknie znajduje sie lista wszystkich zdarzeń, które są rejestrowane przez system. Narzędzie pozwala na określenie, które zdarzenia mają być interpretowane jako alarmowe. Aby zmienić typ z normalnego na alarmowy i przeciwnie, wystarczy kliknąć przycisk **Zmień**.

Zdarzenie alarmowe w trybie monitorowania jest zobrazowane dodatkowo w oknie **Alarmy** i powoduje pulsowanie na czerwono paska **Alarmy**.

3.5.8. Polecenie Operatorzy programu

Domyślnie w programie PR Master występuje użytkownik ADMIN, który ma prawo do uruchamiania wszystkich poleceń w systemie. W przypadku, gdy system jest rozbudowany, a za jego obsługę odpowiada większa grupa osób, korzystanie wyłącznie z konta ADMIN jest niebezpieczne. Może bowiem doprowadzić do sytuacji, w której jakiś użytkownik przypadkowo zmodyfikuje lub usunie ustawienia wprowadzone do systemu przez inną osobę.

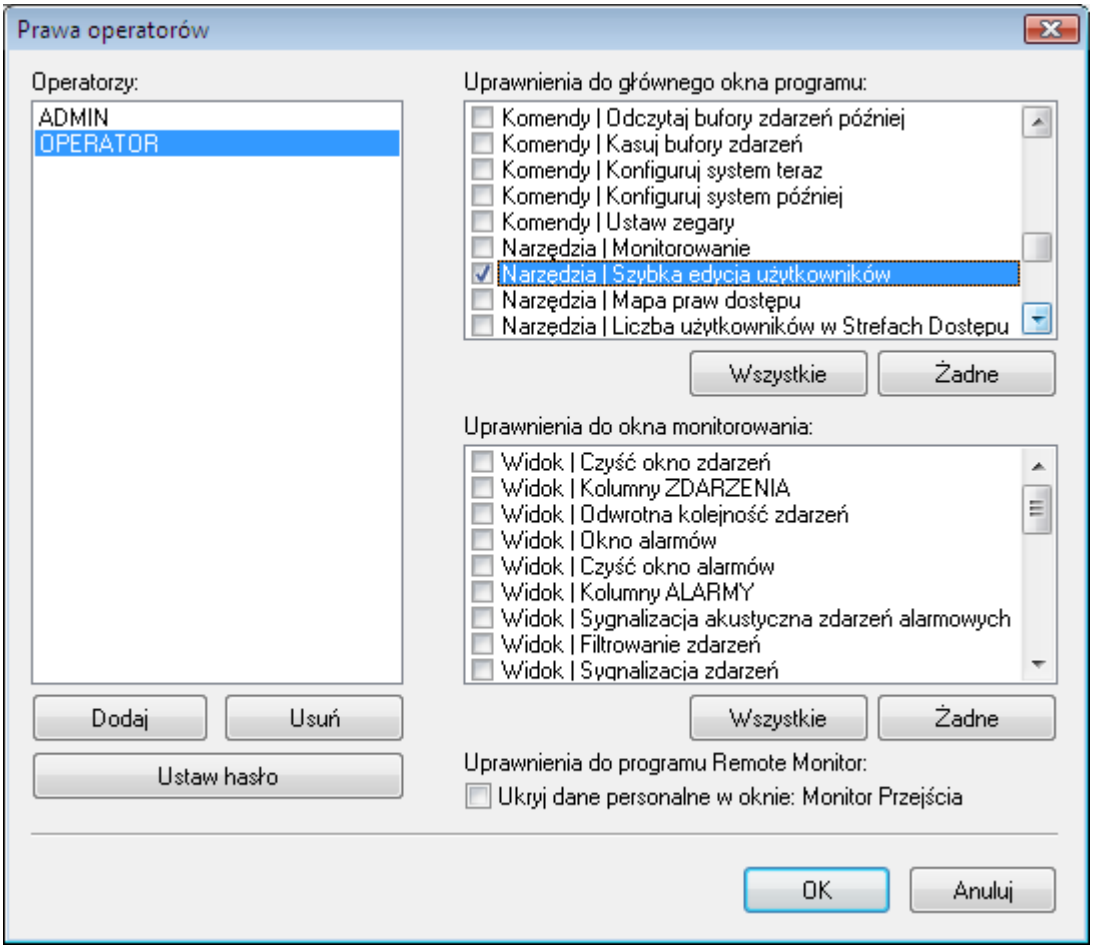
Polecenie **Operatorzy programu** pozwala zdefiniować konta o ograniczonym dostępie do wskazanych funkcji programu. Wybranie polecenia spowoduje wyświetlenie kartoteki operatorów programu (rysunek 3.132).



Rysunek 3.132. *Lista operatorów systemu RACS 4*

Domyślnie na liście operatorów znajduje się tylko użytkownik ADMIN. Ma on uprawnienia do uruchamiania wszystkich poleceń w programie PR Master i nie można mu tych praw odebrać.

Aby zdefiniować nowego operatora, należy kliknąć przycisk **Dodaj**. Spowoduje to wyświetlenie okna dialogowego **Nowy operator**, w którym należy podać login nowego operatora i zdefiniować dla niego hasło. Po wykonaniu tej czynności, nowy operator pojawi się na liście. Początkowo, nie ma on żadnych uprawnień w systemie — w obszarach **Uprawnienia do głównego okna programu**, **Uprawnienia do okna monitorowania** i **Uprawnienia do programu Remote Monitor** wszystkie pola wyboru są niezaznaczone. Aby dodać prawo wskazanego operatora do wybranego polecenia, należy zaznaczyć pole wyboru obok nazwy odpowiedniej opcji. Załóżmy, że chcemy aby nowo zdefiniowany operator miał prawo wyłącznie do dopisywania nowych użytkowników. W takim przypadku zaznaczamy pole wyboru **Narzędzia | Szybka edycja użytkowników** (rysunek 3.133).



Rysunek 3.133. *Użytkownik OPERATOR ma prawo wyłącznie do szybkiej edycji użytkowników*

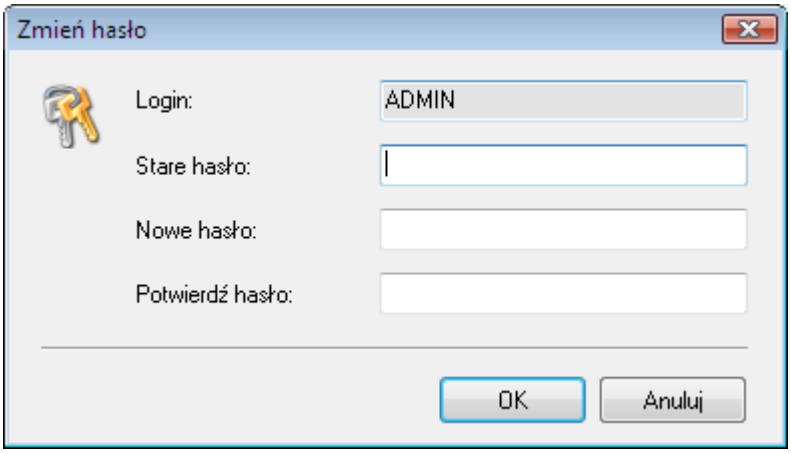
Przycisk **Wszystkie** znajdujący się pod grupą określonych opcji powoduje zaznaczenie wszystkich opcji w grupie. Przycisk **Żadne** powoduje wyczyszczenie wszystkich opcji z grupy.

Przycisk **Usuń** pod listą operatorów usuwa operatora z systemu. Oczywiście, użytkownika ADMIN nie można usunąć.

Przycisk **Ustaw hasło** pozwala na zmianę hasła wskazanego operatora (w tym także operatora ADMIN)

3.5.9. Polecenie Zmień hasło

Polecenie **Zmień hasło** pozwala na zmianę hasła użytkownika, który jest aktualnie zalogowany. Jego wybranie powoduje wyświetlenie okna dialogowego **Zmień hasło** (rysunek 3.134).



Rysunek 3.134. *Użytkownik OPERATOR ma prawo wyłącznie do szybkiej edycji użytkowników*

W polu **Stare hasło** należy podać obowiązujące hasło do konta. W polach **Nowe hasło** i **Potwierdź hasło** należy podać nowe hasło, po czym zatwierdzić je przyciskiem **OK**.

3.5.10. Polecenie Zablokuj program

Polecenie **Zablokuj program** służy do zablokowania dostępu do poleceń programu w przypadku, gdy operator jest zmuszony odejść od komputera. Użycie tej opcji spowoduje zminimalizowanie okna programu. Odblokowanie poleceń jest możliwe po podaniu obowiązującego hasła.

3.5.11. Polecenie Opcje

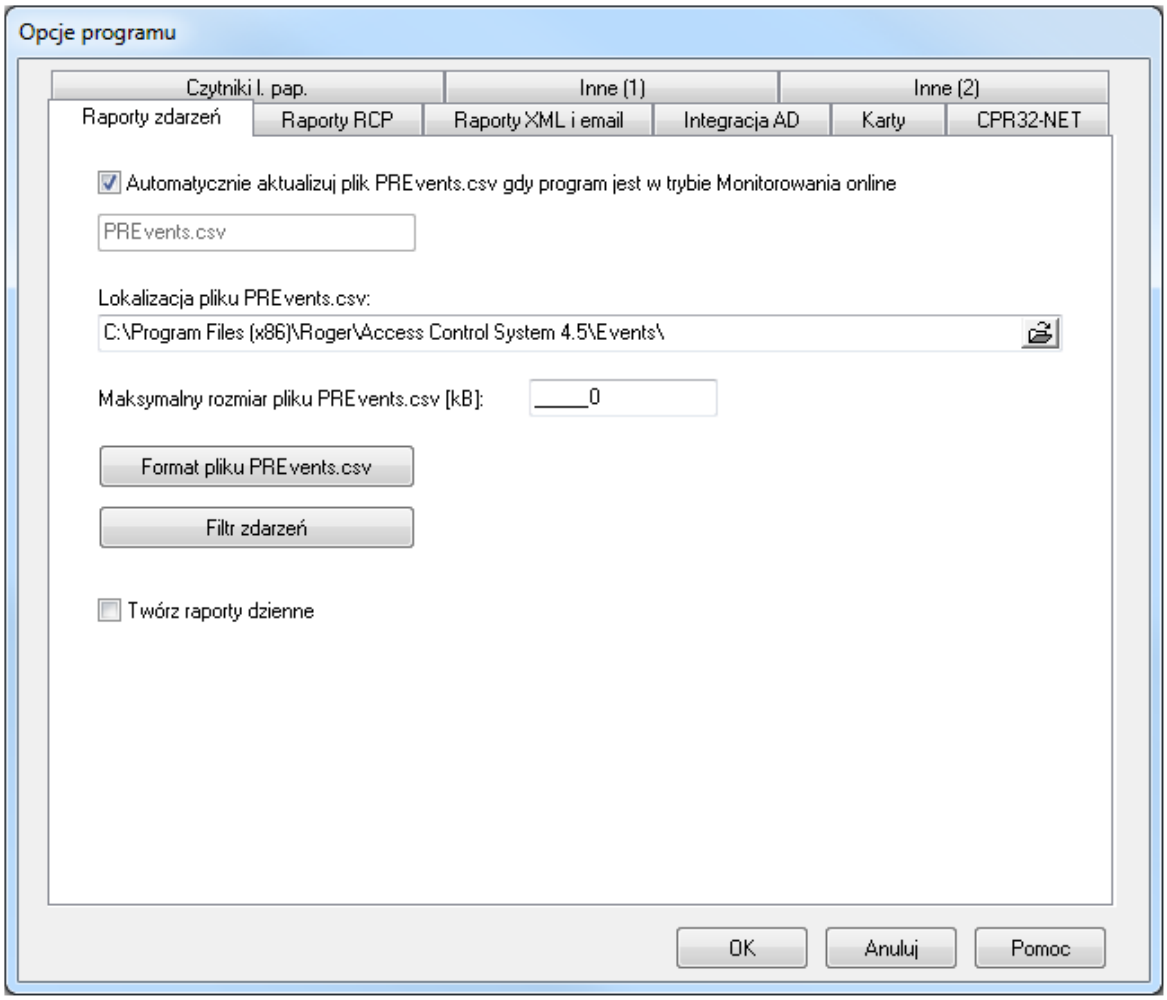
Polecenie **Opcje** otwiera okno opcji programu. Okno jest podzielone na następujące zakładki:

- Raporty zdarzeń
- Raporty RCP
- Raporty XML i email
- Inne (1) i Inne (2)
- Karty
- CPR32-NET
- Czytniki l. pap.
- Integracja AD

Opcje należące do tych grup opisano w poniższych punktach.

3.5.11.1. Raporty zdarzeń

Zakładka **Raporty zdarzeń** służy do ustawiania opcji generowania pliku **PREvents.csv**. Pokazano ją na rysunku 3.135.

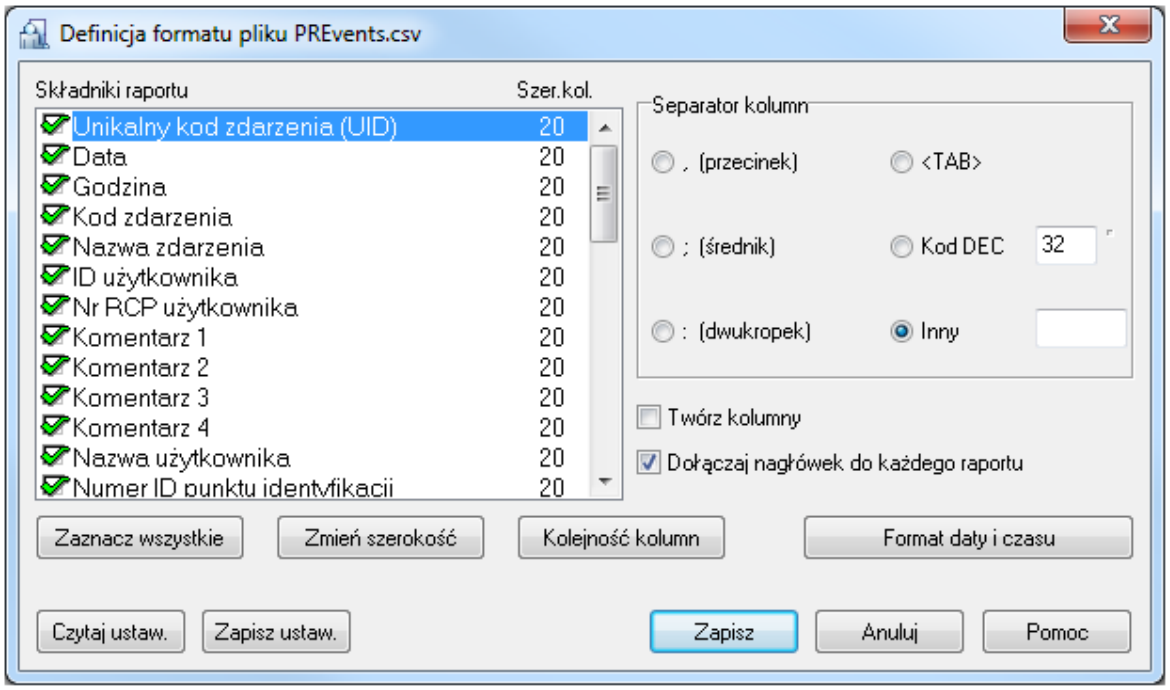


Rysunek 3.135. *Opcje generowania raportu zdarzeń*

Wszystkie kontrolki znajdujące się w zakładce są aktywne dopiero wtedy, gdy jest zaznaczone pole wyboru **Automatycznie aktualizuj plik PREvents.csv gdy program jest w trybie Monitorowania online**.

Pole **Lokalizacja pliku PREvents.csv** umożliwia wskazanie katalogu, w którym będzie zapisany plik **PREvents.csv**. Pole **Maksymalny rozmiar pliku PREvents.csv** służy do określenia maksymalnego rozmiaru pliku z raportem. Domyślnie maksymalny rozmiar tego pliku wynosi 1000 kB.

Przycisk **Format pliku PREvents.csv** umożliwia zdefiniowanie dokładnej zawartości raportu zdarzeń. Jego kliknięcie spowoduje wyświetlenie okna dialogowego **Definicja formatu pliku PREvents.csv** (rysunek 3.136).



Rysunek 3.136. *Definiowanie formatu pliku PREvents.csv*

Za pomocą tego okna dialogowego można dokładnie skonfigurować zawartość pliku **PREvents.csv**. Użytkownik może zaznaczyć kolumny, które mają pojawić się w raporcie, określić ich szerokość, zmienić kolejność kolumn oraz ustalić format daty i czasu.

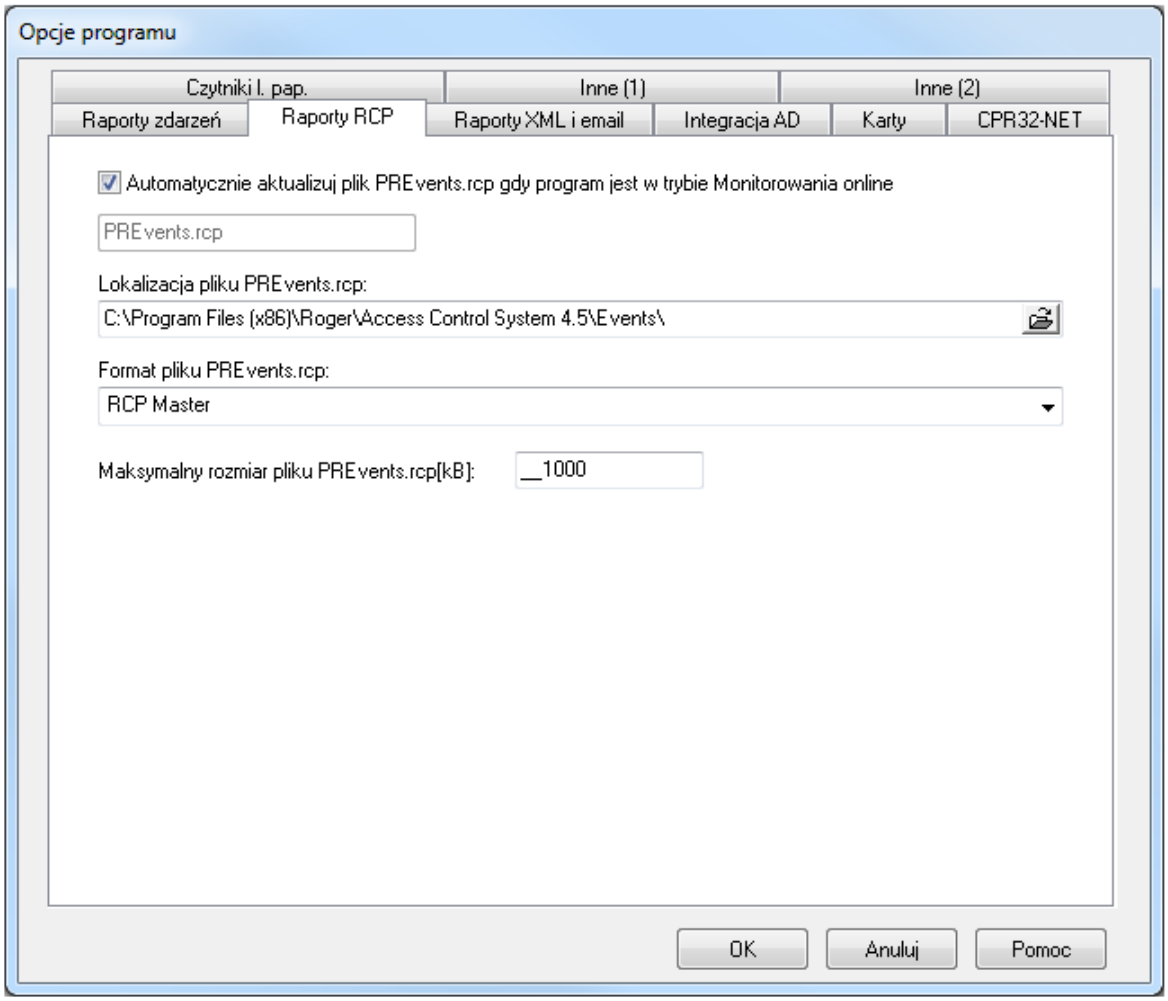
Ustawienia formatu pliku **PREvents.csv** można zapisać do pliku (przycisk **Zapisz ustaw.**), a później je z niego zaimportować (przycisk **Czytaj ustaw.**).

Przycisk **Filtr zdarzeń** spowoduje wyświetlenie okna **Filtr zdarzeń**. Dzięki niemu można na przykład, kierować do pliku PREvents.csv wyłącznie zdarzenia **Odmowa dostępu** dotyczące wskazanego użytkownika.

Więcej informacji na temat sposobu definiowania filtrów można znaleźć w **punkcie 3.3.7.1**.

3.5.11.2. Raporty RCP

Zakładka **Raporty RCP** służy do ustawiania opcji generowania pliku **PREvents.rcp**. Pokazano ją na rysunku 3.137.



Rysunek 3.137. *Opcje generowania raportu RCP*

Wszystkie kontrolki znajdujące się w zakładce są aktywne dopiero wtedy, gdy jest zaznaczone pole wyboru **Automatycznie aktualizuj plik PREvents.rcp gdy program jest w trybie Monitorowania online**.

