Roger Access Control System

Opis funkcjonalny kontrolerów serii PRxx2

Oprogramowanie wbudowane: x.18.8. lub nowsze

Wersja dokumentu: Rev. I

Dokument dotyczy następujących typów urządzeń:
PR102DR, PR402DR, PR402DR-BRD, PR402-BRD, PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302

CE

Spis treści:

I. DEFINICJE I KONWENCJE

1.1 Stosowane pojęcia

Kontroler dostępu (ang. ACU – Access Control Unit)	Urządzenie logiczne najczęściej mikroprocesorowe, którego zadaniem jest elektroniczna weryfikacja osób i sterowanie dostępem do pomieszczenia.
Zintegrowany system kontroli dostępu (ang. IACS – Integrated Access Control System)	System kontroli dostępu złożony z wielu kontrolerów połączonych ze sobą magistralą komunikacyjną, która umożliwia monitorowanie systemu w trybie online a także realizację pewnych złożonych funkcji sterowania wymagających wymiany informacji pomiędzy urządzeniami podłączonymi do magistrali.
System kontroli dostępu RACS (ang. RACS - Roger Access Control System)	System kontroli dostępu składający się z kontrolerów dostępu serii PR (ROGER) i zarządzanych przez program PR Master (ROGER).
Centrala systemu KD	Specjalizowany kontroler pełniący pewne funkcje zarządzające w Zintegrowanym Systemie Kontroli Dostępu (ang. IACS). Funkcja centrali KD zależy od tego, z jakimi urządzeniami ono współpracuje. W odniesieniu do kontrolerów serii PRxx1 centrala (CPR32-SE/CPR32-NET) pełni rolę zewnętrznego bufora zdarzeń jak również zarządza funkcjami czasowymi (np. Harmonogramami dostępu). W odniesieniu do rodziny kontrolerów serii PRxx2 centrala pełni funkcję urządzenia nadrzędnego realizującego funkcje o charakterze globalnym jak np. globalny anti-passback (Strefy APB) czy sterowanie stanem uzbrojenia kontrolerów w ramach Stref Alarmowych.
Urządzenie nadrzędne (ang. host)	Urządzenie pełniące rolę nadrzędną w stosunku do kontrolerów dostępu. Funkcję urządzenia nadrzędnego może pełnić dedykowany do tego celu kontroler, centrala CPR32-SE/CPR32-NET lub komputer PC wraz z programem zarządzającym.
Interfejs RACS CLK/DTA	Interfejs elektryczny, który umożliwia wymianę informacji za pośrednictwem sygnałów na liniach CLK i DTA. System RACS wykorzystuje własny protokół transmisji danych, który dla odróżnienia od innych standardów tego typu jest oznaczany jako RACS CLK/DTA. Standard RACS CLK/DTA jest protokołem adresowalnym (adresy ID=0-15) i umożliwia transmisję danych na odległość do 150m przy wykorzystaniu dowolnych kabli sygnałowych.
Magistrala komunikacyjna	Struktura elektryczna złożona z dwóch przewodów elektrycznych, która jest wykorzystywana do komunikacji pomiędzy różnymi podłączonymi do niej urządzeniami. System RACS wykorzystuje magistralę RS485.
Tryb Drzwi	Sposób sterowania elementem wykonawczym odpowiedzialnym za blokowanie/odblokowywanie drzwi. Kontroler PRxx1 udostępnia następujące Tryby Drzwi: Normalny, Odblokowane, Warunkowo Odblokowane oraz Zablokowane.
Element wykonawczy lub zamek drzwiowy	Urządzenie elektryczne, które zwalnia drzwi umożliwiając dostęp do kontrolowanego pomieszczenia bądź obszaru. Zwykle jest to elektro-zaczep lub zwora magnetyczna.

Kod Obiektu (ang. Facility Code)	Charakterystyczna część kodu karty, która wskazuje, że dana karta pochodzi z pewnej grupy kart wyprodukowanych bądź zaprogramowanych dla konkretnego systemu. Karty z kodem obiektu są zwykle stosowane przez odbiorców o charakterze korporacyjnym lub instytucjonalnym (np. sieci sklepów, banki, instytucje o zasięgu ogólnokrajowym) albo w instalacjach KD gdzie występuje duża ilość użytkowników, lecz nie zachodzi potrzeba rozpoznawania, do jakiego konkretnie użytkownika dana karta należy (osiedla mieszkaniowe, kampusy uniwersyteckie itp.).
Identyfikator	Element fizyczny lub metoda, którą stosuje osoba w celu identyfikacji. Identyfikatorem może być karta zbliżeniowa, kod PIN, odcisk linii papilarnych, itp. W niektórych przypadkach identyfikator może się składać z dwóch lub większej liczby składników i wtedy wszystkie te elementy są wymagane do pomyślnej identyfikacji. NA przykład tryb Karta i PIN oznacza, że Identyfikator = Karta + PIN.
Logowanie	Proces identyfikacji użytkownika na podstawie jego identyfikatora (karty, kodu PIN, linii papilarnych itp.)
Tryb Identyfikacji	Metoda stosowana przez kontroler w celu identyfikacji użytkownika. Kontroler PRxx1 udostępnia następujące Tryby Identyfikacji: Karta i PIN, Karta lub PIN, Tylko Karta oraz Tylko PIN.
Tryb bistabilny (zatrzask)	Tryb bistabilny (zatrzask) odnosi się do sytuacji, kiedy jakiś element (np. linia wyjściowa) zmienia swój stan na przeciwny do momentu kiedy jakieś inne zdarzenie nie przywróci stanu poprzedniego.
Tryb monostabilny (chwilowy)	Tryb monostabilny odnosi się do sytuacji, kiedy jakiś element (np. linia wyjściowa) zmienia swój stan na przeciwny, a po upływie określonego czasu samoczynnie powraca do stanu poprzedniego.
Reset pamięci	Proces polegający na wyzerowaniu aktualnej zawartości pamięci urządzenia i zapisaniu jej wartościami domyślnym (fabrycznymi).
Czytniki serii PRT	Rodzina czytników skonstruowanych i produkowanych przez firmę ROGER. Każdy z czytników serii PRT może być dołączony do kontrolera PRxx1 za pośrednictwem interfejsu CLK/DTA.
Restart	Proces polegający na zainicjowaniu pracy urządzenia na identycznych zasadach jak to ma miejsce po załączeniu zasilania.
RS485	Standard transmisji szeregowej. Standard precyzuje warstwę elektryczną, lecz nie odnosi się do warstwy protokołu.
Tryb Autonomiczny	Konfiguracja, w której kontroler działa bez fizycznego połączenia z jakimkolwiek urządzeniem nadrzędnym lub kontroler jest podłączony do komputera PC jedynie po to by umożliwić jego zaprogramowanie.
Tryb Sieciowy	Konfiguracja, w której kontrolery połączone magistralą komunikacyjną wymieniają dane za pośrednictwem urządzenia nadrzędnego i tworzą system sieciowy. Warunkiem koniecznym pracy systemu RACS w Trybie Sieciowym jest zastosowanie centrali CPR32-SE/CPR32-NET. Do konfigurowania i zarządzania systemem sieciowym wymagane jest podłączenie komputera PC z

	oprogramowaniem PR Master.
Flagi Systemowe	Stany logiczne w pamięci kontrolera, które reprezentują pewne określone zjawiska lub stany urządzenia.
Licznik, Tajmer (ang. Timer)	Funkcja, która służy do odmierzania czasu. Liczniki mogą być stosowane w odniesieniu do różnych elementów logiki kontrolera, np. linii wyjściowych, zwłok czasowych, itp.
Ekspandery	Moduły elektroniczne dołączane do urządzenia w celu rozszerzenia jego możliwości i funkcjonalności.
Strefa Alarmowa	Jest to wybrany obszar systemu kontroli dostępu obejmujący grupę kontrolerów współbieżnie zmieniających swój aktualny stan uzbrojenia/rozbrojenia.
Strefa anti-passback (Strefa APB)	Jest to wybrany obszar systemu kontroli dostępu, do którego dostęp jest nadzorowany przez wiele punktów identyfikacji (czytników). Użytkownik jest zmuszony do naprzemiennej identyfikacji na wejściu i wyjściu ze strefy APB.