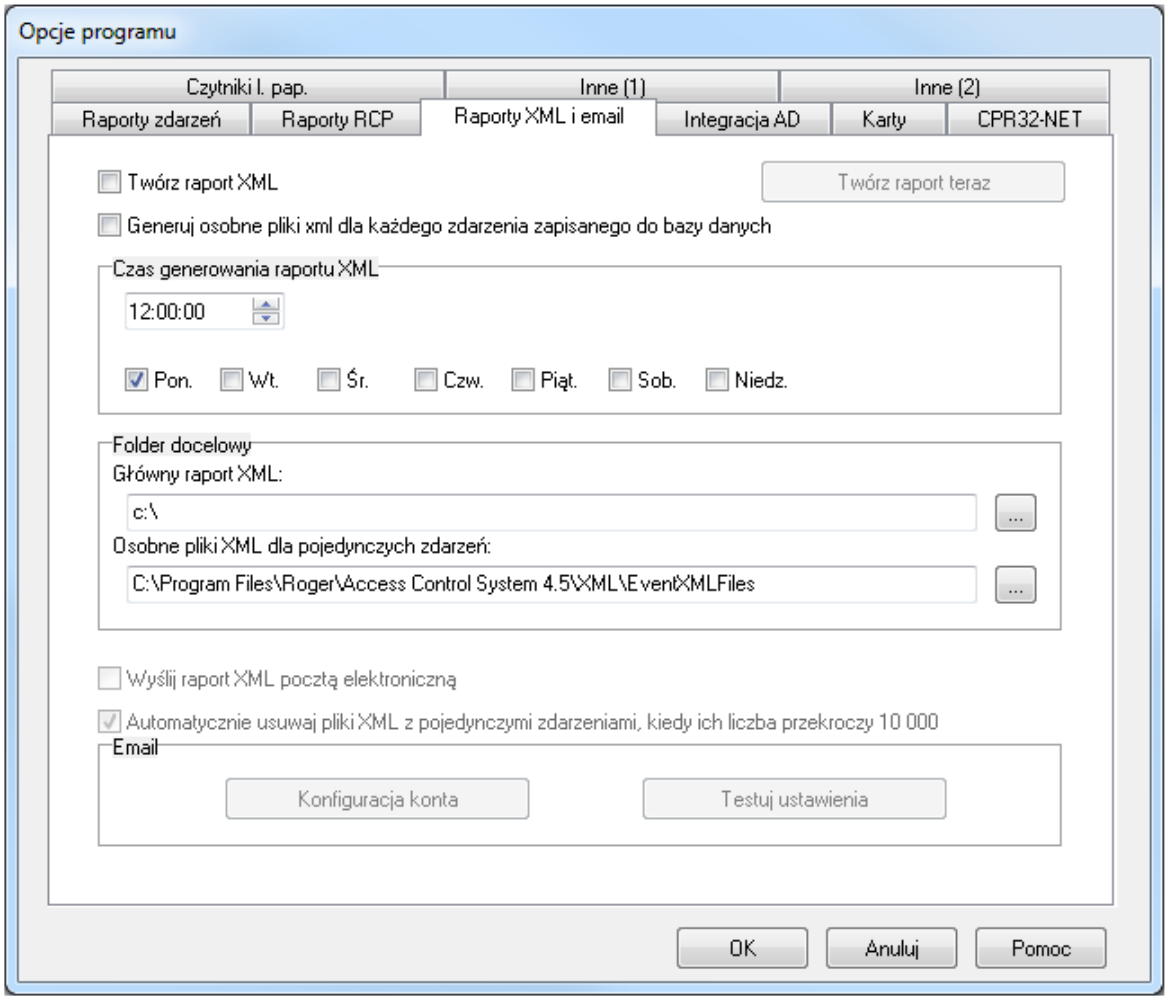
Pole **Lokalizacja pliku PREvents.rcp** umożliwia wskazanie katalogu, w którym będzie zapisany plik **PREvents.rcp**.

Pole **Format pliku PREvents.rcp** umożliwia wybór jednego z dostępnych formatów pliku z raportem RCP. Dostępne są następujące formaty:

- RCP Master
- Gratyfikant (f-my Insert)
- Agrobex
- Symfonia RCP
- SDF Singapore
- CIS Singapore
- Sykom
- RCP Access Pro (f-my Polman).
- Optima

3.5.11.3. Raporty XML i email

Zakładka **Raporty XML i email** służy do ustawiania opcji generowania raportów XML. Pozwala również wprowadzić ustawienia przesyłania raportów pocztą elektroniczną. Pokazano ją na rysunku 3.138.

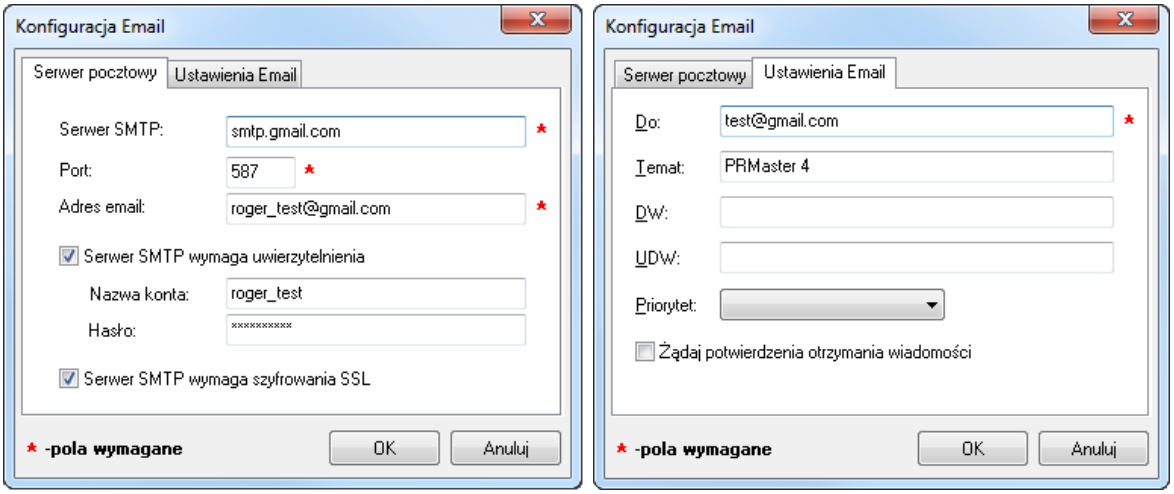


Rysunek 3.138. *Opcje generowania raportu RCP*

Kontrolki znajdujące się w obszarach **Czas generowania raportu XML** oraz **Folder docelowy** są aktywne dopiero po zaznaczeniu pola wyboru **Twórz raport XML**. Natomiast kontrolki znajdujące się w obszarze **Email** są aktywne po zaznaczeniu pola wyboru **Wyślij raport XML pocztą elektroniczną**.

W obszarze **Czas generowania raportu XML** należy określić godzinę generowania raportu XML oraz określić dni tygodnia, w których ma być generowany raport XML. Przycisk **Twórz raport teraz** powoduje natychmiastowe utworzenie raportu. Zostanie on zapisany w lokalizacji wskazanej w polu **Folder docelowy**, w pliku, którego nazwa składa się z daty i godziny generowania.

Jeśli zaznaczy się pole wyboru **Wyślij raport XML pocztą elektroniczną**, można zdefiniować konto pocztowe, na które będzie przesłany raport e-mail. W tym celu, należy kliknąć przycisk **Konfiguracja konta**. Spowoduje to wyświetlenie okna dialogowego **Konfiguracja Email** (rysunek 3.139).

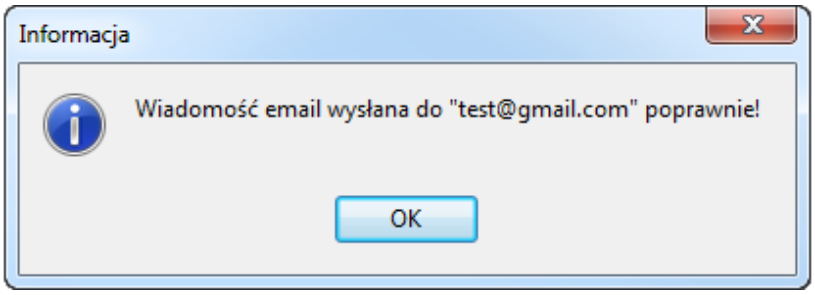


Rysunek 3.139. *Konfiguracja konta pocztowego do wysyłania raportów XML*

Okno **Konfiguracja Email** składa się z dwóch zakładek: **Serwer pocztowy** i **Ustawienia Email**. Przykładowe wypełnieni pól w tych zakładkach pokazano na rysunku 3.139. Należy pamiętać o podaniu poprawnego adresu e-mail osoby, do której przesyłamy raport (pole **Do:** w zakładce **Ustawienia Email**) oraz właściwym ustawieniu opcji serwera poczty wychodzącej.

Jeśli serwer poczty wychodzącej wymaga uwierzytelniania oraz szyfrowania SSL to należy zaznaczyć odpowiednie opcje i podać nazwę konta oraz hasło.

Po skonfigurowaniu konta e-mail, można skorzystać z przycisku **Testuj ustawienia**. Jeśli wszystkie ustawienia są prawidłowe, program poinformuje, że wiadomość wysłano poprawnie (rysunek 3.140).



Rysunek 3.140. *Konfiguracja konta pocztowego zakończona sukcesem*

Zaznaczenie opcji **Generuj osobne pliki xml dla każdego zdarzenia zapisanego do bazy danych** powoduje, że w podkatalogu **EventXMLFiles** folderu z raportami XML dla każdego zdarzenia zapisywanego do bazy danych są generowane oddzielne pliki XML o nazwach **ROGxxxxxxxx.xml**, gdzie xxxxxxxx oznacza kolejny numer pliku. Pliki te mają następującą zawartość:

```
<ROG>
        <TIME>2010-07-01 08:42:40</TIME>
        <READER>1010</READER>
        <CARD>1E00EFD0B2</CARD>
        <ACCESS>N</ACCESS>
</ROG>
```

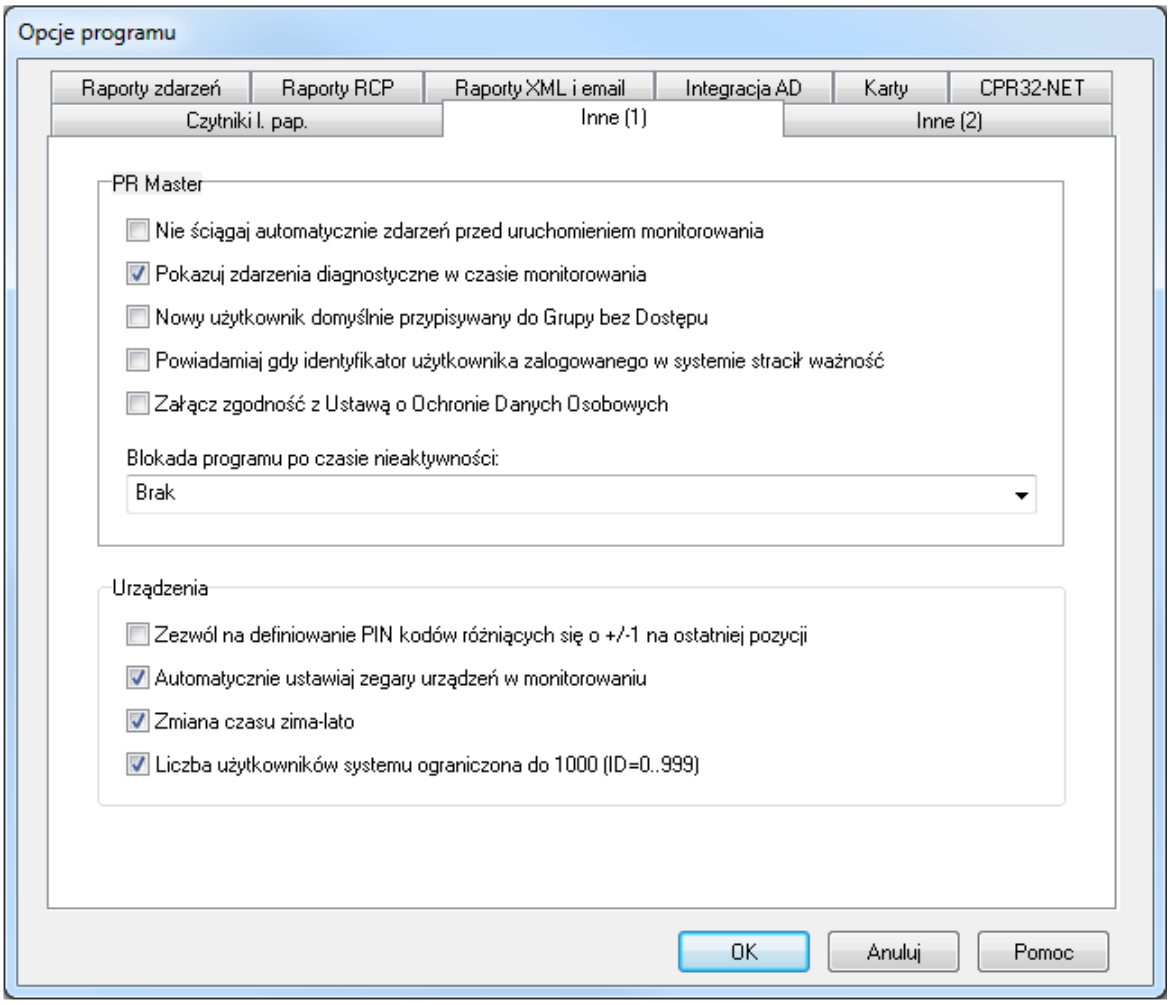
Poszczególne pola mają następujące znaczenie:

- <TIME> — czas wystąpienia zdarzenia,
- <READER> — identyfikator czytnika,
- <CARD> — kod odczytanej karty bądź kod zdarzenia (szesnastkowo),
- <ACCESS> — pole o wartości T lub N informujące o tym, czy kontroler przydzielił dostęp, czy nie.

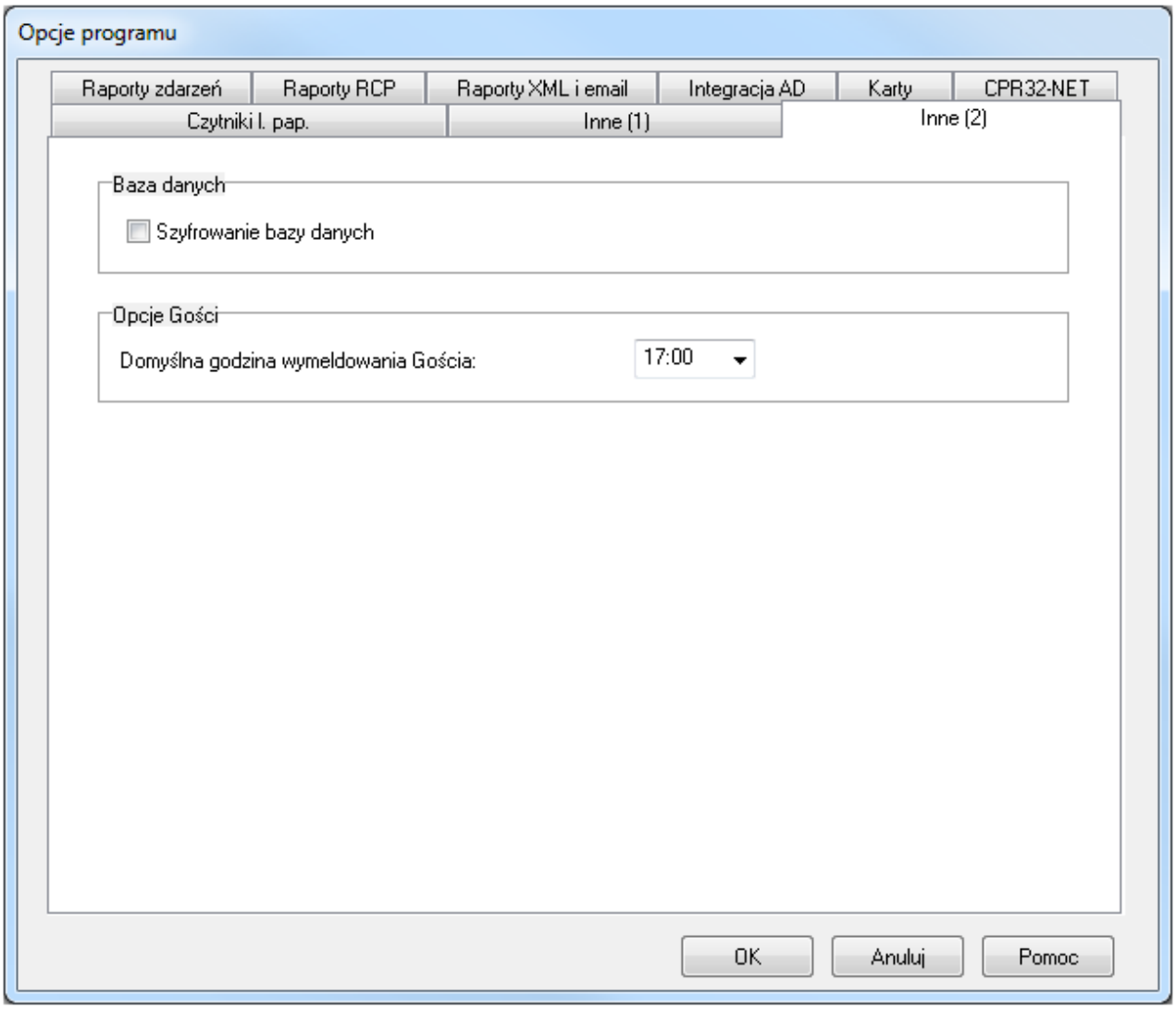
Pliki te mogą być wykorzystane do integracji systemu RACS 4 z innymi systemami.

3.5.11.4. Inne

Dostępne są dwie zakładki **Inne (1)** oraz **Inne (2)** (rysunek 3.141) zawierające różne opcje mające wpływ na sposób działania systemu.



Rysunek 3.141a. *Inne opcje systemowe*



Rysunek 3.141b. *Inne opcje systemowe*

Aby włączyć określoną opcję, należy zaznaczyć pole wyboru znajdujące się obok jej opisu lub wybrać z listy. Większość opcji dostępnych w tych zakładkach nie wymaga komentarza.

Zaznaczenie opcji **Nie ściągaj automatycznie zdarzeń przed uruchomieniem monitorowania** powoduje, że w momencie uruchomienia monitorowania program PR Master nie ściąga automatycznie do bazy danych zdarzeń zarejestrowanych przez urządzenia przez co monitorowanie jest uruchamiane od razu bez opóźnień. Te zdarzenia nie są tracone i nadal można je pobrać np. poleceniem **Odczytaj bufory zdarzeń** – patrz **punkt 3.4.1**. Gdy opcja nie jest zaznaczona to uruchomienie trybu monitorowania powoduje automatyczny odczyt zdarzeń z bufora(ów) systemu i zapisanie ich do bazy danych programu.

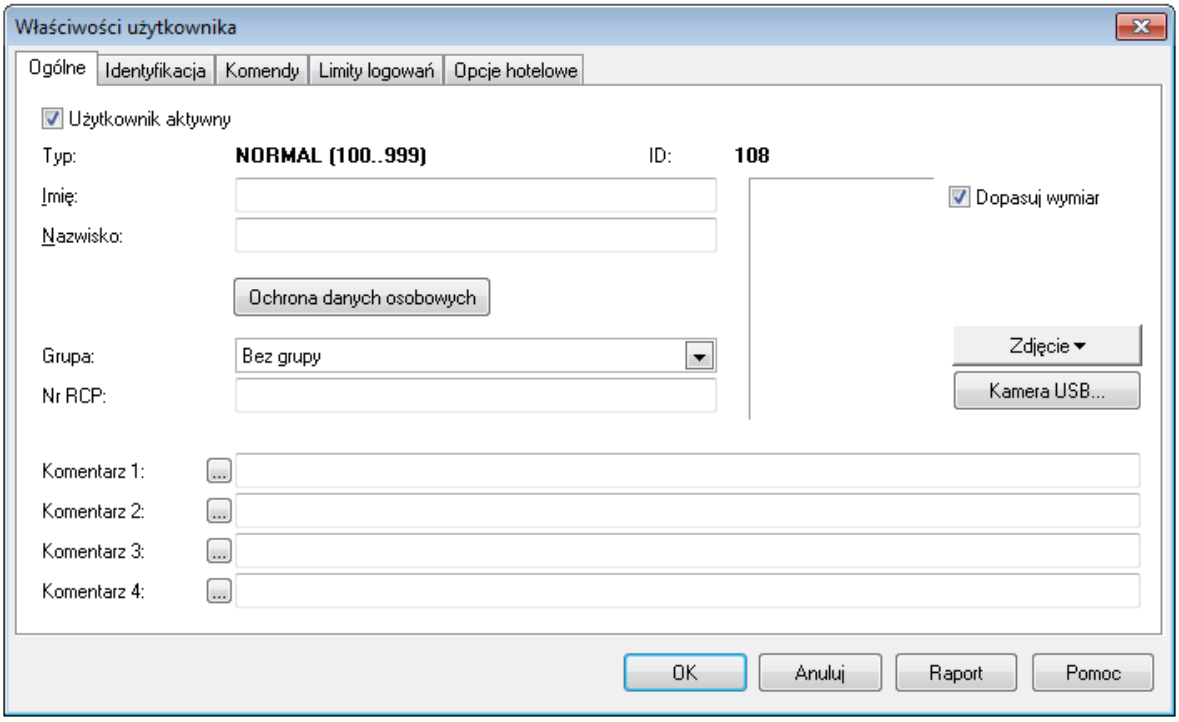
Opcja **Powiadamiaj gdy identyfikator użytkownika zalogowanego w systemie stracił ważność** pozwala na monitorowanie i wykrywanie użytkowników przebywających w obiekcie pod kontrolą systemu KD po upłynięciu terminu ważności ich identyfikatorów. Przedział ważności definiuje się we właściwościach danego użytkownika w zakładce **Identyfikacja**. Wykrycie użytkownika wymaga uruchomienia programu PR Master w trybie monitorowania i dotyczy użytkowników przebywających w wewnętrznych Strefach Dostępu. Daną strefę można oznaczyć jako wewnętrzną lub zewnętrzną w jej właściwościach za pomocą polecenia **Strefy Dostępu** w oknie głównym programu PR Master. W momencie wykrycia użytkownika z przeterminowanym identyfikatorem w strefie wewnętrznej program PR Master w trybie monitorowania wyświetla ostrzeżenie w oknie zawierającym podstawowe informacje na temat takiego użytkownika.

Weryfikacja wszystkich użytkowników jest realizowana automatycznie co godzinę i można ją dodatkowo uruchomić na żądanie za pomocą przycisku **Sprawdź ważn.** w oknie narzędzia **Znajdź użytkownika** (patrz **punkt 4.1.10**).

Opcja **Załącz zgodność z Ustawą o Ochronie Danych Osobowych** umożliwia uzyskanie zgodności programu PR Master z wymogami:

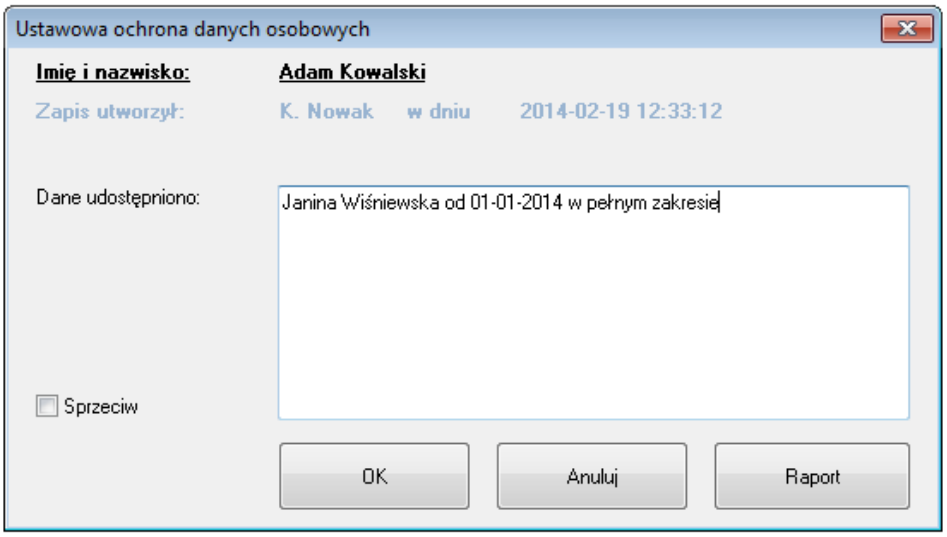
- Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Po załączeniu tej opcji nie jest możliwe jej odznaczenie w ramach danej konfiguracji (bazy danych) jak też nie jest możliwa edycja imion i nazwisk użytkowników dodanych do systemu. Od momentu jej załączenia w oknie dodawania użytkownika zarówno poprzez opcję **Użytkownicy** w oknie głównym programu PR Master jak i za pomocą opcji **Szybka Edycja Użytkownika**, w zakładce **Ogólne** pojawia się przycisk **Ochrona danych osobowych** (rysunek 3.142).