1.2 Przyjęta konwencja

Funkcje, opcje oraz komendy RACS	pisane czcionką pogrubioną
Przykłady	pisane kursywą
Pojęcia Własne systemu RACS 4	pisane z wielkiej litery
STANY, FLAGI I LICZNIKI	pisane kapitalikami
Uwagi	oddzielone od reszty tekstu liniami z góry i dołu

II. CHARAKTERYSTYKA OGÓLNA

2.1 Wstęp

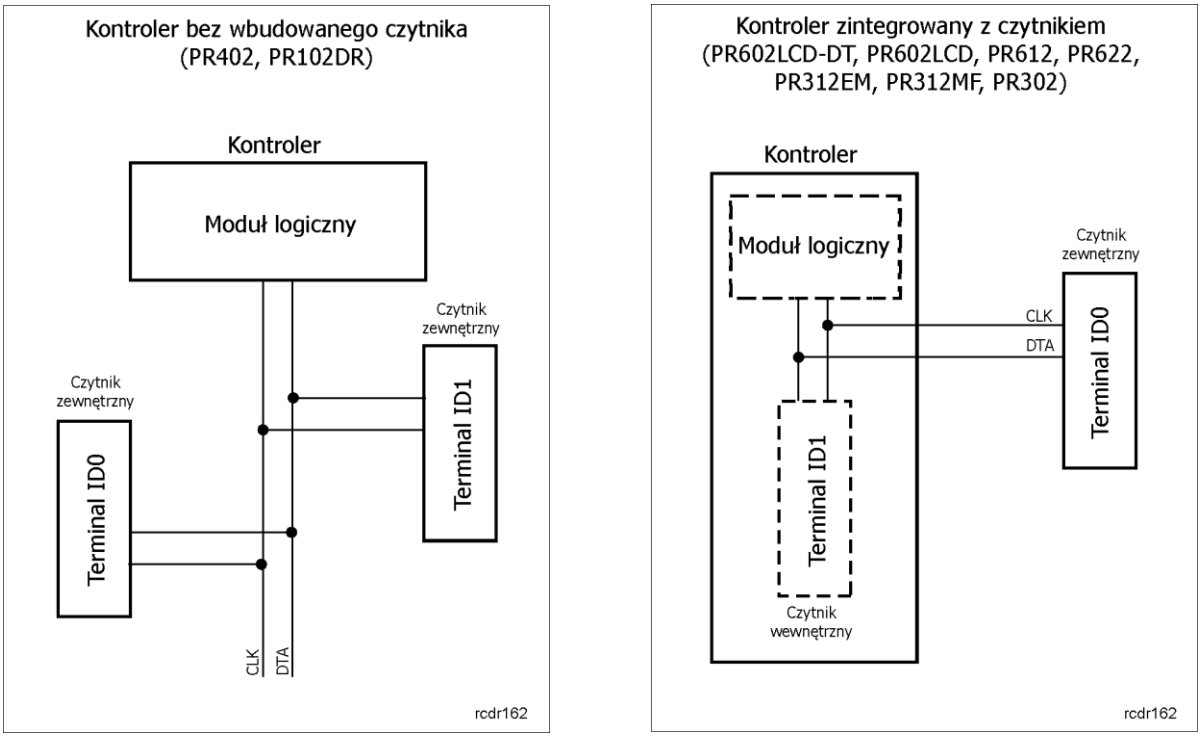
Niniejsza instrukcja dotyczy kontrolerów serii PRxx2 i obejmuje ona zarówno kontrolery z wbudowanym czytnikiem kart EM125kHz (PR602LCD, PR612, PR622, PR312EM i PR302), z wbudowanym czytnikiem kart MIFARE® (PR312MF), z dwusystemowym czytnikiem kart EM125kHz/MIFARE (PR602LCD-DT) jak i kontrolery bez wbudowanego czytnika do montażu w obudowie metalowej z dala od drzwi (PR102DR, PR402DR, PR402-BRD). Kontroler PR402-BRD w postaci modułu elektronicznego został wycofywany z produkcji a jego następcą jest kontroler PR402DR dostępny zarówno w obudowie z tworzywa sztucznego do montażu na szynie DIN 35mm (PR402DR) jak i w postaci modułu elektronicznego (PR402DR-BRD). Obie wersje kontrolerów PR402DR są również dostępne w wersji dostosowanej jedynie do zasilania 12VDC. Stosowane w niniejszej instrukcji określenie PR402 odnosi się do wszystkich możliwych wersji PR402 (wycofanych i nowych), natomiast określenie PR402DR dotyczy wszystkich czterech dostępnych wersji tego kontrolera. Kontroler PR102DR to ekonomiczny i uproszczony sprzętowo kontroler powstały na bazie popularnego kontrolera PR402DR. PR102DR podobnie jak PR402DR jest dostępny zarówno w obudowie z tworzywa sztucznego do montażu na szynie DIN 35mm (PR102DR) jak i w postaci modułu elektronicznego (PR102DR-BRD). W niniejszej instrukcji określenie PR102DR dotyczy wszystkich wersji tego kontrolera. Kontroler PR602LCD-DT zastępuje wycofany z produkcji kontroler PR602LCD.