Rysunek 3.142. *Przycisk Ochrona danych osobowych*

Po wybraniu przycisku **Ochrona danych osobowych** wyświetlane jest okno pokazane na rysunku 3.143.



Rysunek 3.143. *Okno ochrony danych osobowych*

Dane osoby wprowadzającej zapis oraz data wprowadzenia zapisu są nieedytowalne i odpowiadają nazwie operatora programu (patrz **punkt 3.5.8**) zalogowanego do programu PR Master w momencie dodania/zaimportowania użytkownika do systemu. W oknie ochrony danych osobowych możliwe jest również generowanie raportu dla użytkownika za pomocą przycisku **Raport** a następnie jego wydrukowanie lub zapisanie w formacie *.rtf oraz *.csv.

Opcja **Blokada programu po czasie nieaktywności** umożliwia zdefiniowanie czasu nieaktywności w programie PR Master po którym nastąpi jego zablokowanie. Odblokowanie wymaga podania hasła bieżącego operatora programu. Czas do zablokowania jest odliczany i wyświetlany w belce dolnej głównego okna programu PR Master.

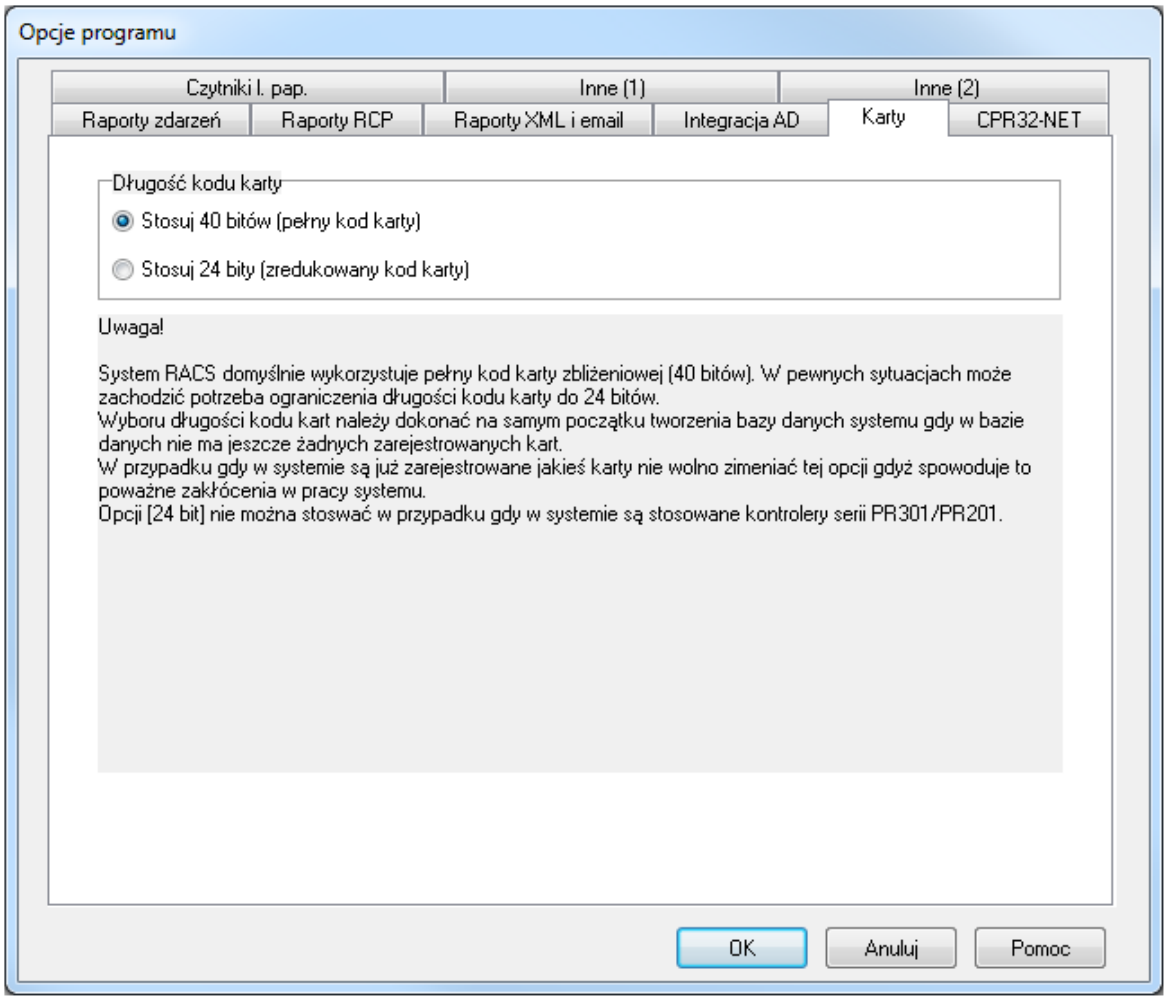
Opcja **Zezwól na definiowanie PIN kodów różniących się o +/-1 na ostatniej pozycji**. Jest związana z sygnalizacją wejścia pod przymusem (DURESS). Jeżeli użytkownik wprowadzi kod zwiększony lub zmniejszony o jeden na ostatniej pozycji to kontroler może to zinterpretować jako wprowadzenie kodu pod przymusem. Wprowadzenie kodu pod przymusem, oprócz normalnej reakcji kontrolera (otwarcie drzwi, przełączenie pomiędzy stanem UZBR./ROZB.) powoduje dodatkowo zarejestrowanie zdarzenia **Wejście pod przymusem** oraz może wywoływać sygnalizację na wyjściu alarmowym kontrolera. Na przykład, jeśli kod użytkownika ma postać [6789][#], to wprowadzenie kodu [6788][#] lub [6780[#] traktowane jest przez kontroler jako użycie kodu pod przymusem. Z tego powodu, gdy opcja nie jest zaznaczona, program PR Master nie dopuszcza do definiowania kodów PIN różniących się na ostatniej pozycji o 1. W przypadku gdy stosowanie kodów DURESS w systemie KD nie jest celowe, należy zaznaczyć opcję **Zezwól na definiowanie PIN kodów różniących się o +/-1 na ostatniej pozycji**. Po jej zaznaczeniu program PR Master będzie dopuszczał definiowanie kodów PIN dowolnej postaci.

Opcja **Liczba użytkowników systemu ograniczona do 1000 (ID=0..999)** jest stosowana gdy liczba użytkowników systemu jest poniżej 1000. Gdy opcja jest załączona to przesyłanie konfiguracji do urządzeń systemu jest szybsze.

Opcja **Domyślna godzina wymeldowania Gościa** pozwala ustawić domyślną wartość dla pola **Do** podczas dodawania Gości za pomocą opcji **Goście** w oknie głównym programu PR Master (patrz **punkt 3.2.4**).

3.5.11.5. Karty

Zakładka **Karty** w oknie **Opcje programu** pozwala na dokonanie wyboru pomiędzy stosowaniem kodu karty o długości 40 bitów, a 24 bitów. Zakładkę zaprezentowano na rysunku 3.144.

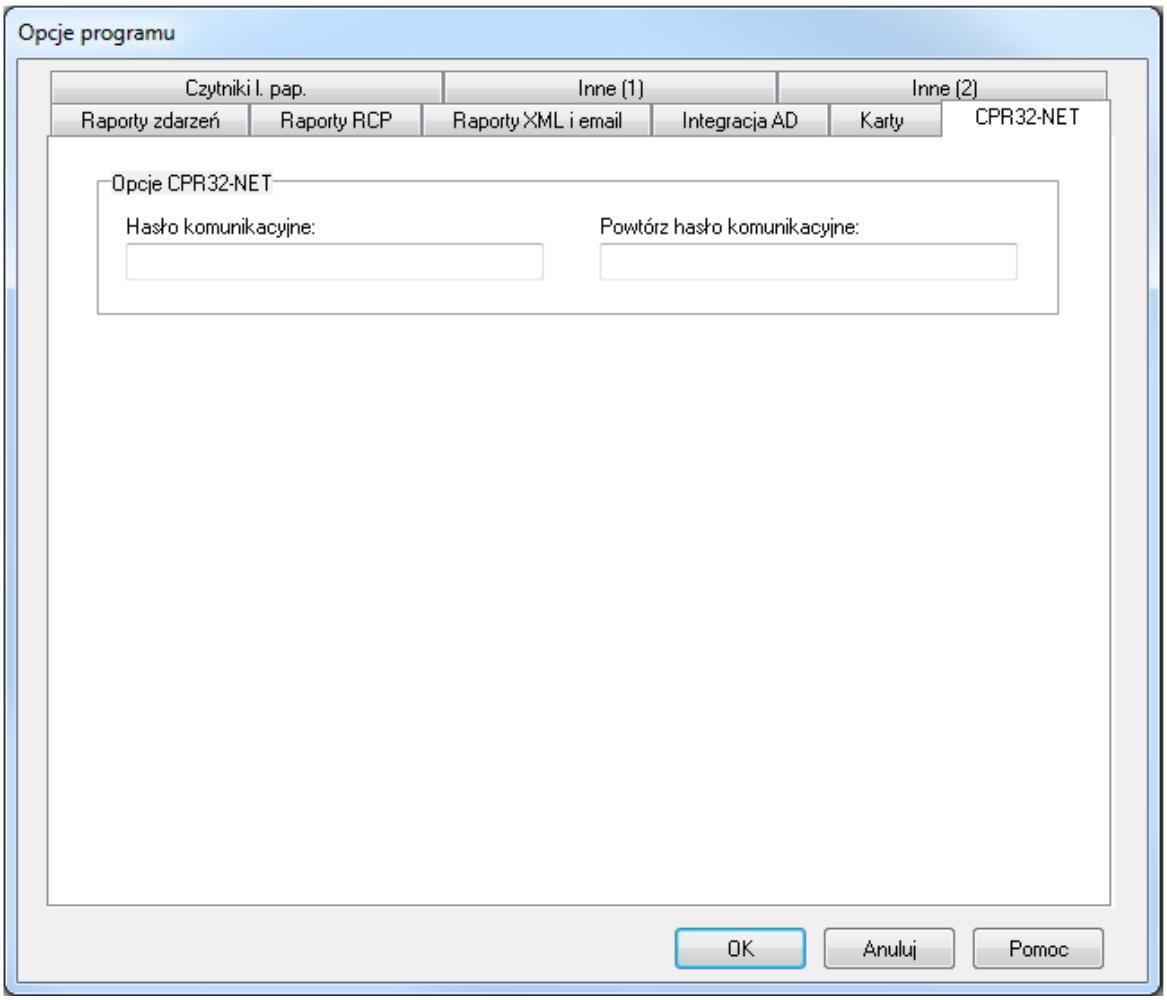


Rysunek 3.144. *Opcje rozmiaru kodu karty*

Należy pamiętać, aby opcję długości rozmiaru karty wybrać na początku tworzenia bazy danych, jeszcze przed zarejestrowaniem jakiejkolwiek karty. Zmiana opcji w późniejszym czasie może spowodować zakłócenia pracy systemu.

3.5.11.6 CPR32-NET

Zakładka **CPR32-NET** (rysunek 3.145) umożliwia przede wszystkim wprowadzenie hasła do komunikacji szyfrowanej z centralą po stronie programu PR Master. Więcej informacji na temat komunikacji szyfrowanej podano w instrukcji obsługi centrali CPR32-NET, dostępnej na stronie **www.roger.pl**.

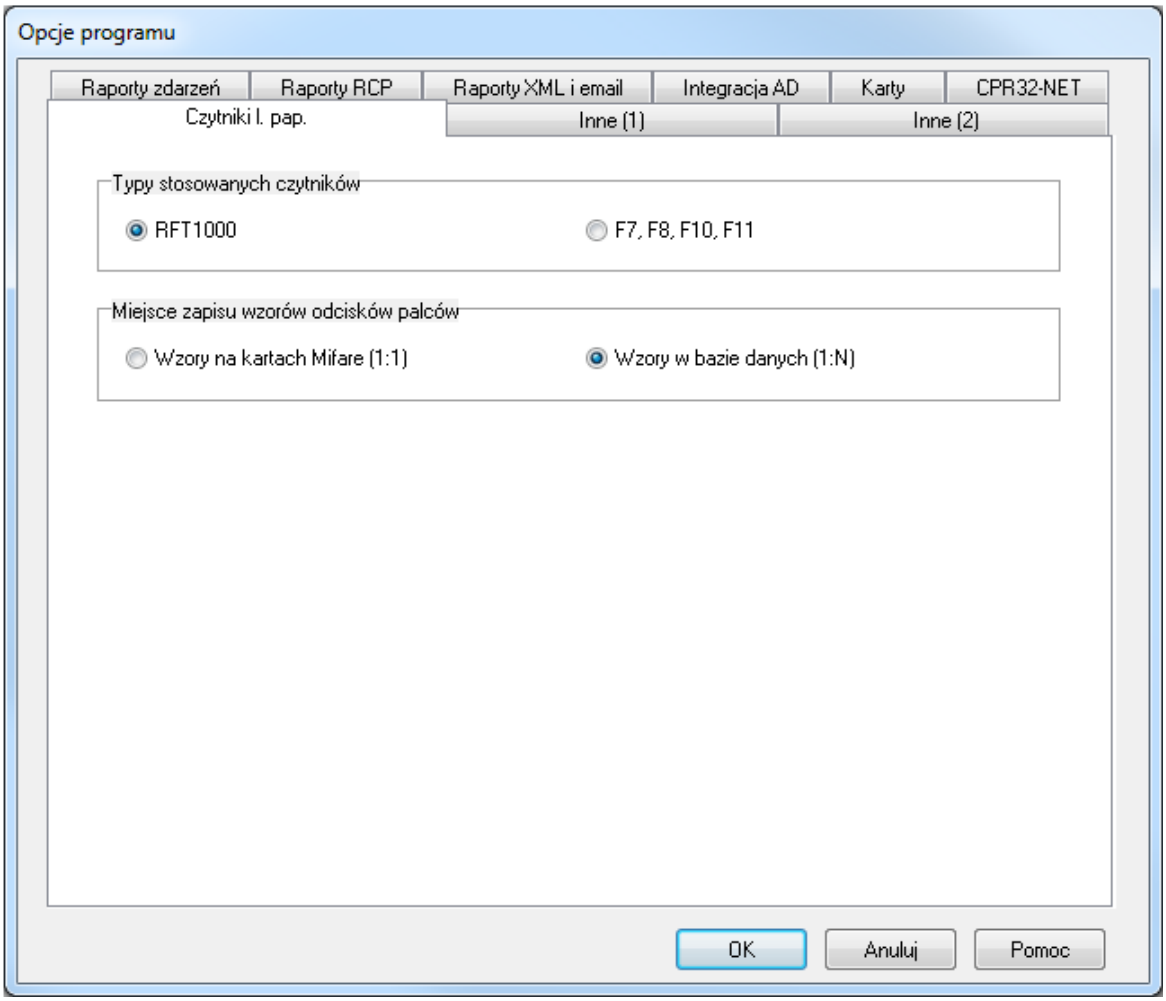


Rysunek 3.145. *Opcje centrali CPR32-NET*

3.5.11.7 Czytniki l.pap.

Zakłada **Czytniki l.pap.** umożliwia wybór obsługiwanych czytników linii papilarnych tj. nowszych RFT1000 lub starszych nie oferowanych już w sprzedaży czytników F7, F8, F9, F11. Dodatkowo w przypadku czytników RFT1000 możliwe jest wskazanie trybu rozpoznania. Więcej informacji na temat czytnika RFT1000 podano w jego instrukcji obsługi dostępnej na stronie **www.roger.pl**.

Zakładkę zaprezentowano na rysunku 3.146.



Rysunek 3.146. *Opcje czytników linii papilarnych*

3.5.11.8 Integracja AD

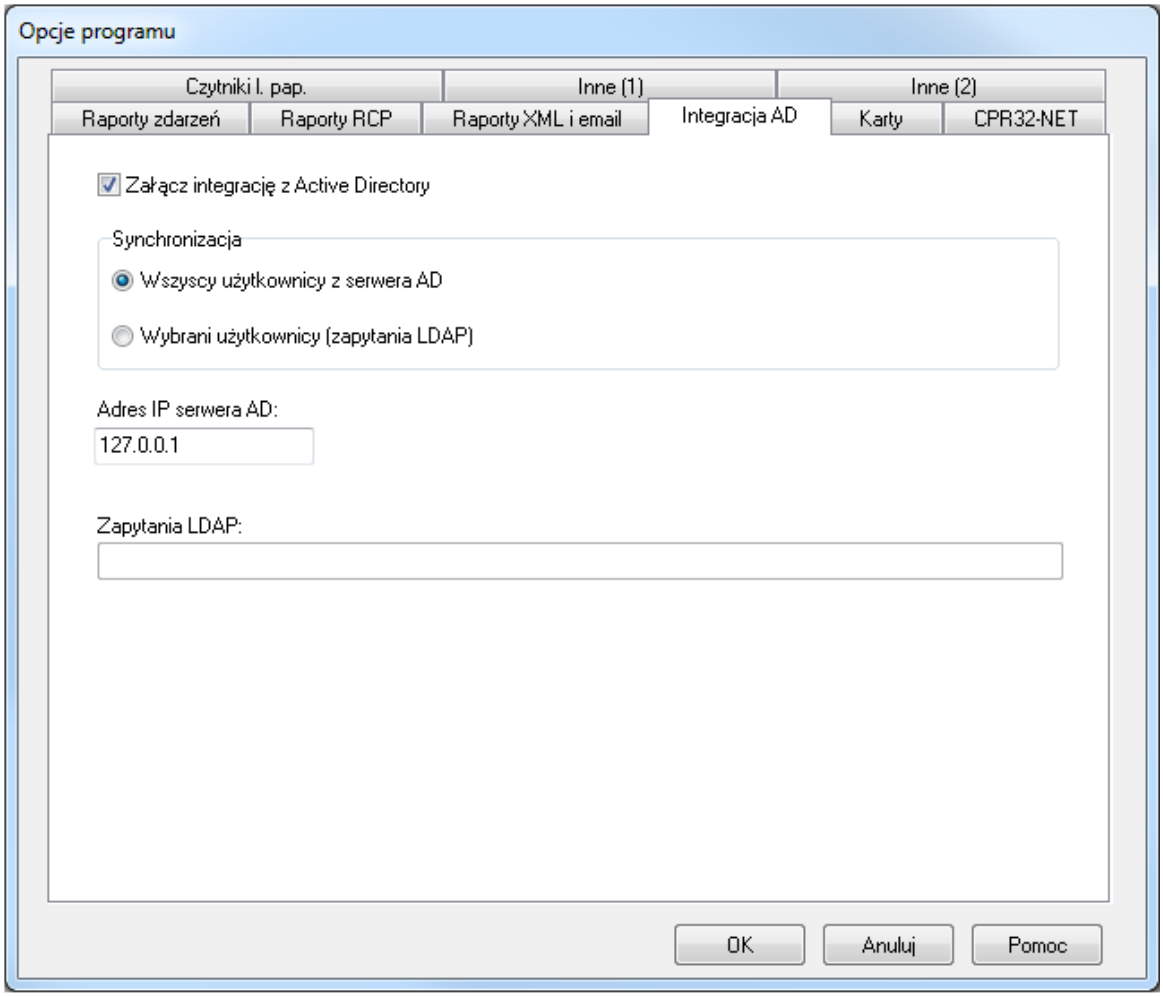
Zakładka **Integracja AD** (rysunek 3.147) umożliwia załączenie integracji z usługą katalogową Active Directory. Integracja umożliwia synchronizację listy użytkowników AD z listą użytkowników systemu RACS 4 ale nie zwalnia operatora programu PR Master z konieczności ustawienia praw dostępu poprzez przypisanie do odpowiedniej grupy dostępu a następnie przesłania nowych ustawień do systemu RACS 4. Po załączeniu integracji w oknie wywoływanym za pomocą opcji **Użytkownicy** w oknie głównym programu PR Master dostępna jest opcja **Synchronizuj z Active Directory** (Rysunek 3.148). Jej wywołanie uruchamia synchronizację listy użytkowników programu PR Master z listą użytkowników Active Directory polegającą na modyfikacji tej pierwszej listy tak by odzwierciedlała tą drugą. Użytkownicy nieobecni w Active Directory są usuwani z bazy danych programu PR Master natomiast obecni w Active Directory są do niej dodawani. Użytkownicy dezaktywowani w Active Directory są dezaktywowani również w bazie danych programu PR Master. Do porównania użytkowników stosowane są ich imiona, nazwiska i adresy e-mail. W związku z tym w ramach integracji konieczne jest by użytkownicy Active Directory mieli zdefiniowane nie tylko imiona i nazwiska ale również adresy e-mailowe w odpowiednich polach. Możliwa jest synchronizacja wszystkich lub wybranych użytkowników z serwera AD. W pierwszym przypadku konieczne jest podanie adresu IP serwera AD, natomiast w drugim stosowane są zapytania LDAP. Możliwe jest zdefiniowanie wielu zapytań LDAP rozdzielonych średnikiem. Przykład zapytania LDAP:

OU=SBSUsers,OU=Users,OU=MyBusiness,DC=ROGER,DC=local

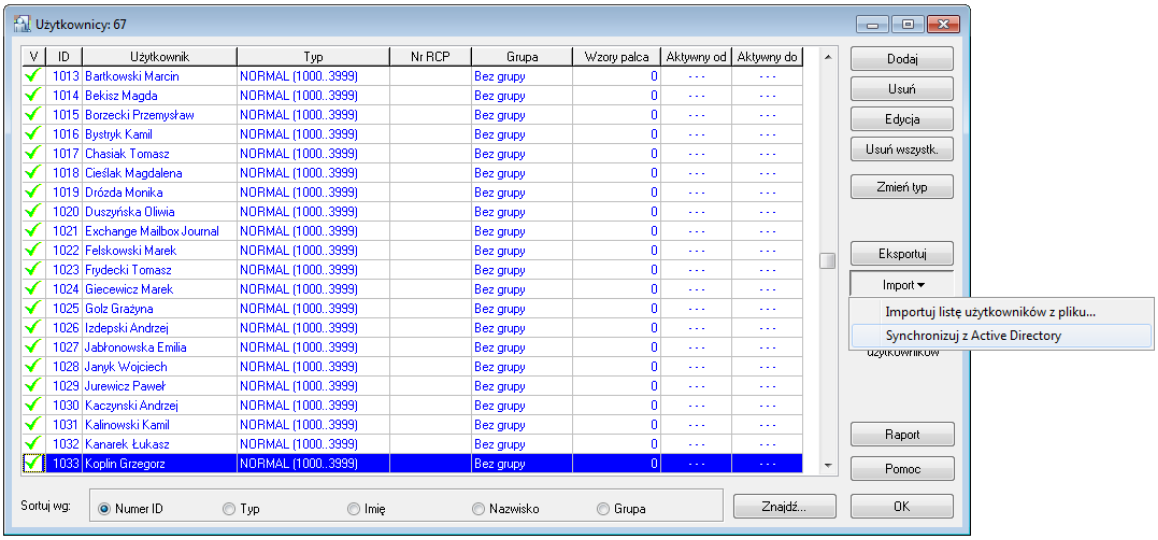
gdzie:

OU – jednostka organizacyjna

DC – składnik nazwy domenowej



Rysunek 3.147. *Opcje integracji AD*

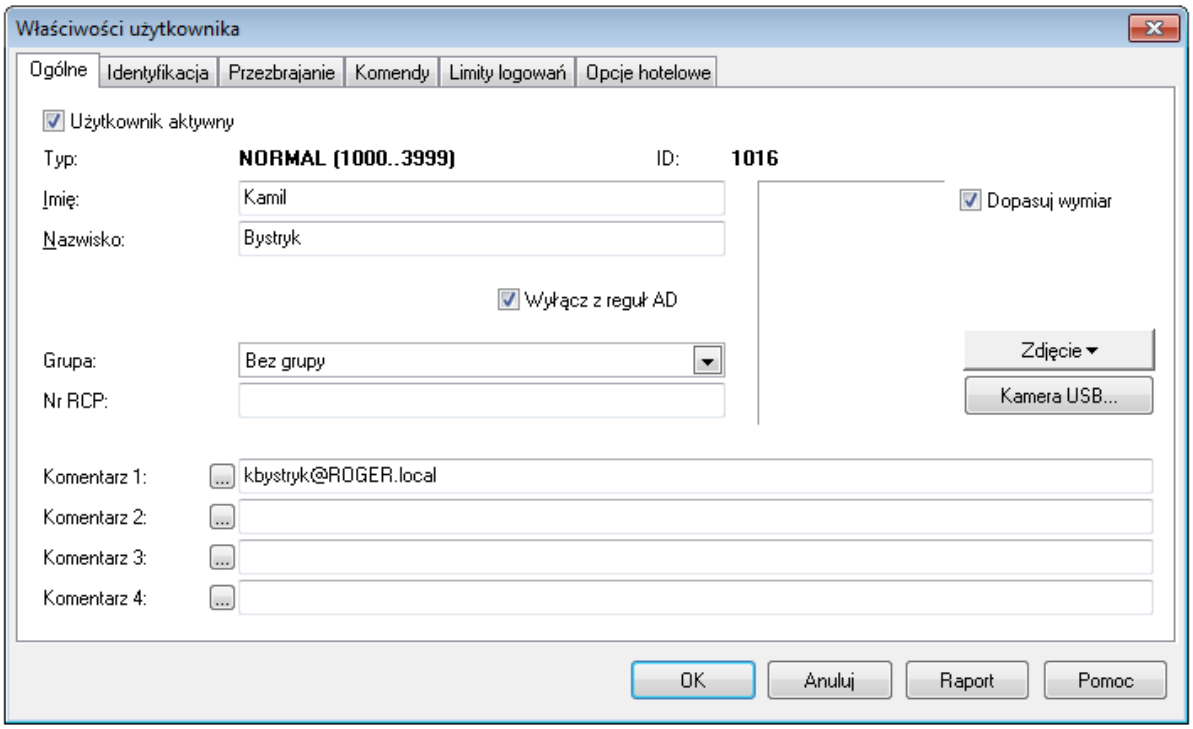


Rysunek 3.148. *Polecenie Synchronizuj z Active Directory*

Użytkownicy dodani po synchronizacji są zaznaczani na niebiesko. Dzięki temu w systemie już funkcjonującym gdzie modyfikacje dotyczą zwykle pojedynczych rekordów możliwe jest zdefiniowanie praw dostępu nowego użytkownika za pomocą funkcji Szybka edycja użytkownika i nie ma potrzeby przesyłania pełnej konfiguracji do systemu.

Użytkownicy zaimportowani z Active Directory mają przydzielane ID powyżej 1000. W związku z tym w ramach integracji konieczne jest stosowanie kontrolerów serii PRxx2 gdyż potrafią one obsłużyć ponad 1000 użytkowników.

Wybranych użytkowników można wyłączyć z reguł synchronizacji. Dzięki temu użytkownicy, których nie zdefiniowano w Active Directory nadal mogą być obsługiwani w systemie RACS 4 (np. personel sprzątający) i nie są oni usuwani w ramach synchronizacji. Aby wyłączyć danego użytkownika z reguł należy w jego właściwościach w zakładce **Ogólne** zaznaczyć opcję **Wyłącz z reguł AD** (Rysunek 3.149). Opcja ta jest widoczna jedynie gdy załączona jest integracja z AD.



Rysunek 3.149. *Opcja wyłączenia z reguł Active Directory*

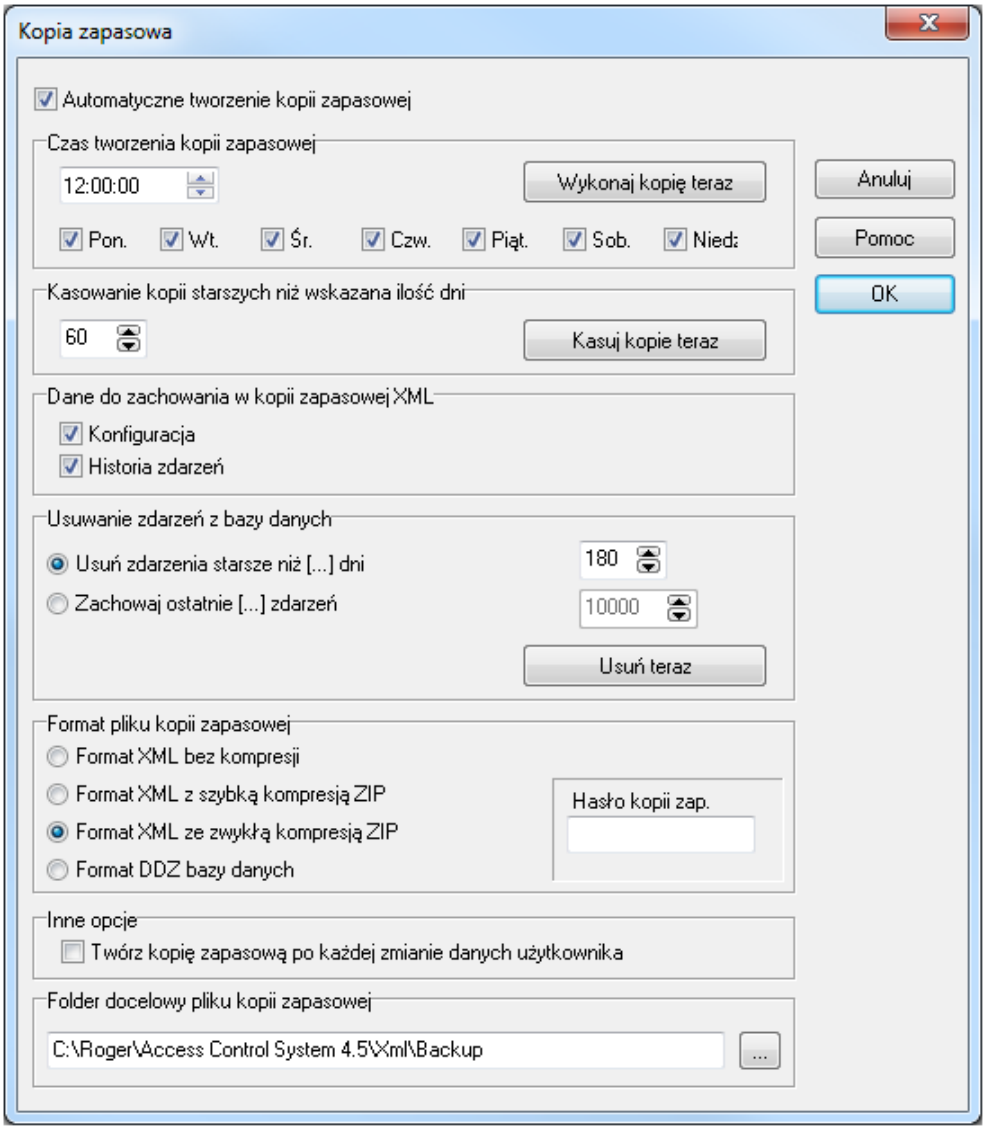
3.5.12. Polecenie Kopia zapasowa

Polecenie **Kopia zapasowa** powoduje wyświetlenie okna dialogowego pozwalającego na zdefiniowanie trybu i harmonogramu wykonywania kopii zapasowych (rysunek 3.150). Większość kontrolek znajdujących się w tym oknie dialogowym jest aktywnych dopiero wtedy, gdy zostanie zaznaczone pole wyboru **Automatyczne tworzenie kopii zapasowej**. Jeśli pole wyboru nie jest zaznaczone, kopie zapasowe nie będą wykonywane automatycznie. W takim przypadku można wykonać kopię zapasową na żądanie. Do tego celu służy przycisk **Wykonaj kopię teraz**.

W obszarze **Czas tworzenia kopii zapasowej** należy wskazać dni tygodnia i godzinę wykonywania kopii. Należy pamiętać, że przy rozbudowanej bazie danych, operacja tworzenia kopii zapasowej może być czasochłonna, dlatego należy dobrać taką godzinę, o której wykonywanie kopii zapasowej w jak najmniejszym stopniu zakłóci pracę systemu. Najlepiej, jeśli są to godziny nocne, kiedy system rejestruje stosunkowo niewielką liczbę zdarzeń.

Obszar **Kasowanie kopii starszych niż wskazana ilość dni** pozwala na zdefiniowanie okresu przechowywania, po którego upływie kopie zapasowe będą usuwane z dysku. Operacja ta będzie wykonywana automatycznie, przy okazji tworzenia kopii zapasowej. Przycisk **Kasuj kopie teraz** powoduje usunięcie przestarzałych kopii zapasowych na żądanie operatora.

W obszarze **Dane do zachowania w kopii zapasowej** znajdują się dwa pola wyboru: **Konfiguracja** oraz **Historia zdarzeń**. Zaznaczenie pola wyboru spowoduje, że w kopii zapasowej XML znajdą się dane wskazanego typu. W przypadku anulowania zaznaczenia dane te zostaną pominięte.



Rysunek 3.150. *Opcje wykonywania kopii zapasowych*

Obszar **Usuwanie zdarzeń z bazy danych** pozwala określić kryteria usuwania zdarzeń z bazy danych. Istnieje możliwość ustalenia liczby dni, po których upływie zdarzenia będą usunięte z bazy danych, albo zdefiniowania rozmiaru historii zdarzeń w postaci stałej liczby zdarzeń, jakie mogą być przechowywane w bazie danych. Jeśli liczba zdarzeń w bazie danych przekroczy tę wartość, najstarsze zdarzenia będą usuwane z bazy. Operacja usuwania zdarzeń jest wykonywana automatycznie, przy okazji tworzenia kopii zapasowej. Przycisk **Usuń teraz** powoduje usunięcie zdarzeń z bazy danych na żądanie operatora.

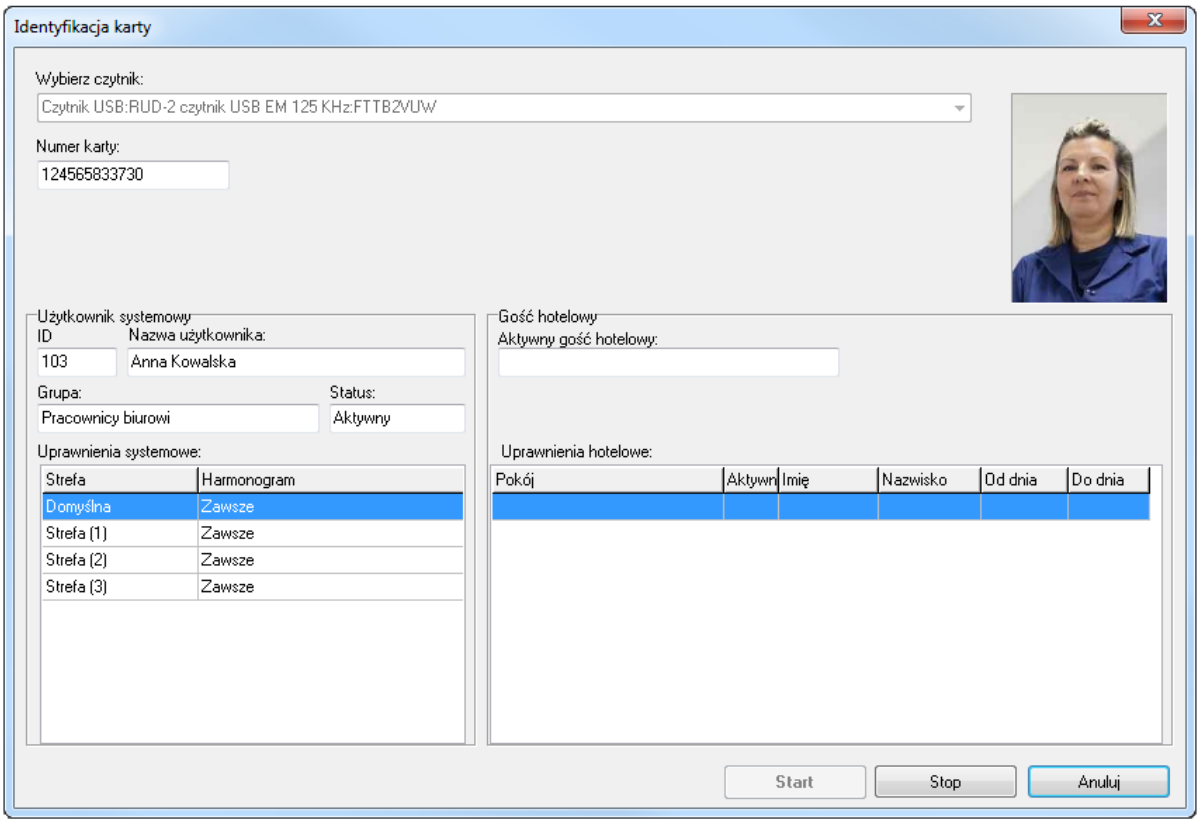
Obszar **Format pliku kopii zapasowej** umożliwia wskazanie formatu pliku, w jakim będzie zapisywana kopia zapasowa. Do wyboru jest format XML bez kompresji, formaty XML z szybką lub

zwykłą kompresją ZIP oraz format kopii bazy danych DDZ. Opcjonalnie można określić hasło dla kopii zapasowej ZIP i DDZ.

W obszarze **Folder docelowy pliku kopii zapasowej** należy wskazać katalog, w którym będzie zapisana kopia zapasowa. Wciśnięcie przycisku ... umożliwia wybór folderu z listy w formie drzewa.

3.5.13 Polecenie Zidentyfikuj uprawnienia karty

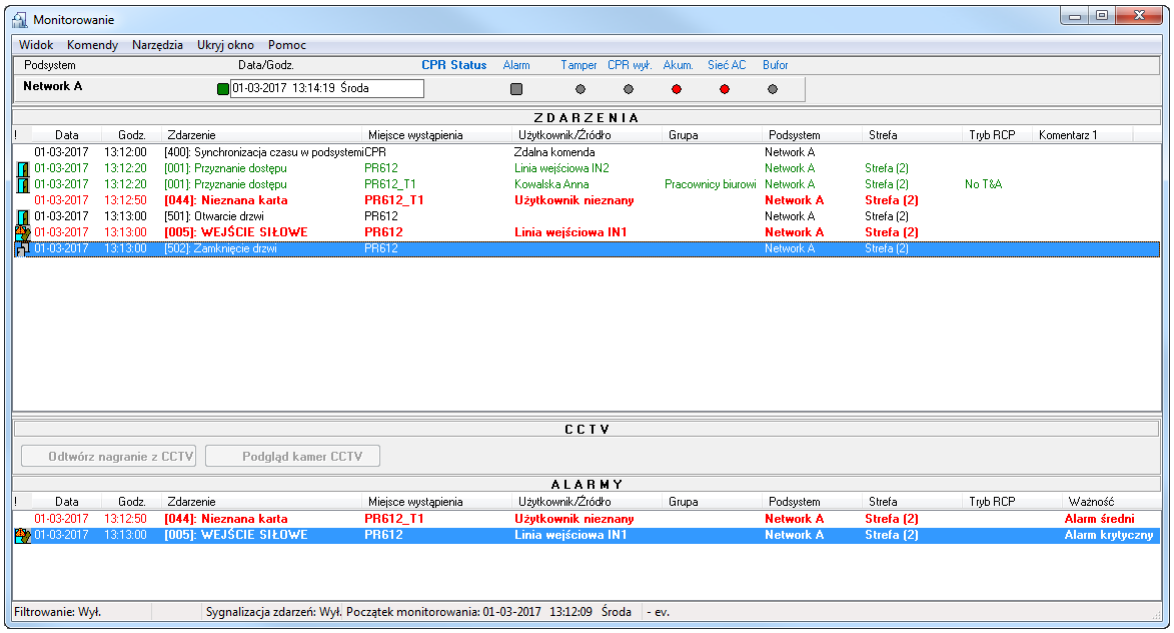
Polecenie **Zidentyfikuj uprawnienia karty** umożliwia określenie czy dana karta należy do użytkownika systemu czy też jest kartą nieznaną (rysunek 3.151). Po otwarciu okna automatycznie wybierany jest pierwszy czytnik na liście więc wystarczy jedynie odczytać na nim karty by zidentyfikować związane z nią uprawnienia.



Rysunek 3.151. *Okno Zidentyfikuj uprawnienia karty*

ROZDZIAŁ 4.
MONITOROWANIE

Monitorowanie jest specjalnym trybem pracy programu PR Master, w którym zdarzenia rejestrowane w systemie RACS 4 są na bieżąco wyświetlane w dedykowanym oknie. Kiedy program PR Master jest w trybie monitorowania, zdarzenia zachodzące w systemie są natychmiast dopisywane do bazy danych systemu i dostępne do tworzenia raportów. Tryb monitorowania można włączyć poprzez wybranie polecenia **Narzędzia**/**Monitorowanie** lub kliknięcie ikony **Monitorowanie** w panelu **Najczęściej wykonywane zadania** z prawej strony głównego okna programu. Okno programu w trybie monitorowania pokazano na rysunku 4.1.



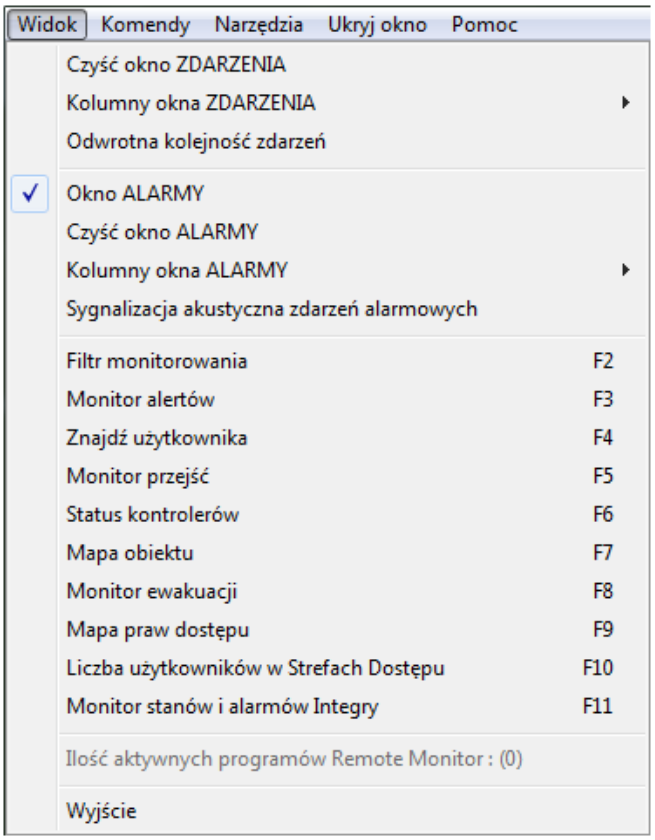
Rysunek 4.1. *Okno programu PR Master w trybie monitorowania*

W tym trybie program ma oddzielne menu, a standardowe menu programu PR Master jest niedostępne. Poniżej paska menu znajduje się lista podsystemów wraz z graficzną informacją dotyczącą alarmów występujących w danym podsystemie. Poniżej znajduje się obszar **ZDARZENIA**, w którym na bieżąco dopisują się zdarzenia zachodzące w systemie. Poniżej obszaru zdarzeń jest obszar **CCTV**, w którym można realizować działania związane z integracją systemu RACS 4 z CCTV. Natomiast na dole widoczny jest obszar **ALARMY**, gdzie wyświetlają się informacje o alarmach zachodzących w systemie.

W pasku stanu wyświetlają się informacje na temat zastosowanych filtrów, stanu sygnalizacji zdarzeń oraz dacie i godzinie początku monitorowania.

4.1. MENU WIDOK

Menu **Widok** pokazano na rysunku 4.2.



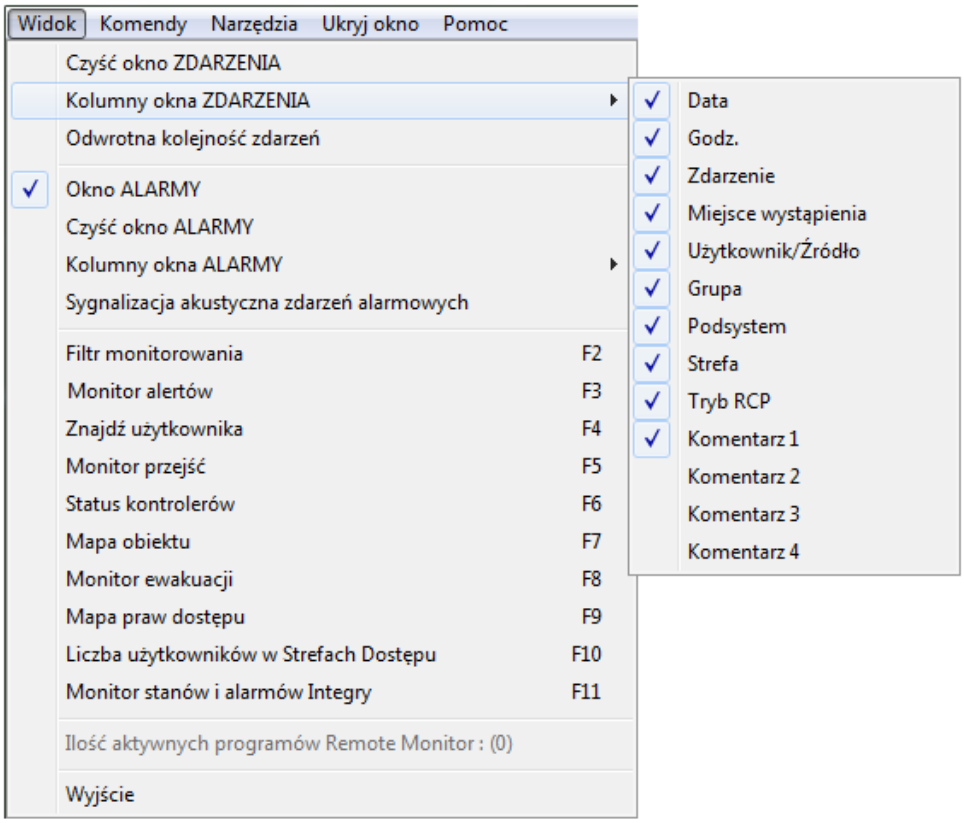
Rysunek 4.2. *Menu Widok programu PR Master w trybie monitorowania*

4.1.1. Polecenie Czyść okno ZDARZENIA

Polecenie powoduje wyczyszczenie okna **ZDARZENIA** wraz ze zdarzeniami wyświetlanymi w oknie **ALARMY**. Zdarzenia nie są jednak usuwane z bazy danych, tylko znikają z okna monitorowania. Funkcja może być przydatna w sytuacji, kiedy chcemy zacząć obserwować zdarzenia od pewnego momentu i nie chcemy rozpraszać swojej uwagi zbyt dużą liczbą zdarzeń w oknie monitorowania.

4.1.2. Polecenie Kolumny okna ZDARZENIA

Polecenie **Kolumny okna ZDARZENIA** otwiera menu z listą kolumn do wyboru (rysunek 4.3). Zaznaczenie określonej kolumny powoduje, że dana kolumna wyświetli się w oknie **ZDARZENIA**.



Rysunek 4.3. *Wybór kolumn do wyświetlenia w oknie ZDARZENIA*

4.1.3. Polecenie Odwrotna kolejność zdarzeń

Standardowo zdarzenia w oknie **Monitorowanie** wyświetlają się w porządku od najstarszych do najnowszych — tzn. na górze listy wyświetlają się najstarsze zdarzenia. Zaznaczenie opcji **Odwrotna kolejność zdarzeń** spowoduje, że na górze listy będą się wyświetlały najnowsze zdarzenia.

4.1.4. Polecenie Okno ALARMY

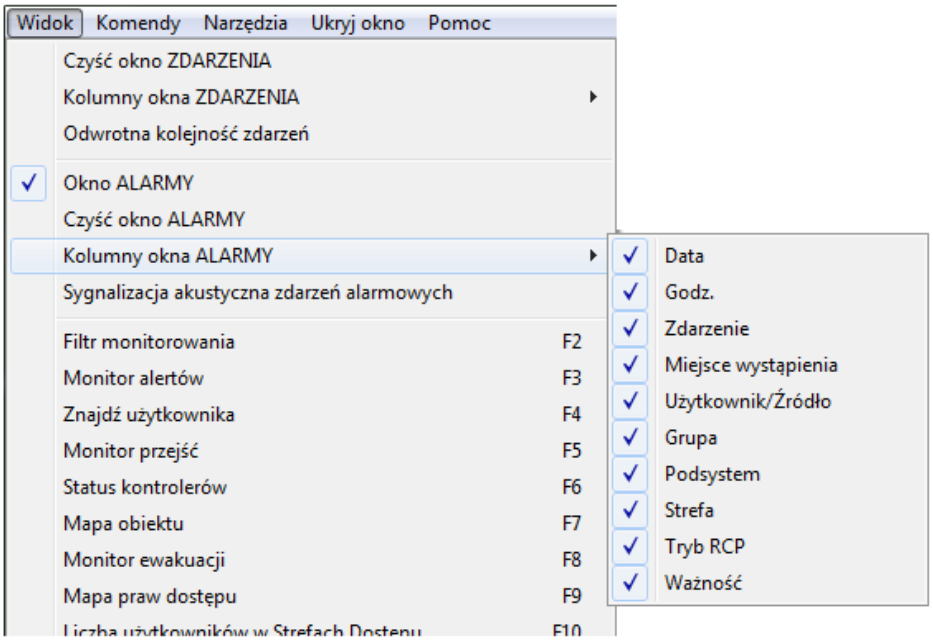
Opcja **Okno ALARMY** pozwala włączać i wyłączać okno **ALARMY**. Jeśli jest zaznaczona, okno **ALARMY** się wyświetla.

4.1.5. Polecenie Czyść okno ALARMY

Polecenie powoduje wyczyszczenie zdarzeń wyświetlanych oknie **ALARMY**. Zdarzenia nie są jednak usuwane z bazy danych, tylko znikają z okna monitorowania. Funkcja może być przydatna w sytuacji, kiedy chcemy zacząć obserwować alarmy od pewnego momentu i nie chcemy rozpraszać swojej uwagi zbyt dużą liczbą alarmów w oknie monitorowania

4.1.6. Polecenie Kolumny okna ALARMY

Polecenie **Kolumny okna ALARMY** otwiera menu z listą kolumn do wyboru (rysunek 4.4). Zaznaczenie określonej kolumny powoduje, że dana kolumna wyświetli się w oknie **ALARMY**.



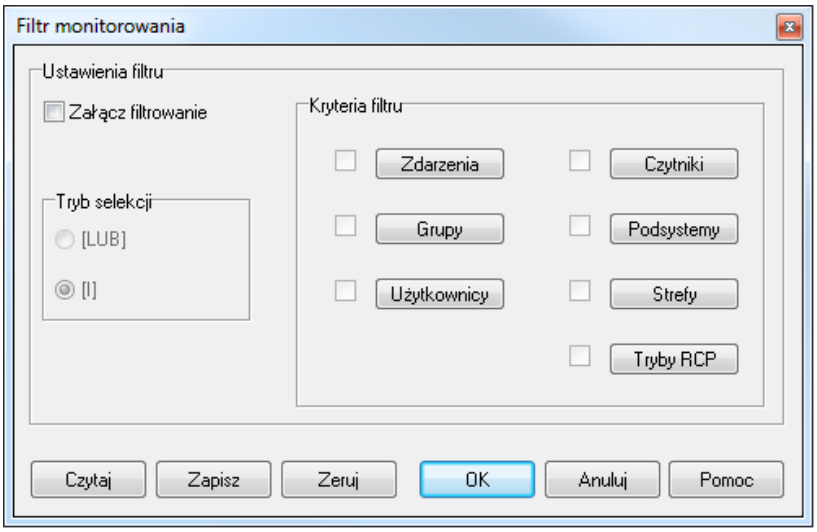
Rysunek 4.4. *Wybór kolumn do wyświetlenia w oknie ALARMY*

4.1.7. Polecenie Sygnalizacja akustyczna zdarzeń alarmowych

Włączenie tej opcji powoduje, że zdarzenia alarmowe będą dodatkowo sygnalizowane akustycznie na komputerze. Jeśli opcja jest wyłączona, zdarzenie alarmowe wyświetli się w oknie **ZDARZENIA** i **ALARMY** ale bez sygnalizacji dźwiękowej.

4.1.8. Polecenie Filtr monitorowania

Wybranie polecenia **Filtr monitorowania** powoduje wyświetlenie okna dialogowego **Filtr monitorowania** (rysunek 4.5).



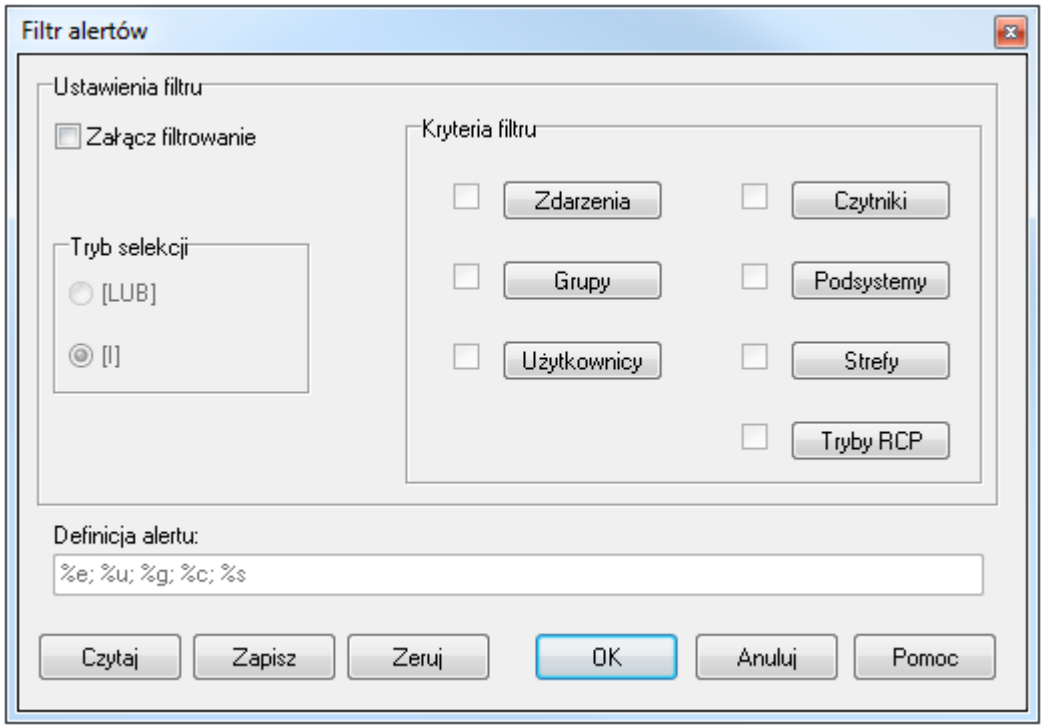
Rysunek 4.5. *Definiowanie filtru w oknie Monitorowanie*

Obsługa tego okna jest identyczna, jak w przypadku definiowania filtra zdarzeń (patrz **punkt 3.3.7**).

Zdefiniowany filtr dotyczy wszystkich zdarzeń zarejestrowanych od momentu włączenia trybu monitorowania. Oznacza to, że jeśli po włączeniu monitorowania użyto polecenia **Czyść okno zdarzeń**, a następnie zdefiniowano filtr, to na liście zdarzeń będą uwzględnione także te zdarzenia, które zostały wcześniej wyczyszczone. Polecenie filtrowania może więc wykorzystać do przywrócenia zawartości okna **Monitorowanie**. Wystarczy wybrać polecenie **Załącz filtrowanie** i kliknąć **OK** w oknie **Filtr monitorowania**.

4.1.9. Polecenie Monitor alertów

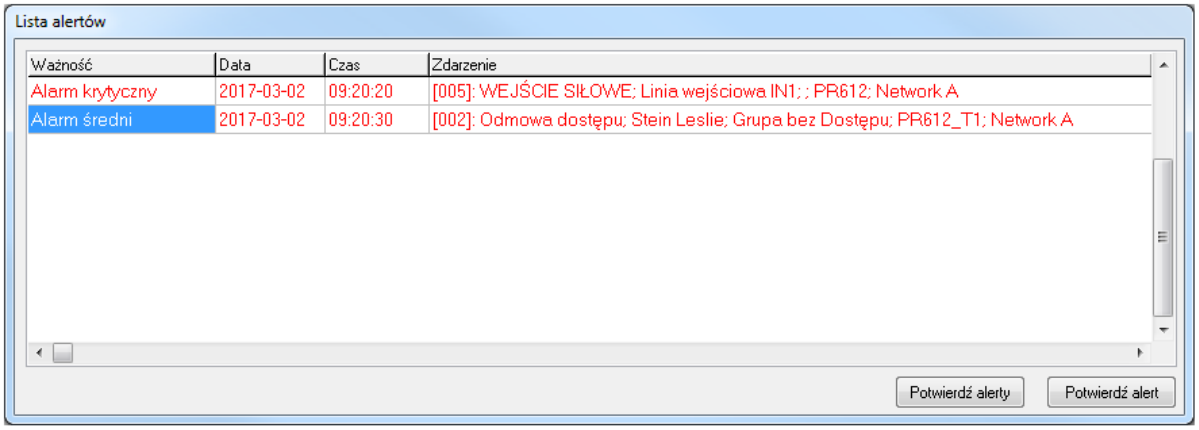
Użycie tej opcji umożliwia zdefiniowanie filtra zdarzeń na podstawie którego program PR Master w trybie monitorowania będzie generował alerty wymagające interwencji operatora. Wybranie polecenia spowoduje wyświetlenie okna dialogowego **Filtr alertów** (rysunek 4.6a).



Rysunek 4.6a. *Definiowanie filtra alertów*

Obsługa tego okna jest podobna do okna definiowania filtru zdarzeń (patrz **punkt 3.3.7**). Okno różni się występowaniem dodatkowego pola **Definicja alertu**. Pozwala ono zdefiniować format komunikatu wyświetlanego w momencie wystąpienia alertu. Domyślne ustawienia to %e; %u; %g; %c; %s. Odpowiadają one odpowiednio zdarzeniu, użytkownikowi, grupie, kontrolerowi/czytnikowi i podsystemowi. Domyślną definicję można zawsze przywrócić wybierając przycisk **Zeruj**. W polu **Definicja alertu** można również wprowadzić własną informację tekstową do wyświetlania wraz z alertami.

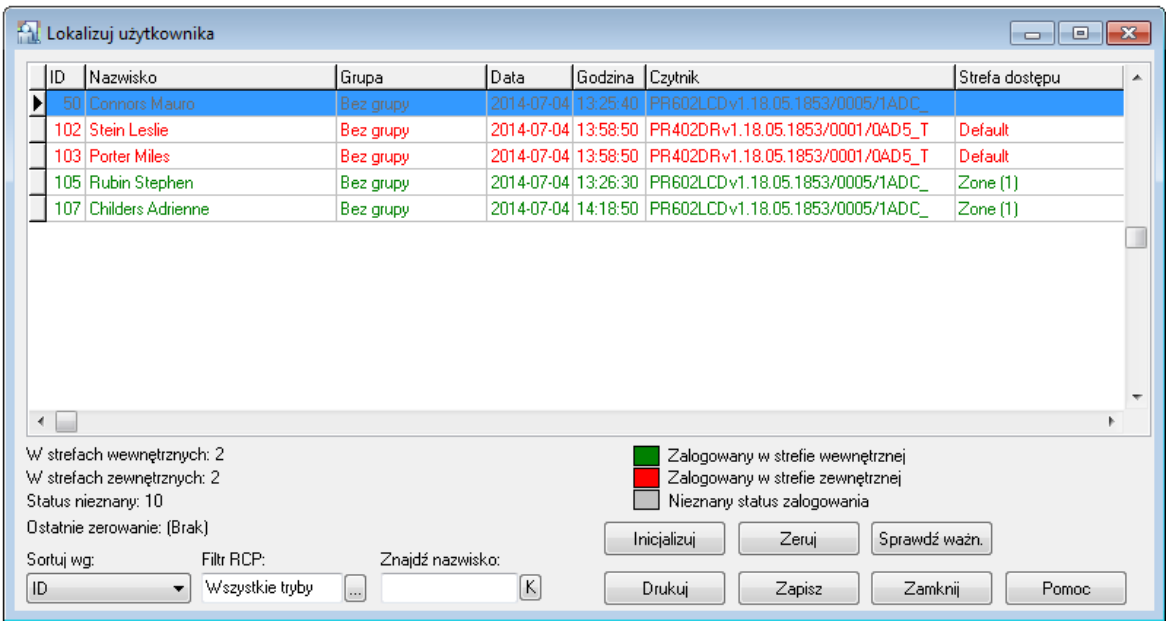
W momencie wystąpienia zdarzenia określonego przez kryteria filtru, w trybie monitorowania programu PR Master wyświetlane jest okno dialogowe **Lista alertów**. Mogą być w nim wyświetlane dowolne zdarzenia spełniające kryteria filtru choć najwięcej praktycznego sensu będzie miał filtr obejmujący zdarzenia alarmowe. Wpisy na liście są posortowane pod względem ważności zdarzenia (alarm krytyczny u góry). Ważność danego zdarzenia można zmieniać (patrz **punkt 3.5.6**). Alerty wymagają potwierdzenia przez operatora.



Rysunek 4.6b. *Przykładowa lista alarmów*

4.1.10. Polecenie Znajdź użytkownika

Polecenie **Znajdź użytkownika** pozwala na zlokalizowanie miejsca (czytnika), na którym ostatnio zalogował się użytkownika. Wybranie polecenia spowoduje wyświetlenie okna dialogowego **Lokalizuj użytkownika** (rysunek 4.7).



Rysunek 4.7. *Miejsce ostatniego logowania użytkowników*

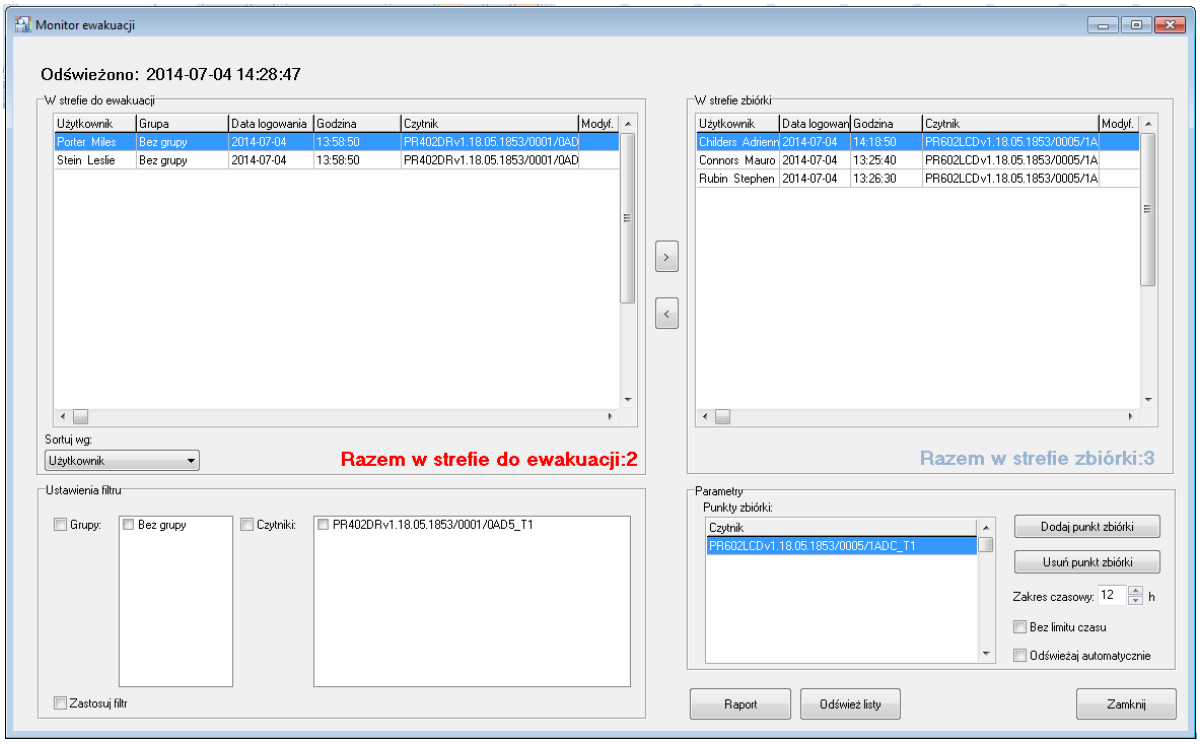
Okno zawiera listę użytkowników wyświetlaną różnymi kolorami w zależności od statusu logowania. Poniżej znajduje się sumaryczne zestawienie liczby osób o określonych statusach oraz wyjaśnienie znaczenia kolorów. Kolor zależy od tego do jakiej strefy wszedł użytkownik a typ strefy zewnętrzna/wewnętrzna określa się podczas definiowania danej strefy (patrz **punkt 3.2.7**). Lista wyboru **Sortuj wg** pozwala na posortowanie listy użytkowników wg identyfikatora, nazwiska, grupy, daty/czasu, czytnika lub strefy dostępu. Pole **Filtr RCP** umożliwia wskazanie tylko tych kontrolerów, które rejestrują wskazany tryb rejestracji czasu pracy. Pole **Znajdź** umożliwia wyszukanie na liście użytkownika o podanym nazwisku. System przeprowadza tzw. „wyszukiwanie aktywne", tzn. w miarę wpisywania kolejnych liter lokalizowany jest użytkownik spełniający wpisane kryterium.

Przycisk **Inicjalizuj** inicjuje listę logowań w oparciu o bieżący rejestr zdarzeń systemu RACS 4. Przycisk **Zeruj** zeruje listę ostatnich logowań a przycisk **Sprawdź ważn**. jest stosowany do weryfikacji ważności identyfikatorów użytkowników (patrz **punkt 3.5.11.4**).

Przycisk **Drukuj** pozwala na wydrukowanie listy logowań na drukarce, natomiast przycisk **Zapisz** pozwala na zapisanie jej w pliku **.rtf** lub **.csv**.

4.1.11. Polecenie Monitor ewakuacji

Polecenie **Monitor ewakuacji** umożliwia wyświetlenie listy osób wymagających ewakuacji z budynku pod nadzorem systemu kontroli dostępu RACS 4. Wybranie polecenia skutkuje wyświetleniem okna dialogowego **Monitor ewakuacji** (rysunek 4.8).