Niniejsza instrukcja opisuje przede wszystkim funkcje i opcje kontrolerów PRxx2, które konfiguruje się z poziomu oprogramowania PR Master. Zawiera ona również informacje na temat architektury, komunikacji i trybów pracy. Dane, które są niezbędne do instalacji urządzeń podane są w instrukcjach poszczególnych kontrolerów, natomiast informacje dotyczące całościowej obsługi oprogramowania PR Master (w tym ustawienia harmonogramów, Grup Dostępu, Stref Dostępu, Trybu Monitorowania, Historii Zdarzeń, itd.) podane są w instrukcji tego właśnie programu.

2.2 Budowa i przeznaczenie

Kontrolery serii PRxx2 są kontrolerami dostępu przeznaczonymi do dozoru jednego przejścia, przy czym może ono być kontrolowane po jednej lub po dwóch stronach. Kontroler serii PRxx2 obsługuje logicznie dwa punkty identyfikacji (czytniki) zwane odpowiednio Terminalem ID0 oraz Terminalem ID1. Czytniki wbudowane w kontrolery PR602LCD, PR602LCD-DT, PR612, PR622, PR312EM, PR312MF i PR302 są logicznie traktowane jako Terminal ID1, natomiast kontrolery PR402 i PR102DR nie posiadają wbudowanego czytnika i współpracują wyłącznie z czytnikami zewnętrznymi. Czytniki zewnętrzne podłączane do kontrolerów serii PRxx2 mogą pracować w formacie RACS CLK/DTA (terminale serii PRT firmy ROGER), Wiegand 26-66bit lub Magstripe. Kontroler PR602LCD-DT jest wyposażony w klawiaturę oraz wyświetlacz LCD i jest on zalecany jako terminal do rozliczania czasu pracy (RCP) – patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master.

Kontrolery serii PRxx2 w odróżnieniu od kontrolerów serii PRxx1 posiadają wbudowaną pamięć zdarzeń oraz zegar czasu rzeczywistego. Oznacza to, że do realizacji ogólnie pojętych funkcji czasowych oraz rejestrowania zdarzeń nie wymagają centrali serii CPR. Bufor pamięci w kontrolerach PRxx2 potrafi zapamiętać 32 000 zdarzeń. Centrala serii CPR może natomiast być wykorzystana do realizacji takich funkcji globalnych jak Globalny Anti-passback czy Strefy Alarmowe (3.11 Antypowrót (ang. Anti-passback) oraz 3.12 Strefy Alarmowe). Dodatkowo centrala CPR32-NET umożliwia integrację z centralami alarmowymi serii INTEGRA (SATEL) oraz zamkami bezprzewodowymi systemu SALLIS (SALTO) oraz 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.



Rys. 1 Ogólna koncepcja współpracy kontrolera z czytnikami

W kontrolerze PRxx2 można zarejestrować do 4000 użytkowników. W systemie RACS 4 każdy użytkownik posiada swój unikalny numer ID oraz może posiadać kartę i/lub kod PIN.
Przesyłanie oprogramowania do kontrolera odbywa się za pośrednictwem magistrali komunikacyjnej RS485 i nie wymaga demontażu urządzenia z miejsca jego zainstalowania.
Kontrolery serii PRxx2 mogą działać samodzielnie (Tryb autonomiczny Offline i Online) lub być elementem zintegrowanego systemu kontroli dostępu (Tryb Sieciowy).
Kontrolery PRxx2 programuje się z poziomu komputera, nie ma możliwości ich programowania manualnego aczkolwiek istnieje zestaw komend i poleceń, które można wprowadzać do kontrolera lokalnie z poziomu klawiatury. Te polecenia służą głównie do sterowania jego pracą a nie do programowania (patrz 3.18 Komendy z klawiatury). Programowanie zdalne przeprowadza się z poziomu komputera PC z zainstalowanym programem zarządzającym PR Master (ROGER).
Komunikacja z pojedynczymi kontrolerami jak też zarządzanie systemem KD wymaga zastosowania centrali CPR32-NET albo sprzętowego interfejsu komunikacyjnego takiego jak:

- UT-4 lub UT-4DR (Ethernet <-> RS485)
- UT-2USB lub RCI-2 (USB <-> RS485)
- UT-2 (RS-232 <-> RS485)
- RUD-1 (USB <-> RS485)