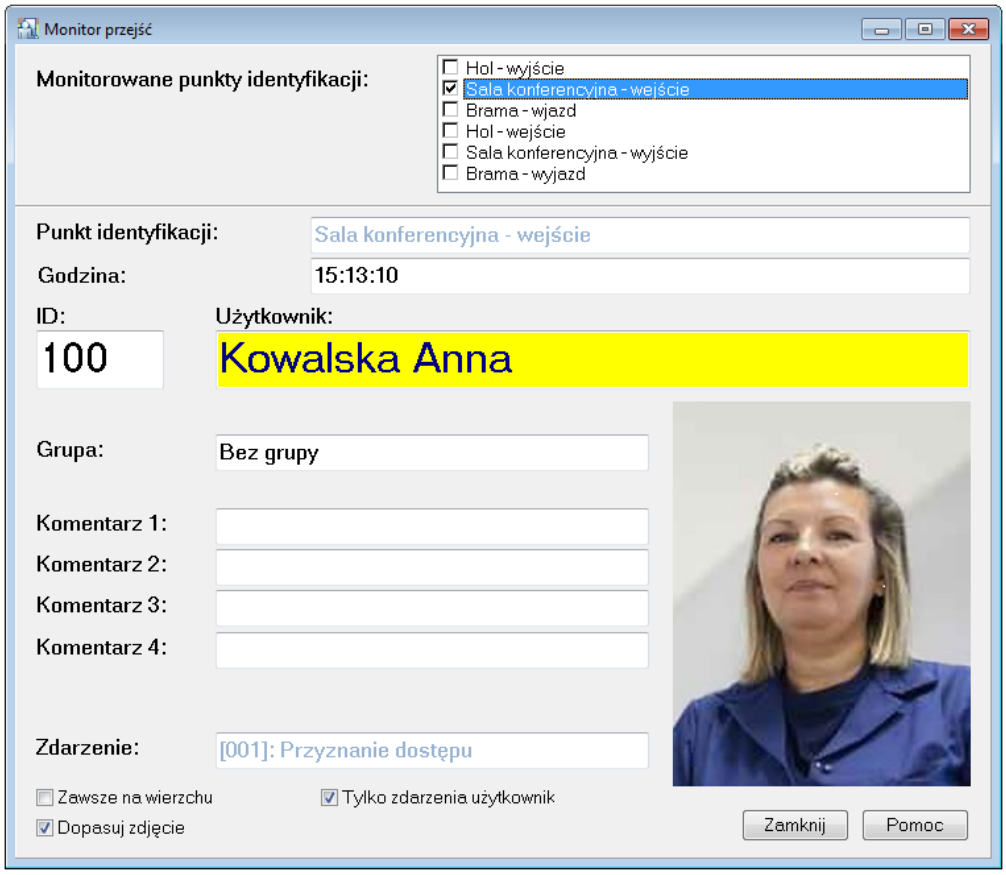


Rysunek 4.8. *Monitor ewakuacji*

Okno przedstawia dwie listy użytkowników. Po lewej podani są ci użytkownicy systemu kontroli dostępu, którzy nie dotarli do punktu(-ów) zbiórki i mogą wymagać ewakuacji a po prawej te osoby, które dotarły do punktu(-ów) zbiórki. Punkt zbiórki czyli czytnik w systemie kontroli dostępu wybiera się w prawym dolnym rogu okna w obszarze **Parametry**. W tym samym obszarze możliwe jest również ustawienie zakresu czasowego obserwacji dla Monitora ewakuacji (domyślnie 12h). Administrator może ręcznie przemieszczać użytkowników pomiędzy listami za pomocą przycisków > oraz <. Może to być wymagane, gdy do miejsca zbiórka dotarła osoba, która zapomniała/zgubiła swój identyfikator. W dolnym lewym rogu okna czyli w obszarze **Ustawienia filtra** możliwe jest filtrowanie osób w strefie ewakuacji po takich parametrach jak Grupy Dostępu czy ostatni czytnik identyfikacji użytkownika. Raport z Monitora ewakuacji można wygenerować a następnie wydrukować i/lub zapisać w formacie pliku **.rtf** lub **.csv** za pomocą przycisku **Raport**. Konfiguracja Monitora ewakuacji jest automatycznie zapisywana w programie PR Master. Przykładowo, jeżeli wybierzemy dany punkt zbiórki to zostanie on zapamiętany i przy ponownym uruchomieniu monitora będzie on już ustawiony. Dzięki temu możliwe jest ustawienie konfiguracji ewakuacyjnej z wyprzedzeniem i w sytuacji awaryjnej jedynie włączenie monitora bez tracenia czasu na wprowadzania jakichkolwiek ustawień.

4.1.12. Polecenie Monitor przejść

Polecenie **Monitor przejść** umożliwia wizualizację informacji o użytkowniku w momencie użycia identyfikatora na wybranych przejściach. Wybranie polecenia powoduje wyświetlenie okna dialogowego **Monitor przejść** (rysunek 4.9).

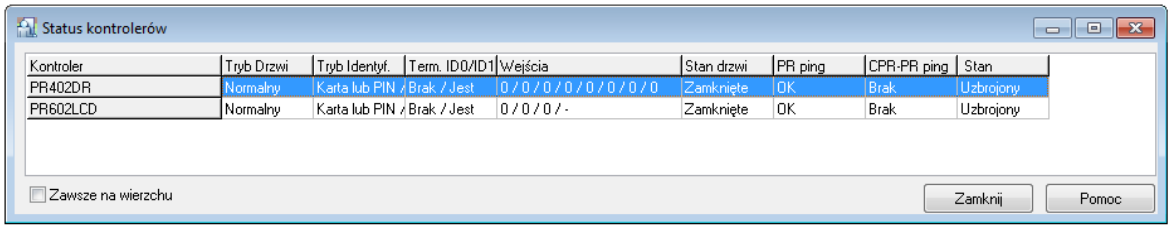


Rysunek 4.9. *Monitor przejść*

W oknie należy wybrać punkty identyfikacji, które mają być monitorowane. W przypadku zgłoszenia się użytkownika na jednym z wybranych punktów, program pokazuje informacje o zdarzeniu oraz informacje o samym użytkowniku wraz z jego fotografią. Dzięki temu można zweryfikować, czy danym identyfikatorem posługuje się właściwa osoba. Ma to szczególne znaczenie w systemach o dużej liczbie użytkowników. W przypadku zaznaczenia opcji **Tylko zdarzenia użytkowników**, w oknie będą wyświetlane jedynie zdarzenia związane z identyfikacją użytkowników.

4.1.13. Polecenie Status kontrolerów

Polecenie **Status kontrolerów** wyświetla okno zawierające informacje o kontrolerach pracujących w systemie RACS 4 (rysunek 4.10).

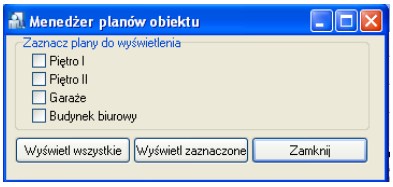


Rysunek 4.10. *Status kontrolerów*

W oknie można odczytać takie informacje, jak tryb drzwi, status terminali ID0/ID1, stany wejść, drzwi, komunikacji z kontrolerem oraz statusu UZBR./ROZBR. Dane w tabeli są odświeżane co 5 sekund. Symbol BD oznacza brak danych. Dane można sortować poprzez dwukrotne kliknięcie danej kolumny.

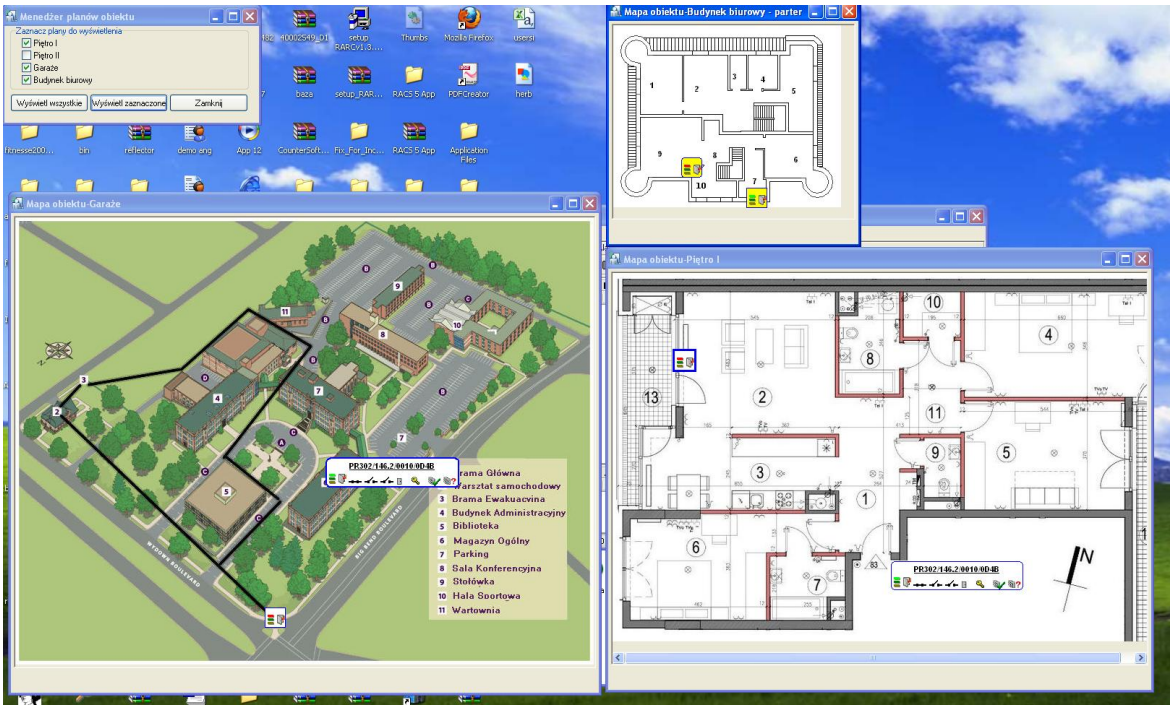
4.1.14. Polecenie Mapa obiektu

Polecenie **Mapa obiektu** pozwala na wizualne monitorowanie systemu z wykorzystaniem zdefiniowanych wcześniej planów obiektów (patrz **punkt 3.2.14**). Po wybraniu polecenia, w lewym górnym rogu ekranu wyświetla się okno Menedżera planów obiektu (rysunek 4.11) pozwalające użytkownikowi na wskazanie planów obiektu, które maja się wyświetlić.



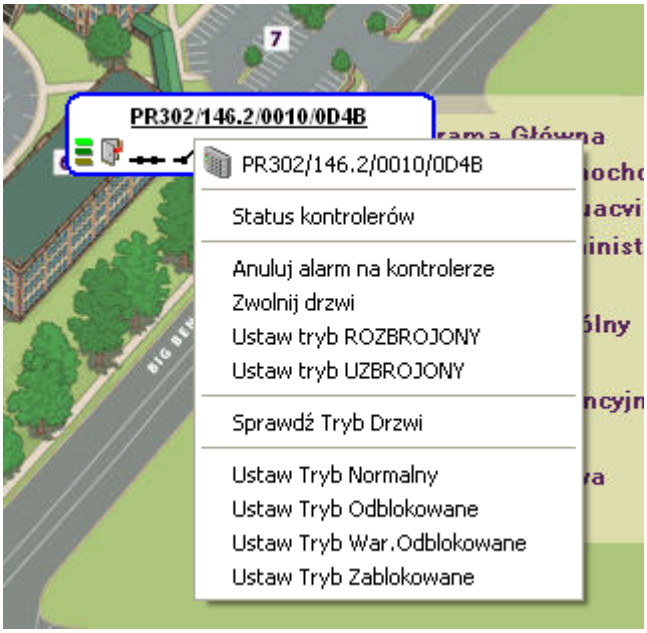
Rysunek 4.11. *Menedżer planów obiektu — wskazywanie planów do wyświetlania*

Po wskazaniu wybranych planów i kliknięciu przycisku **Wyświetl zaznaczone**, program wyświetla zdefiniowane wcześniej plany obiektu. Ekran monitorowania może wyglądać tak, jak pokazano na rysunku 4.12).



Rysunek 4.12. *Wizualne monitorowanie obiektu*

W tym trybie można śledzić w czasie rzeczywistym stany kontrolerów, a także wydawać do nich komendy. Aby uzyskać dostęp do menu z komendami należy kliknąć prawym przyciskiem ikonę kontrolera (rysunek 4.13).



Rysunek 4.13. *Menu komend do kontrolera*

Kliknięcie ikony kontrolera lewym przyciskiem myszki powoduje wyświetlenie pełnych informacji o jego statusie. Dzięki temu można dowiedzieć się więcej o kontrolerze reprezentowanym przez maksymalnie zredukowaną ikonę (patrz rysunek 4.14 - porównaj z rysunkiem 4.13)

Rysunek 4.14. *Po kliknięciu ikony kontrolera wyświetlają się pełne informacje na jego temat*

Po wybraniu planów obiektu do wyświetlania, można zamknąć okno **Menedżera planów obiektu**. Można także dowolnie przemieszczać i zamykać okna poszczególnych planów. Trzeba jednak pamiętać, że PR Master automatycznie zapamiętuje ostatnie położenie i układ każdego z planów

dzięki czemu przy kolejnym wyświetleniu planu pojawi się on w takiej pozycji, w jakiej było ono przy zamknięciu.

Zamknięcie okna monitorowania systemu powoduje automatyczne zamknięcie wszystkich otwartych planów obiektu.

4.1.15. Polecenie Mapa praw dostępu

Polecenie **Mapa praw dostępu** jest odpowiednikiem polecenia **Narzędzia**/**Mapa praw dostępu** dostępnego poza trybem monitorowania. Opisano je w **punkcie 3.5.3**.

4.1.16. Polecenie Liczba użytkowników w strefach dostępu

Polecenie **Liczba użytkowników w strefach dostępu** jest odpowiednikiem polecenia **Narzędzia**/**Liczba użytkowników w strefach dostępu** dostępnego poza trybem monitorowania. Opisano je w **punkcie 3.5.4**.

4.1.17. Polecenie Monitor stanów i alarmów Integry

Polecenie **Monitor stanów i alarmów Integry** jest stosowane w ramach integracji z centralami alarmowymi serii INTEGRA (SATEL). Integracja wymaga zastosowania centrali CPR32-NET. Więcej informacji na ten temat podano w dedykowanej instrukcji dostępnej na stronie **www.roger.pl**.

4.1.18. Polecenie Ilość aktywnych programów Remote Monitor

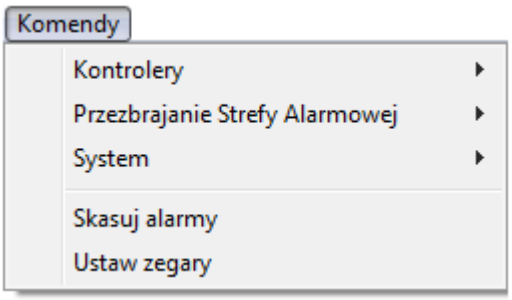
Program Remote Monitor może być klientem programu PR Master. Program ten pozwala na zdalne monitorowanie systemu RACS 4. Polecenie **Ilość aktywnych programów Remote Monitor** pokazuje liczbę uruchomionych klientów Remote Monitor, które nawiązały połączenie z programem PR Master.

4.1.19. Polecenie Wyjście

Polecenie **Wyjście** powoduje zamknięcie trybu monitorowania programu PR Master. Przed zamknięciem, program wyświetla pytanie o potwierdzenie zamiaru zamknięcia tego trybu pracy programu.

4.2. MENU KOMENDY

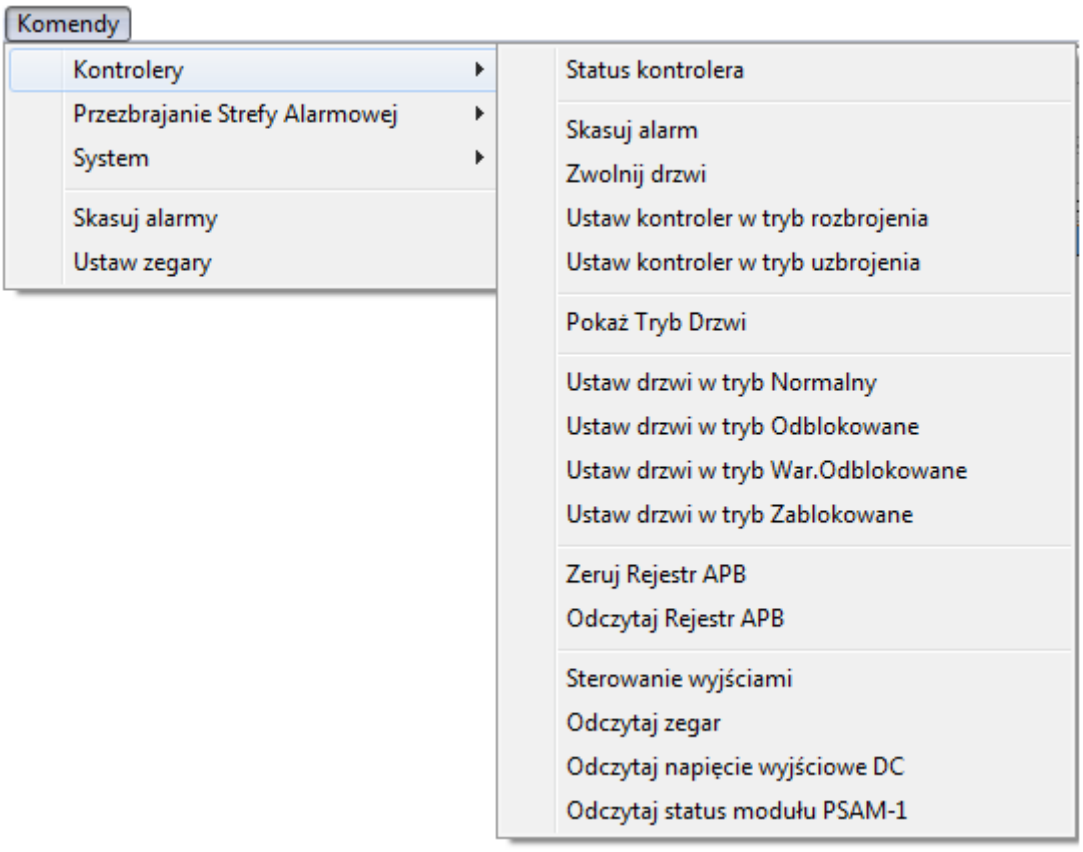
Menu **Komendy** pokazano na rysunku 4.15.



Rysunek 4.15. *Menu Komendy*

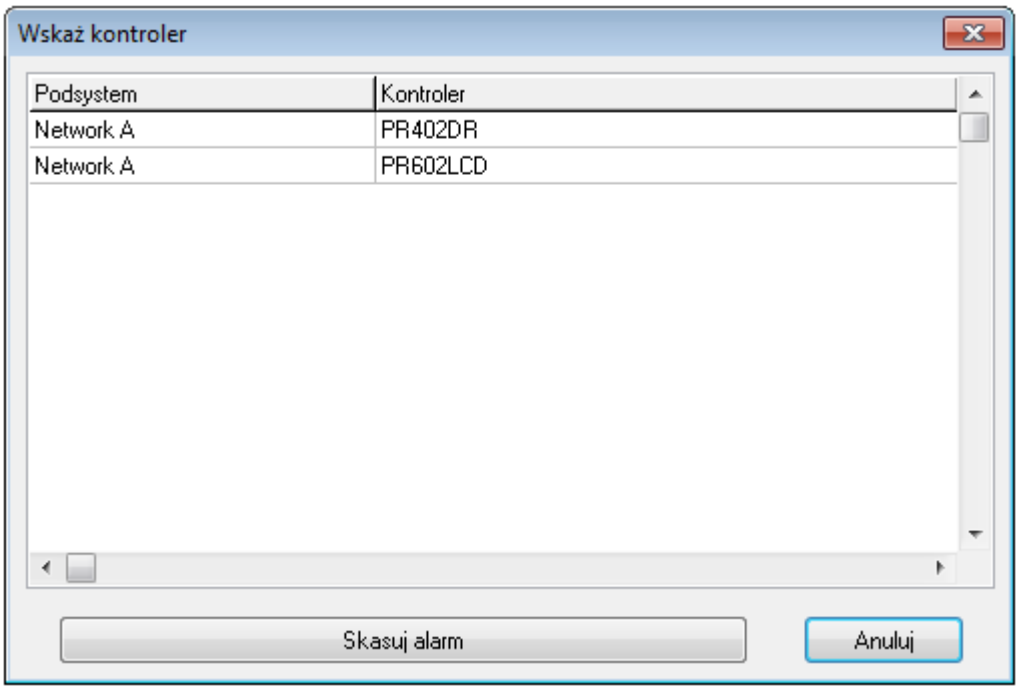
4.2.1. Podmenu Kontrolery

Podmenu **Kontrolery** zawiera listę komend dostępnych do wykonania dla wskazanego kontrolera. Listę komend przedstawiono na rysunku 4.16.



Rysunek 4.16. *Podmenu Kontrolery*

Wybór dowolnej komendy z menu powoduje wyświetlenie okno wyboru kontrolera (rysunek 4.17).

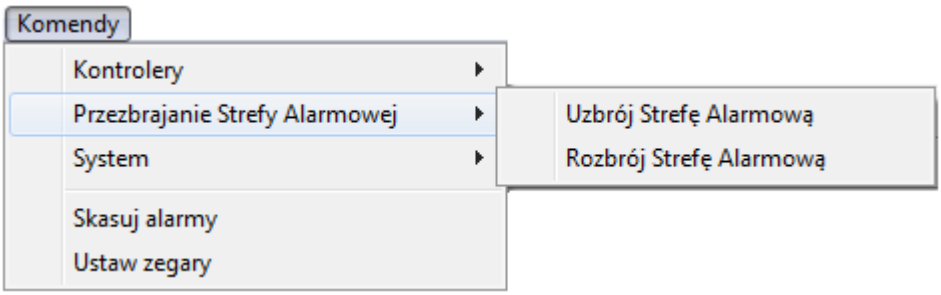


Rysunek 4.17. *Okno wyboru kontrolera do wykonania komendy*

Należy wskazać kontroler na liście, a następnie kliknąć przycisk komendy (w przypadku pokazanym na rysunku **Skasuj alarm**). W przypadku, gdy nie zostanie wybrany żaden kontroler, komenda będzie wykonana dla pierwszego kontrolera z listy.