Tabela 1. Zestawienie kontrolerów serii PRxx2								
Kontroler	Zasilanie	Wejścia NO/NC	Wyjścia tranzyst.	Wyjścia przekaźnikowe	Wbudowany czytnik	Czytniki zewnętrzne	Klawiatura na obudowie	Inne
PR402DR/ PR402DR-BRD	12VDC, 24VDC, 18VAC	8	2	1 x 1.5A/30V, 1 x 5A/30VDC lub też 5A/230VAC	nie	2 x PRT, Wiegand lub Magstripe	nie	- w obudowie DIN 35mm (PR402DR) lub moduł elektroniczny (PR402DR-BRD), - wbudowany zasilacz 1.2A/12VDC, - bezpośrednie podłączenie akumulatora.
PR402DR-12VDC/ PR402DR-BRD-12VDC	12VDC	jw.	jw.	jw.	jw.	jw.	jw.	jw.
PR402-BRD	12VDC, 18VAC	4	jw.	2 x 5A/30VDC lub też 5A/230VAC	jw.	jw.	jw.	- moduł elektroniczny, - wbudowany zasilacz 1.2A/12VDC, - bezpośrednie podłączenie akumulatora.
PR102DR/ PR102DR-BRD	12VDC	2	1	1 x 1.5A/30V	nie	2 x PRT	nie	- w obudowie do montażu na szynie DIN 35mm (PR102DR) lub jako moduł elektroniczny (PR102DR-BRD).
PR602LCD-DT	12VDC	3	2	1 x 1.5A/30V	EM125kHz i MIFARE	1 x PRT, Wiegand lub Magstripe	tak, w tym 4 klawisze funk.	- wersje do pracy w warunkach zewn. oraz wewnętrznych, - wyświetlacz LCD.
PR602LCD	Jw.	Jw.	Jw.	jw.	EM125kHz	jw.	jw.	jw.
PR612	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	tak	- praca w warunkach zewnętrznych, - zaciski śrubowe.
PR622	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	nie	jw.
PR312EM	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	tak, w tym 2 klawisze funk.	- praca w warunkach zewnętrznych, - kabel podłączeniowy, - dostępna wersja bez klawiatury.
PR312MF	jw.	jw.	jw.	jw.	MIFARE	jw.	jw.	jw.
PR302	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT lub Wiegand	tak	- praca w warunkach wewnętrznych, - zaciski śrubowe, - możliwość przezbrojenia do wersji bez klawiatury.

2.3 Skrócona charakterystyka kontrolerów serii PRxx2

Cechy kontrolerów serii zaawansowanej PRxx2:

- Jednostronna lub dwustronna kontrola jednego przejścia
- Współpraca z czytnikami serii PRT (ROGER)
- Współpraca z czytnikami Magstripe oraz Wiegand różnych producentów (PR402, PR602LCD-DT, PR602LCD i PR302)
- Praca autonomiczna lub w zintegrowanym systemie sieciowym
- Zegar czasu rzeczywistego (RTC) z podtrzymaniem bateryjnym
- Programowalne linie wejściowe i wyjściowe
- Możliwość montażu na szynie DIN 35mm (wyłącznie PR402DR i PR102DR)
- Współpraca z ekspanderem WE/WY XM-2
- Kontrola dostępu w windach (maks. 32 piętra, wymaga ekspanderów XM-8)
- Możliwość aktualizacji oprogramowania wbudowanego (firmware)
- Interfejs komunikacyjny RS485
- Zarządzanie systemem przez sieć komputerową LAN/WAN (wymagana centrala CPR32-NET lub interfejs UT-4DR albo UT-4)
- Oprogramowanie zarządzające PR Master (Windows XP i nowsze)
- Integracja z systemami alarmowymi za pośrednictwem linii we/wy z wykorzystaniem Stref Alarmowych (maks. 32 strefy w systemie)
- Integracja z systemami telewizji przemysłowej (CCTV)
- Identyfikacja użytkownika za pomocą karty i/lub kodu PIN
- Nieulotny bufor 32.000 zdarzeń (FIFO)
- 4000 użytkowników
- 250 grup dostępu
- 99 harmonogramów czasowych ogólnego przeznaczenia
- 128 przedziałów czasowych w ramach pojedynczego harmonogramu
- 4 Harmonogramy Świąteczne (H1-H4)
- Definiowanie przedziału czasowego ważności karty użytkownika
- Definiowanie maksymalnej ilości logowań danego użytkownika (limit jednorazowy oraz odnawialny)
- Wejście Komisyjne (wymaga dwóch użytkowników)
- Dostęp Warunkowy (o ile jest już ktoś z środku)
- Tryb High Security (konieczność identyfikacji na dwóch czytnikach)
- Losowe wyznaczanie osób do rewizji
- Anti-passback Lokalny (dla jednego przejścia)
- Anti-passback Globalny (dla grup przejść, wymaga centrali CPR32-SE lub CPR32-NET)
- Rejestracja zdarzeń dla celów rejestracji czasu pracy (RCP)
- Znak CE