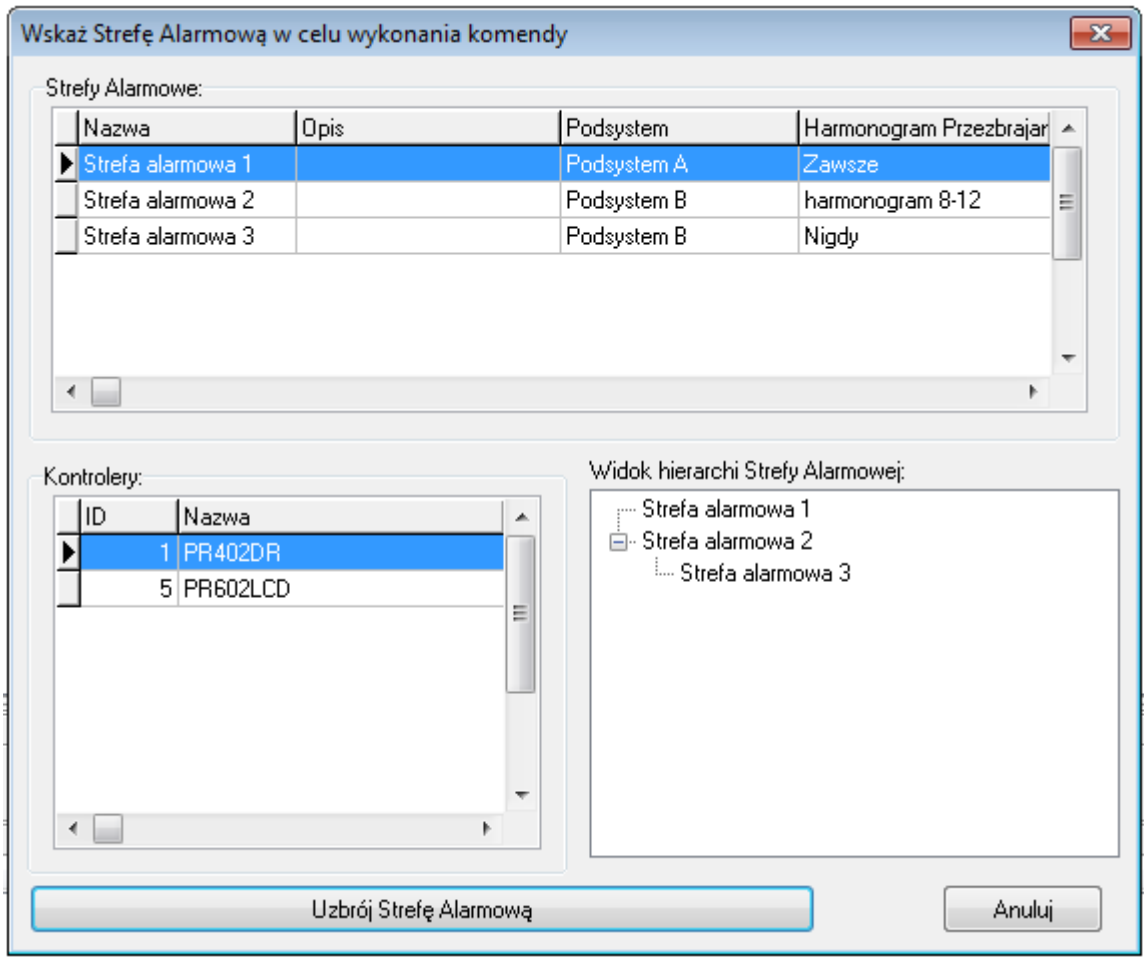
4.2.2 Podmenu Przezbrajanie Strefy Alarmowej

Podmenu **Przezbrajanie Strefy Alarmowej** zawiera listę komend dostępnych do wykonania dla wskazanej strefy alarmowej. Listę komend przedstawiono na rysunku 4.18.



Rysunek 4.18. *Okno wyboru strefy alarmowej do wykonania komendy*

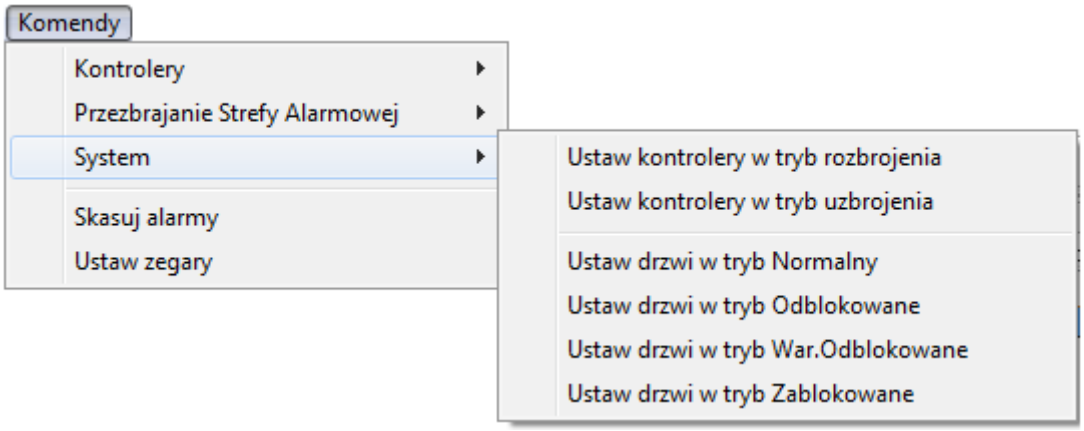
Wybór dowolnej komendy z menu powoduje wyświetlenie okno wyboru strefy alarmowej (rysunek 4.19).



Rysunek 4.19. *Okno wyboru strefy alarmowej do wykonania komendy*

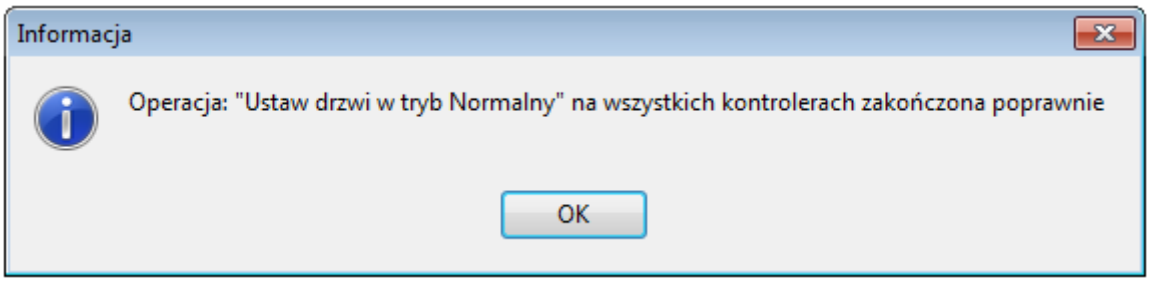
4.2.3. Podmenu System

Podmenu **System** zawiera listę komend dotyczących całego systemu. Przedstawiono je na rysunku 4.20.



Rysunek 4.20. *Podmenu Systemy*

Wybór dowolnej komendy z menu powoduje wykonanie jej dla wszystkich kontrolerów w całym systemie. Po wykonaniu operacji program wyświetla potwierdzenie jej wykonania (rysunek 4.21).



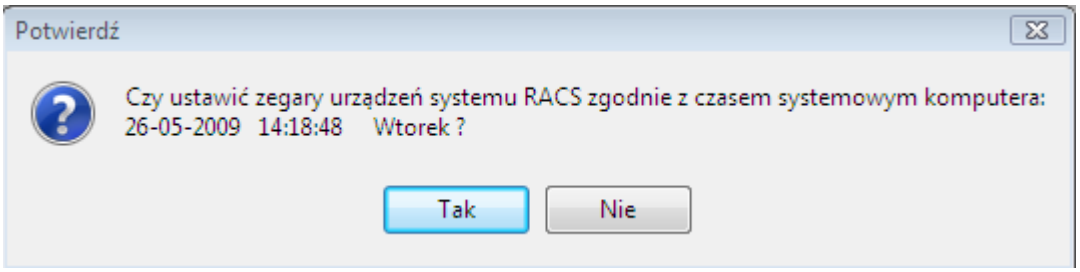
Rysunek 4.21. *Potwierdzenie wykonania komendy na wszystkich kontrolerach w systemie*

4.2.4. Polecenie Skasuj alarmy

Polecenie **Skasuj alarmy** powoduje skasowanie wszystkich występujących aktualnie alarmów w systemie RACS 4. Jeśli w danym momencie w systemie nie ma żadnych alarmów, to wykonanie polecenia nie przynosi żadnego efektu.

4.2.5. Polecenie Ustaw zegary

Polecenie **Ustaw zegary** służy do ustawiania zegarów wszystkich urządzeń systemu RACS 4 zgodnie ze wskazaniami systemowego zegara komputera. Wybranie polecenia spowoduje wyświetlenie okna z pytaniem o potwierdzenie tego zamiaru (rysunek 4.22).

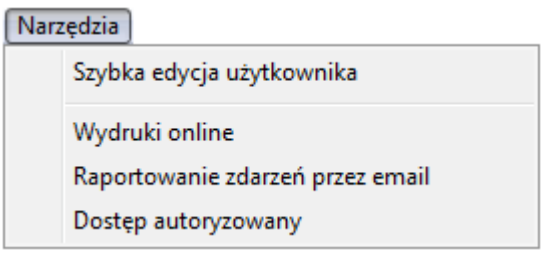


Rysunek 4.22. *Ustawianie zegarów w systemie RACS 4*

Twierdząca odpowiedź na pytanie wyświetlane w tym oknie spowoduje ustawienie zegarów wszystkich urządzeń w systemie RACS 4 zgodnie ze wskazaniami zegara systemowego komputera

4.3. MENU NARZĘDZIA

Menu **Narzędzia** trybu monitorowania pokazano na rysunku 4.23.



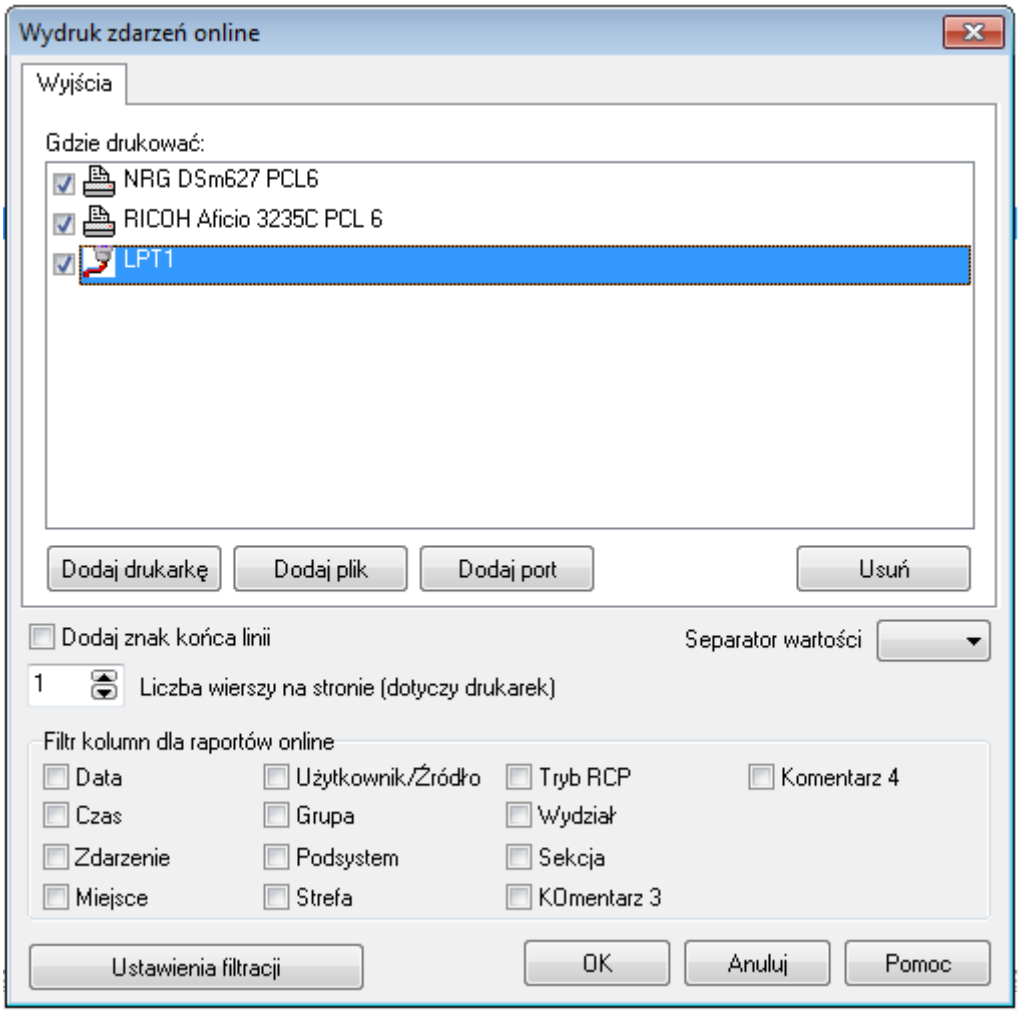
Rysunek 4.23. *Menu Narzędzia*

4.3.1. Polecenie Szybka edycja użytkowników

Polecenie to jest odpowiednikiem polecenia **Narzędzia/Szybka edycja użytkowników** dostępnego poza trybem monitorowania. Opisano je w **punkcie 3.5.2**.

4.3.2. Polecenie Wydruki online

Polecenie **Wydruki online** umożliwia wysyłanie na bieżąco wszystkich lub wybranych zdarzeń z systemu RACS 4 do zdefiniowanych urządzeń, plików lub portów. Wybranie polecenia spowoduje wyświetlenie okna dialogowego **Wydruk zdarzeń online** (rysunek 4.24).



Rysunek 4.24. *Ustawienia wydruków online*

Przyciski **Dodaj drukarkę**, **Dodaj plik** i **Dodaj port** w obszarze **Wyjścia** pozwalają na wskazanie odpowiednio drukarek, plików i portów, gdzie będą generowane wydruki. Przycisk **Usuń** pozwala na usunięcie określonych wyjść z listy.

Zaznaczenie pola wyboru **Dodaj znak końca linii** powoduje, że każde zdarzenie na wydruku online będzie zakończone znakiem przejścia do nowego wiersza. Pole **Liczba wierszy na stronie (dotyczy drukarek)** pozwala na ustawienie liczby wierszy na stronie wydruku generowanego na drukarkę.

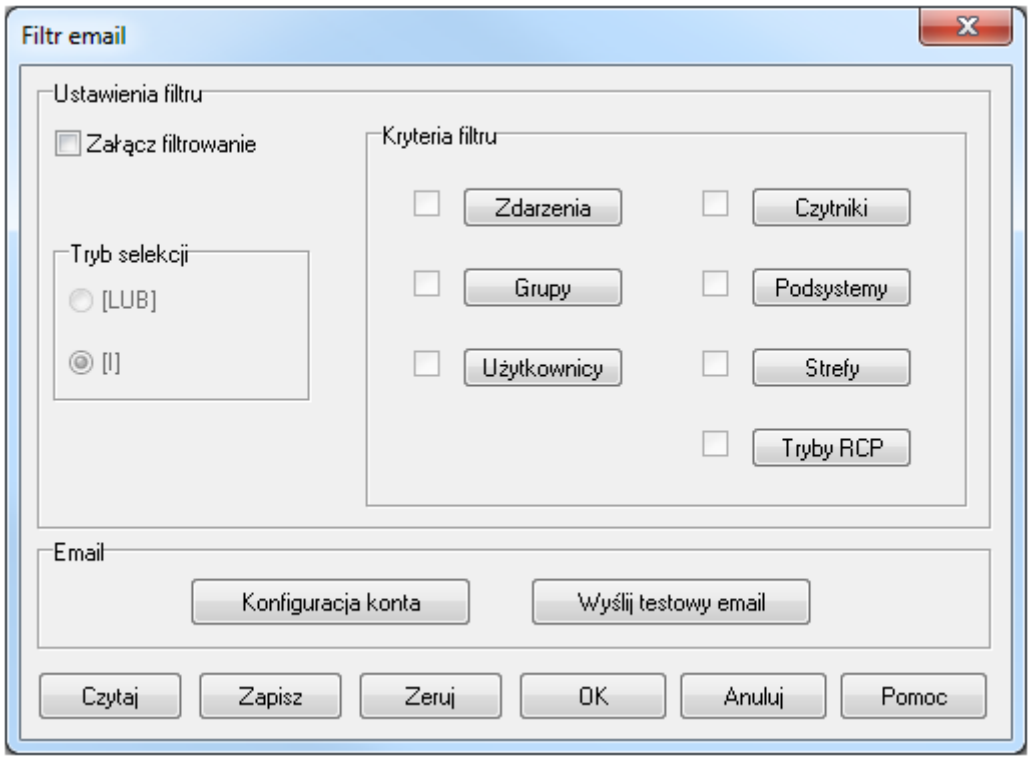
Lista wyboru **Separator wartości** umożliwia wskazanie znaku specjalnego, który rozdziela poszczególne dane. Może to być przecinek, średnik, albo znak specjalny (CR lub LF).

Przycisk **Ustawienia filtracji** powoduje wyświetlenie okna dialogowego **Ustawienia filtrowania**, gdzie można określić filtr zdarzeń umieszczanych na wydruku.

Więcej informacji na temat sposobu definiowania filtrów można znaleźć w **punkcie 3.3.7.1**.

4.3.3. Polecenie Raportowanie zdarzeń przez e-mail

Wybranie polecenia **Raportowanie zdarzeń przez email** spowoduje wyświetlenie okna dialogowego **Filtr email** (rysunek 4.25).

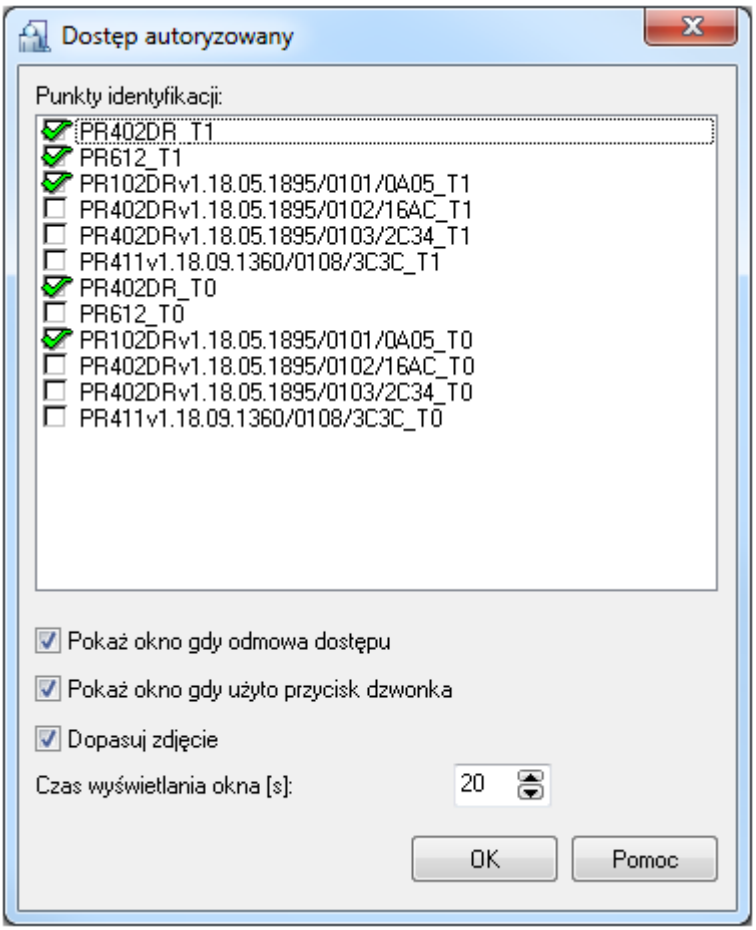


Rysunek 4.25. *Ustawienia raportów zdarzeń wysyłanych pocztą elektroniczną*

W tym oknie można wskazać zdarzenia, które zostaną przesłane pocztą elektroniczną pod wskazany adres. W obszarze **Ustawienia filtru** można dokonać selekcji zdarzeń, które znajdą się w raporcie. Aby wysłać raport, należy najpierw zdefiniować filtr (zaznaczyć pole wyboru **Załącz filtrowanie** oraz zdefiniować kryteria filtru). Sposób ustawienia filtru opisano w **punkcie 3.3.7.1**. Sposób konfiguracji konta e-mail i adresata raportu opisano w **punkcie 3.5.11.3**.

4.3.4. Polecenie Dostęp autoryzowany

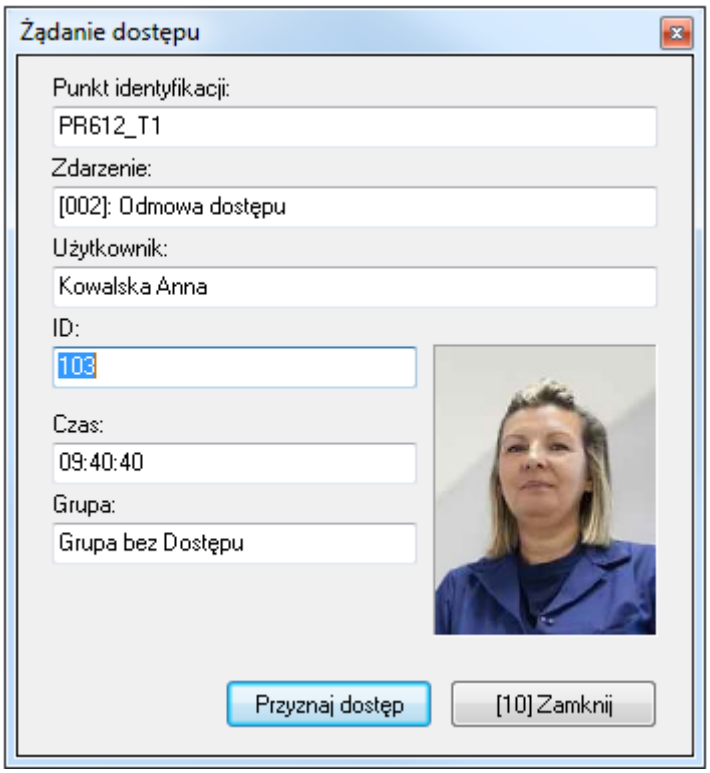
Polecenie **Dostęp autoryzowany** umożliwia zdalne przyznanie dostępu przez operatora programu w sytuacji, kiedy system RACS 4 odmawia dostępu danemu użytkownikowi na danym przejściu. Wybranie polecenia powoduje wyświetlenie okna dialogowego **Dostęp autoryzowany** (rysunek 4.26).



Rysunek 4.26. *Ustawienia dostępu autoryzowanego*

Na liście **Punkty identyfikacji** można wskazać czytniki, których ma dotyczyć funkcja dostępu na żądanie. Zaznaczenie pola wyboru **Pokaż okno gdy odmowa dostępu** spowoduje, że okno **Żądanie dostępu** wyświetli się w sytuacji, gdy system RACS 4 normalnie odmówiłby dostępu. Z kolei zaznaczenie pola wyboru **Pokaż okno gdy użyto przycisk dzwonka**, spowoduje wyświetlenie okna **Żądanie dostępu** w odpowiedzi na przyciśnięcie dzwonka podłączonego do kontrolera. Pole wyboru **Dopasuj zdjęcie** spowoduje wyświetlenie zdjęcia użytkownika żądającego dostępu autoryzowanego. Suwak **Czas wyświetlania okna** określa czas (wyrażony w sekundach), na jaki wyświetli się okno **Żądanie dostępu**.

Jeśli skonfigurowano opcję **Dostęp autoryzowany** to w przypadku odmowy dostępu użytkownikowi, program PR Master wyświetli okno dialogowe **Żądanie dostępu** (rysunek 4.27).



Rysunek 4.27. *Dostęp na żądanie*

W oknie wyświetlają się informacje na temat punktu identyfikacji, zdarzenia oraz dane użytkownika żądającego dostępu. W nawiasie kwadratowym na przycisku **Zamknij** wyświetla się liczba sekund pozostałych do samoczynnego zamknięcia okna. Jeśli przed upływem tego czasu operator kliknie przycisk **Przyznaj dostęp** to kontroler udzieli użytkownikowi dostępu na żądanie.