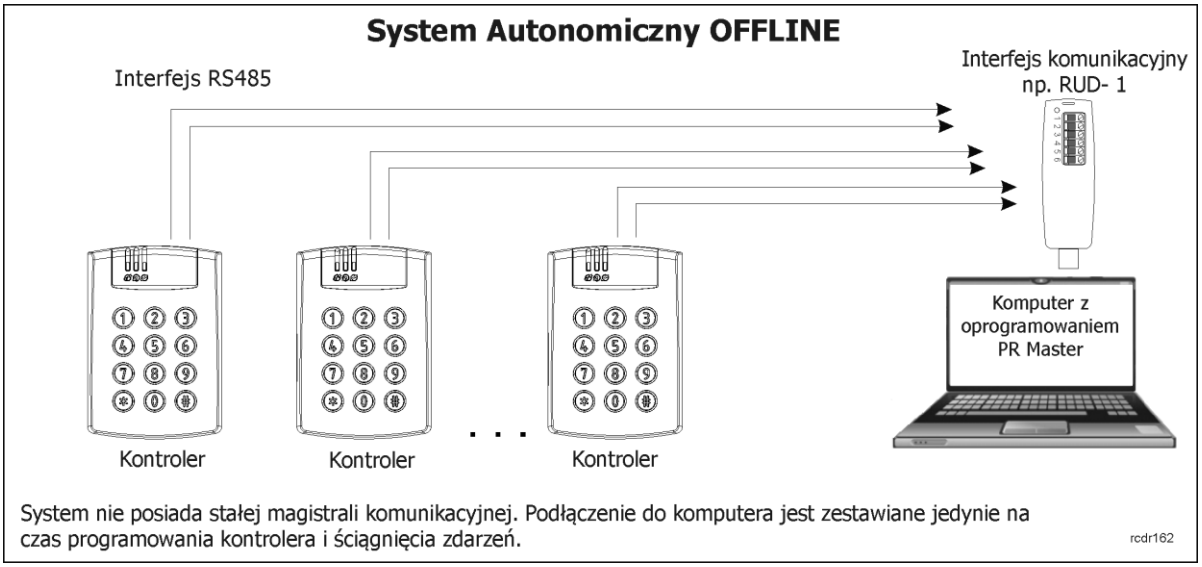
III OPIS FUNKCJONALNY

3.1 Tryby pracy kontrolerów serii PRxx2

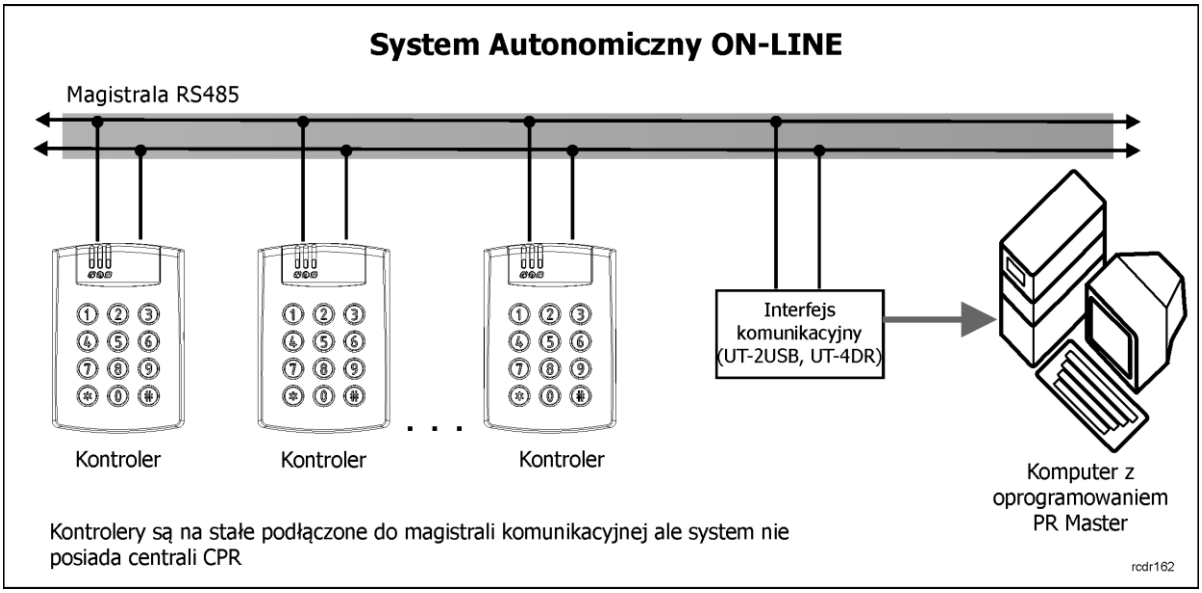
3.1.1 Praca w Trybie Autonomicznym

W trybie autonomicznym kontrolery PRxx2 działają samodzielnie i nie wymieniają informacji z innymi urządzeniami wchodzącymi w skład systemu. W trybie autonomicznym zdarzenia są rejestrowane i zapisywane w wewnętrznej pamięci kontrolera. Wszystkie funkcje czasowe są sterowane przez wewnętrzny zegar kontrolera. Podłączenie do magistrali RS485 jest potrzebne tylko na czas programowania i ściągnięcia historii zdarzeń. Nie ma potrzeby zachowywania stałego połączenia z komputerem (oprogramowaniem PR Master), ale można je zapewnić w celu łatwiejszej konfiguracji czy też ściągania zdarzeń w razie potrzeby. W tym trybie nie są dostępne żadne funkcje o charakterze globalnym (Strefy APB, Strefy Alarmowe). System Autonomiczny Offline to system oddzielnych kontrolerów niepodłączonych do wspólnej magistrali komunikacyjnej RS485. Muszą one być konfigurowane oddzielnie poprzez tymczasowe podłączenie z udziałem sprzętowego interfejsu komunikacyjnego. System Autonomiczny Online z kolei obejmuje kontrolery podłączone do wspólnej magistrali RS485 w celu ich łatwiejszego programowania i ściągania zdarzeń. Nie jest to system sieciowy bo magistrala RS485 w takim układzie służy jedynie do zarządzania kontrolerami.

Uwaga: Ze względu na to, że kontroler PRxx2 nie może być programowany manualnie, przed przekazaniem go do użytkowania należy go podłączyć do komputera poprzez interfejs komunikacyjny albo centralę CPR32-NET i odpowiednio skonfigurować jego adres. Nowy fabrycznie kontroler posiada adres ID=0. Podłączenie dwóch lub więcej kontrolerów o tym samym adresie na magistrali RS485 skutkuje konfliktem komunikacyjnym (patrz 3.2.2 Adresy kontrolerów).



Rys. 2 Praca w Trybie Autonomicznym (Offline)



Rys. 3 Praca w Trybie Autonomicznym (Online)

3.1.2 Praca w Trybie Sieciowym (z centralą CPR)

Gdy system kontroli dostępu posiada magistralę komunikacyjną RS485 i jest ona wykorzystywana do wymiany danych pomiędzy podłączonymi do niej urządzeniami to taki system nosi nazwę Sieciowego Systemu Kontroli Dostępu. W systemie RACS 4 warunkiem koniecznym systemu sieciowego jest obecność w nim centrali CPR32-SE lub CPR32-NET. Stosowanie Trybu Sieciowego jest szczególnie wskazane, gdy użytkownik chce skorzystać z takich funkcji globalnych jak Strefy Alarmowe czy Globalny Anti-passback lub też chce wykorzystać nowe możliwości centrali CPR32-NET.

Uwaga: Samo wykorzystywanie magistrali RS485 nie rozstrzyga tego czy jest to system sieciowy czy nie. Jeśli uszkodzenie lub brak magistrali RS485 nie powoduje zaniku żadnych funkcji systemu to taki system nie jest systemem sieciowym. Dla przykładu, jeśli magistrala RS485 jest używana tylko do programowania kontrolerów i ściągania zdarzeń to taki system jest systemem autonomicznym online ze sztywnym łączem komunikacyjnym do komputera zarządzającego.