4.4. Polecenie Ukryj okno

W menu głównym trybu monitorowania znajduje się polecenie **Ukryj okno**. Jego wybranie powoduje zminimalizowanie okna monitorowanie. Ponowne jego otwarcie odbywa się poprzez kliknięcie ikony programu PR Master na pasku zadań i wymaga podania hasła operatora programu PR Master.

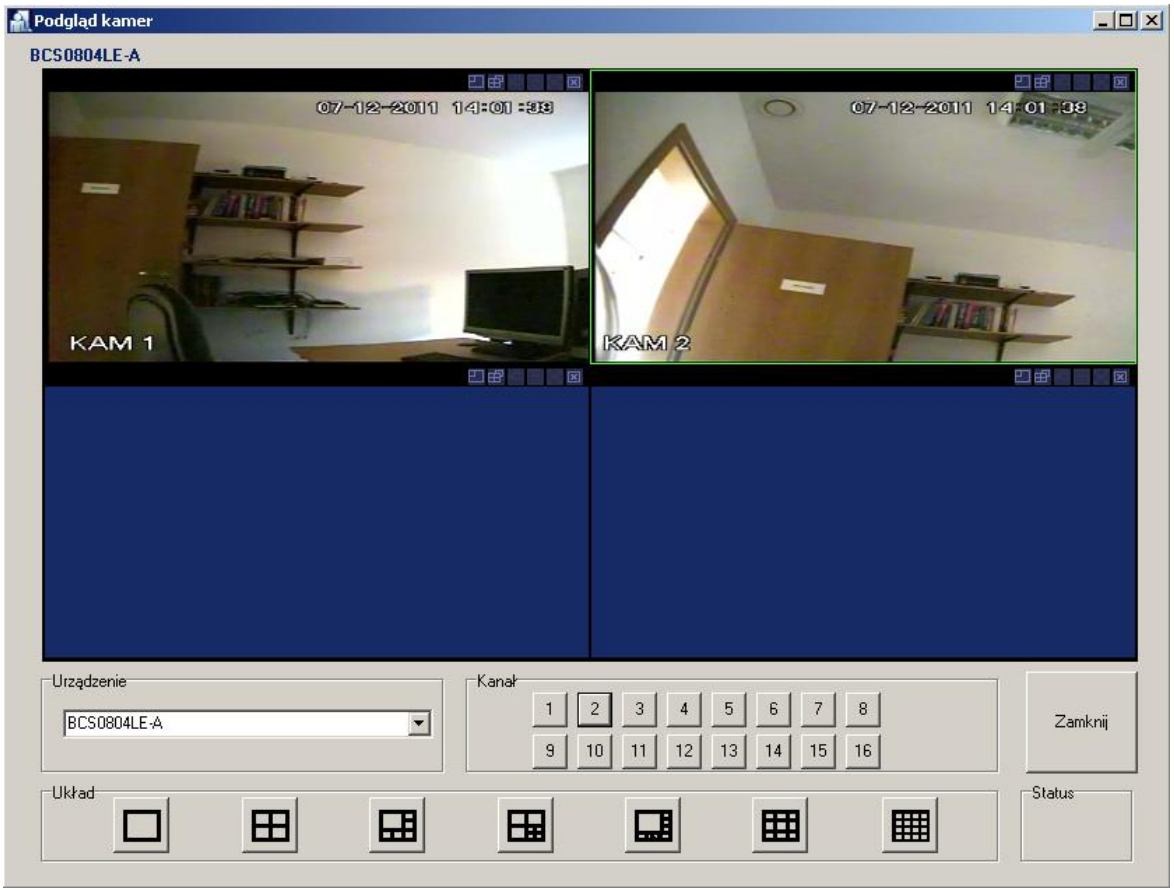
4.5. Przyciski Odtwórz nagranie CCTV oraz Podgląd kamer CCTV

4.5.1. Przycisk Odtwórz nagranie CCTV

Jeżeli skonfigurowana została integracja systemu RACS 4 z obsługiwanymi rejestratorami zgodnie z dedykowaną instrukcją dostępną na stronie **www.roger.pl** to dla określonych zdarzeń możliwe jest odtworzenie filmików zarejestrowanych przez wskazane kamery dla danego przejścia. Do tego celu służy przycisk **Odtwórz nagranie z CCTV**, po użyciu którego wyświetlane jest okno pokazane na rysunku 3.105. Ten przycisk jest dostępny również w Historii zdarzeń (patrz **punkt 3.3.7.2**). W otwartym oknie możliwe jest odtworzenie filmiku, zmiana jego przedziału czasowego jak również uzyskanie informacji na temat jego statusu. W przypadku karty rejestratora GV600/4 możliwe jest również wygenerowanie zdjęcia ze stopklatki poprzez kliknięcie prawym przyciskiem myszki obrazu oraz wybranie odpowiedniej opcji.

4.5.2. Przycisk Podgląd kamer CCTV

Jeżeli skonfigurowana została integracja systemu RACS 4 z obsługiwanymi rejestratorami zgodnie z **punktem 3.2.15** to za pomocą przycisku **Podgląd kamer z CCTV** można otworzyć okno do podglądu obrazu z kamer podłączonych do rejestratora. Przykładowe okno jest pokazane na rysunku 4.28.



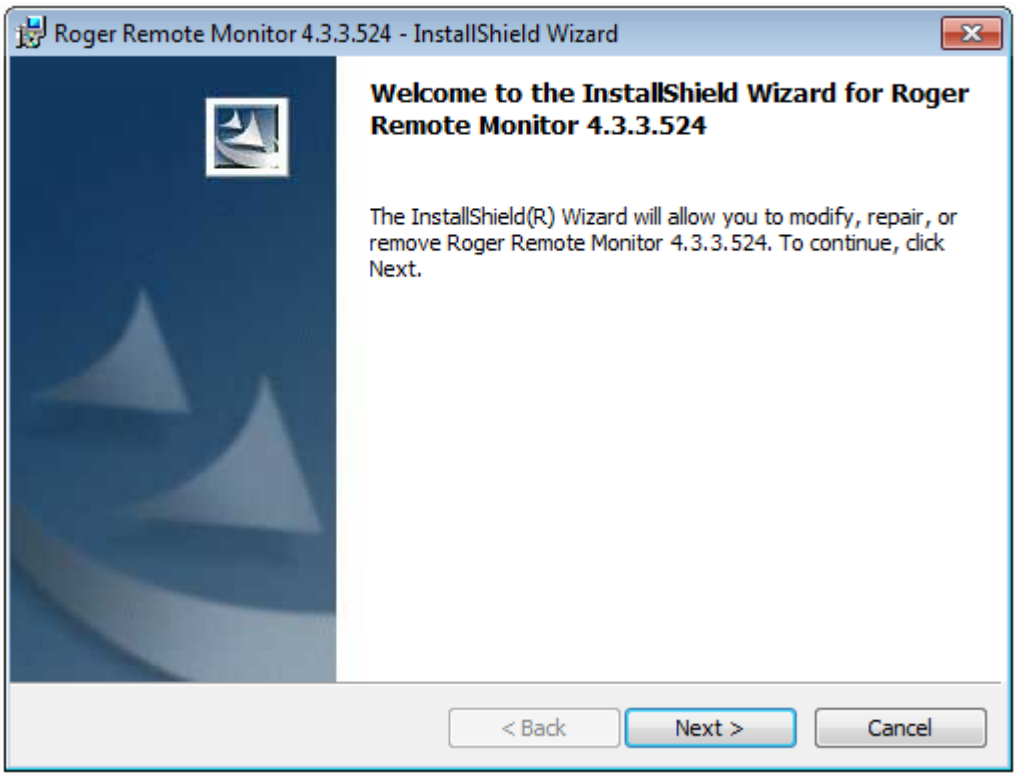
Rysunek 4.28. *Podgląd kamer*

ROZDZIAŁ 5.
OPROGRAMOWANIE REMOTE MONITOR

Program Remote Monitor po zainstalowaniu na komputerze i nawiązaniu połączenia z programem PR Master zainstalowanym na innym komputerze/serwerze umożliwia wykonywanie szeregu operacji w systemie RACS 4. Oznacza to, że Remote Monitor umożliwia wielostanowiskową obsługę systemu RACS 4 w pewnym ograniczonym zakresie funkcjonalnym. Do nawiązania i utrzymania połączenia konieczne jest by program PR Master był przez cały czas uruchomiony w trybie monitorowania.

Wersja instalacyjna programu Remote Monitor jest dostępna zainstalowaniu programu PR Master (domyślna lokalizacja to **C:\Roger\Access Control System 4.5\RemoteMonitorInstall**). Po wybraniu pliku w postaci **setup 4.5.20.xxxx** wyświetlone zostanie okno instalacji (rysunek 5.1). Dalsza instalacja programu odbywa się analogicznie do instalacji programu PR Master (patrz **punkt 1.1**).

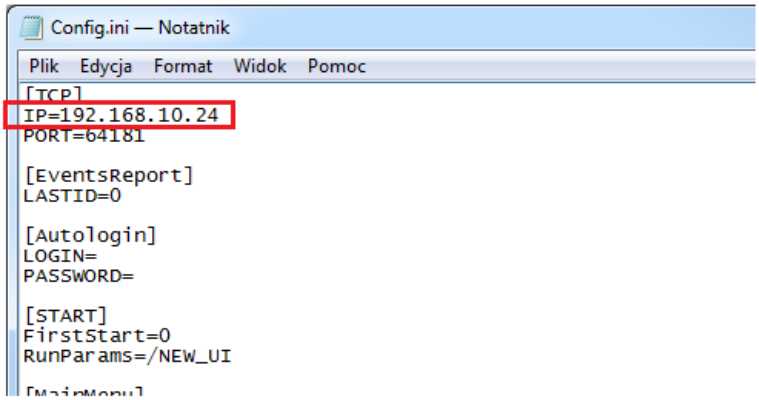
Począwszy od wersji 4.5.20.xxx program Remote Monitor nie jest już rozwijany przez firmę Roger i jest on oferowany w takim stanie jakim jest.



Rysunek 5.1. *Okno instalacji programu Remote Monitor*

5.1. PIERWSZE URUCHOMIENIE PROGRAMU

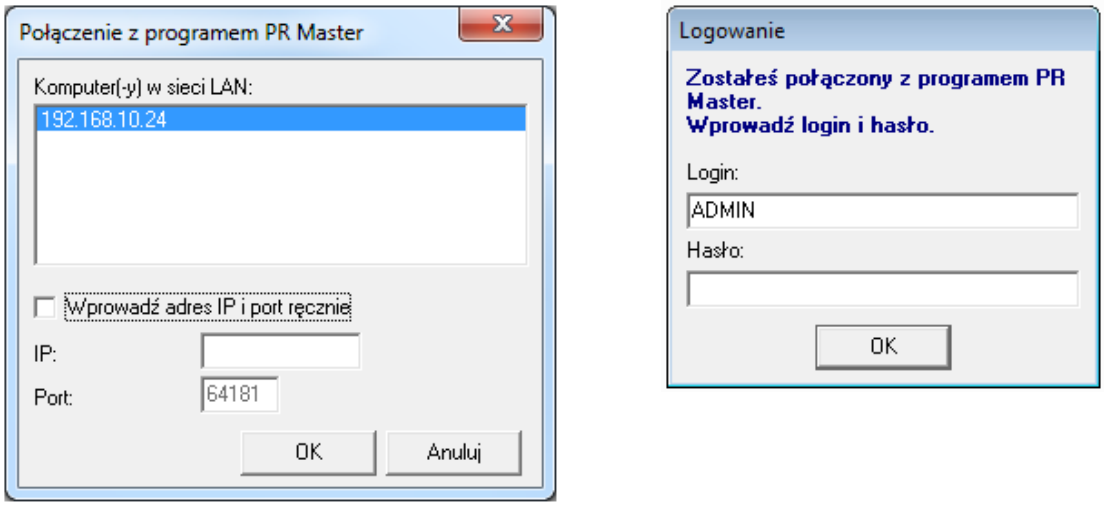
Przed uruchomieniem programu Remote Monitor konieczne jest otwarcie pliku config.ini w folderze programu PR Master – domyślna ścieżka **C:\Roger\Access Control System 4.5** a następnie wpisanie do niego adresu IP komputera na którym zainstalowany jest program PR Master. Przykład z adresem 192.168.10.24 pokazano rys. 5.2a.



Rysunek 5.2a. *Plik config.ini programu PR Master*

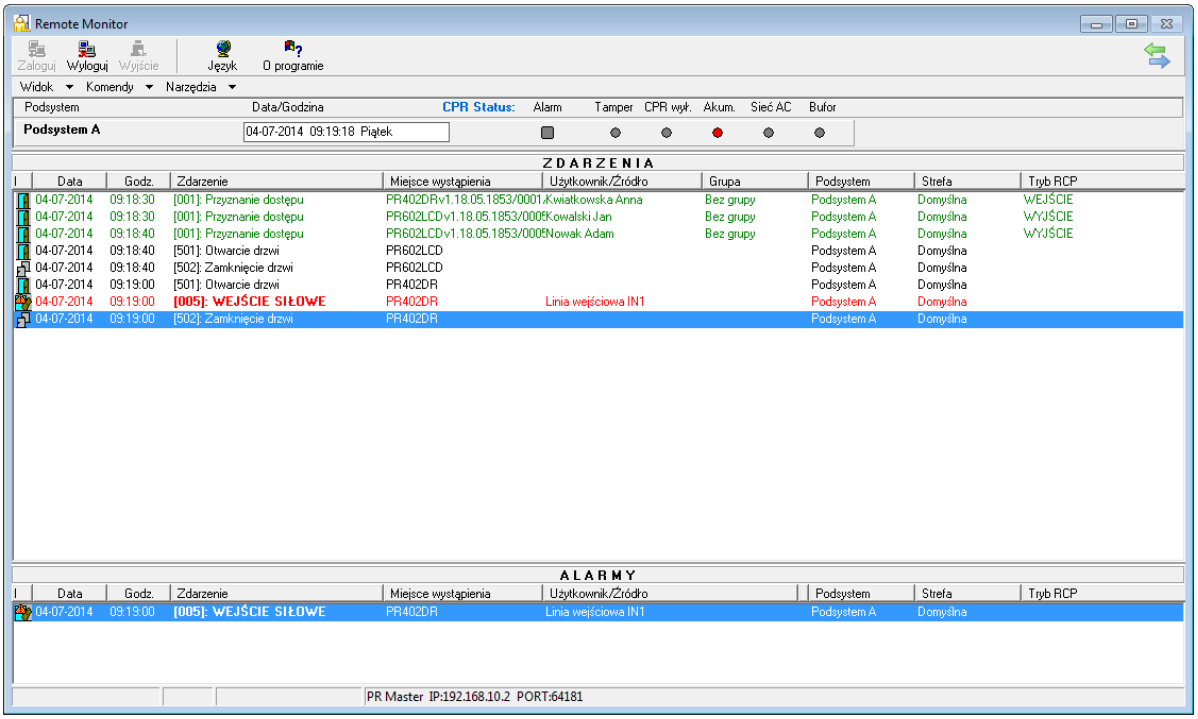
Po uruchomieniu programu w pierwszym kroku należy wybrać wersję językową i następnie nawiązać połączenie (rysunek 5.2b) wybierając z listy adres IP komputera z programem PR Master lub też wprowadzając ręcznie adres IP oraz port komputera z tym programem. Domyślny port to 64181. Zasadniczo program Remote Monitor został zaprojektowany do pracy w sieci lokalnej (LAN) aczkolwiek istnieje techniczna możliwość stosowania go w sieci rozległej (WAN).

Po nawiązaniu połączenia wyświetlane jest okno logowania do programu PR Master (rysunek 5.2). W przedstawionym oknie należy wprowadzić login oraz hasło operatora programu PR Master (patrz **punkt 3.5.8**). W przypadku domyślnych ustawień programu PR Master login to ADMIN a hasło jest puste. W ramach obsługi systemu RACS 4 zaleca się zdefiniowanie haseł operatorów programu PR Master.



Rysunek 5.2b. *Okno połączenia i logowania w Remote Monitor*

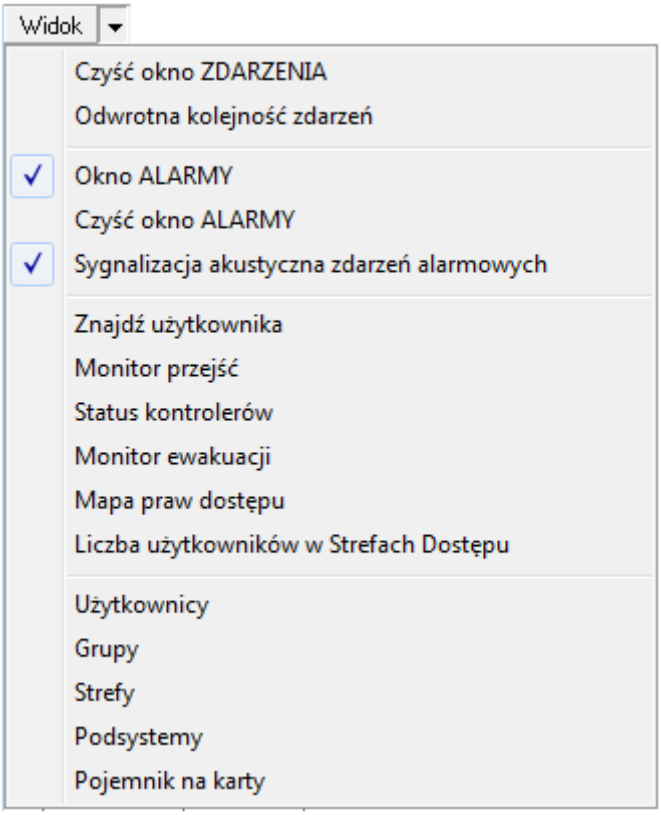
Po pomyślnym połączeniu oraz zalogowaniu wyświetlane jest okno główne programu Remote Monitor (rysunek 5.3), które jest wzorowane na oknie programu PR Master w trybie monitorowania (patrz **rozdział 4**). Umożliwia ona m.in. wyświetlanie na bieżąco zdarzeń zaistniałych w systemie RACS 4.



Rysunek 5.3. *Okno główne programu Remote Monitor*

5.2. MENU WIDOK

Menu **Widok** pokazano na rysunku 5.4.



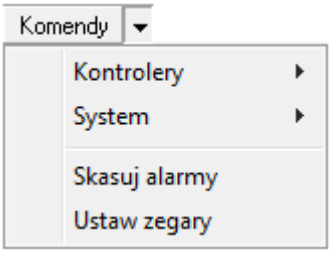
Rysunek 5.4. *Menu Widok programu Remote Monitor*

Menu **Widok** zawiera polecenia i narzędzia dostępne w menu **Widok** programu PR Master w trybie monitorowania. Zostały one już opisane w ramach niniejszego dokumentu (patrz **punkt 4.1**).

Dodatkowo za pomocą poleceń **Użytkownicy**, **Grupy**, **Strefy**, **Podsystemy** oraz **Pojemnik na kartę** możliwy jest odczyt odpowiednich danych z programu PR Master bez możliwości ich edytowania.

5.3. MENU KOMENDY

Menu **Komendy** pokazano na rysunku 5.5.

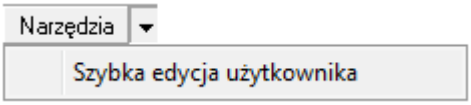


Rysunek 5.5. *Menu Komendy programu Remote Monitor*

Menu **Komendy** zawiera polecenia dostępne w menu **Komendy** programu PR Master w trybie monitorowania. Zostały one już opisane w ramach niniejszego dokumentu (patrz **punkt 4.2**).

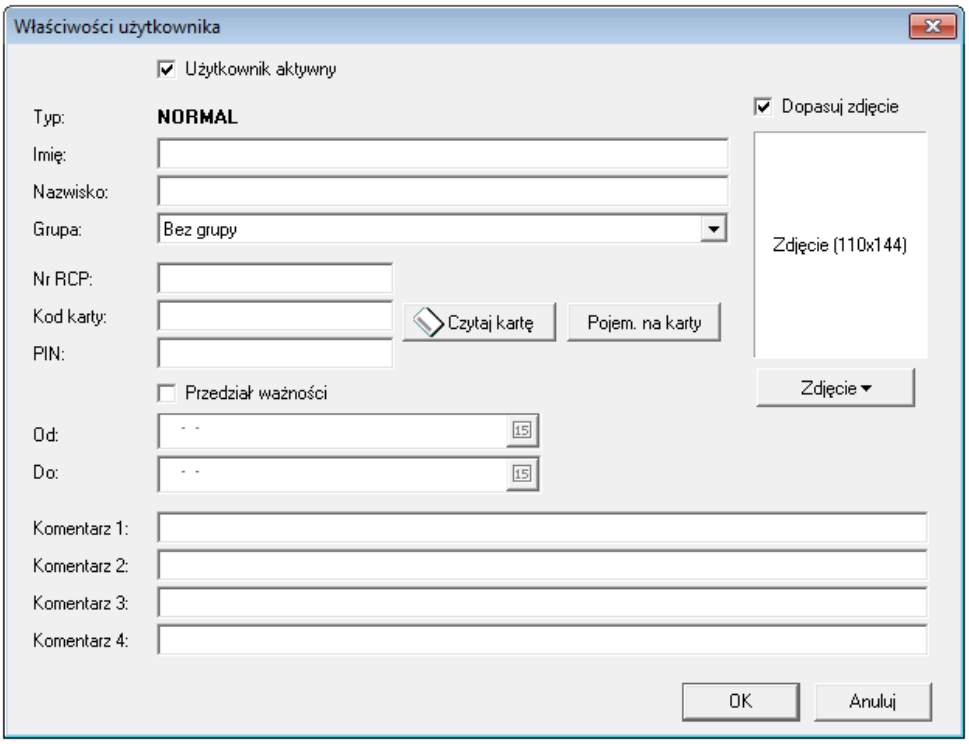
5.4. MENU NARZĘDZIA

Menu **Narzędzia** pokazano na rysunku 5.6.



Rysunek 5.6. *Menu Narzędzia programu Remote Monitor*

Menu **Narzędzia** zawiera polecenie umożliwiające dodawanie i edytowanie użytkowników w systemie RACS 4. Obsługa użytkowników jest realizowana w sposób analogiczny do tego, który jest możliwy w programie PR Master (patrz **punkty 3.2.3** oraz **3.5.2**). Okno dodawania użytkownika za pomocą programu Remote Monitor pokazano na rysunku 5.7. Program Remote Monitor obsługuje jedynie czytniki typu RUD-2 i RUD-3, które podłącza się do portu USB komputera. Odczyt numeru karty za pomocą takiego czytnika jest możliwy po wybraniu przycisku **Czytaj kartę**. Alternatywnie dodawanie kart można również realizować za pośrednictwem pojemnika na karty.



Rysunek 5.7. *Dodawanie użytkownika w Remote Monitor*

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: pomoc.techniczna@roger.pl
Web: www.roger.pl