W przypadku kontrolerów serii PRxx2 obecność centrali CPR32-SE lub CPR32-NET pozwala uzyskać następujące funkcjonalności:

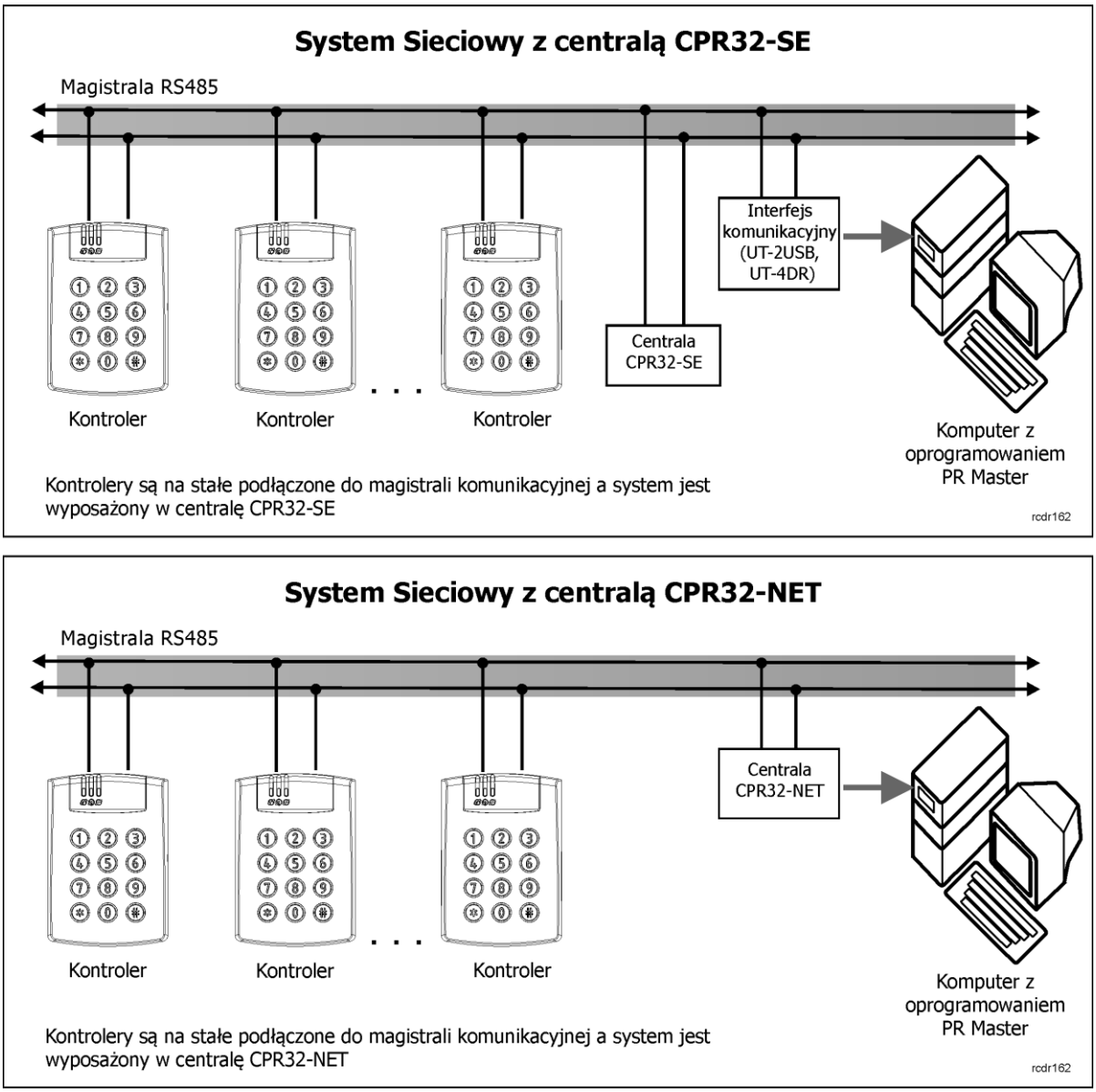
- ciągłe ściąganie zdarzeń z wewnętrznych buforów pamięci kontrolerów PRxx2 i zapisywanie ich w centralnym buforze centrali (250 000 tys.),
- możliwość definiowania Globalnego APB (patrz 3.11 Antypowrót (ang. Anti-passback)),
- możliwość definiowania Stref Alarmowych (patrz 3.12 Strefy Alarmowe),
- synchronizacja czasów i dat w kontrolerach z zegarem centrali CPR.

Dodatkowo centrala CPR32-NET umożliwia:

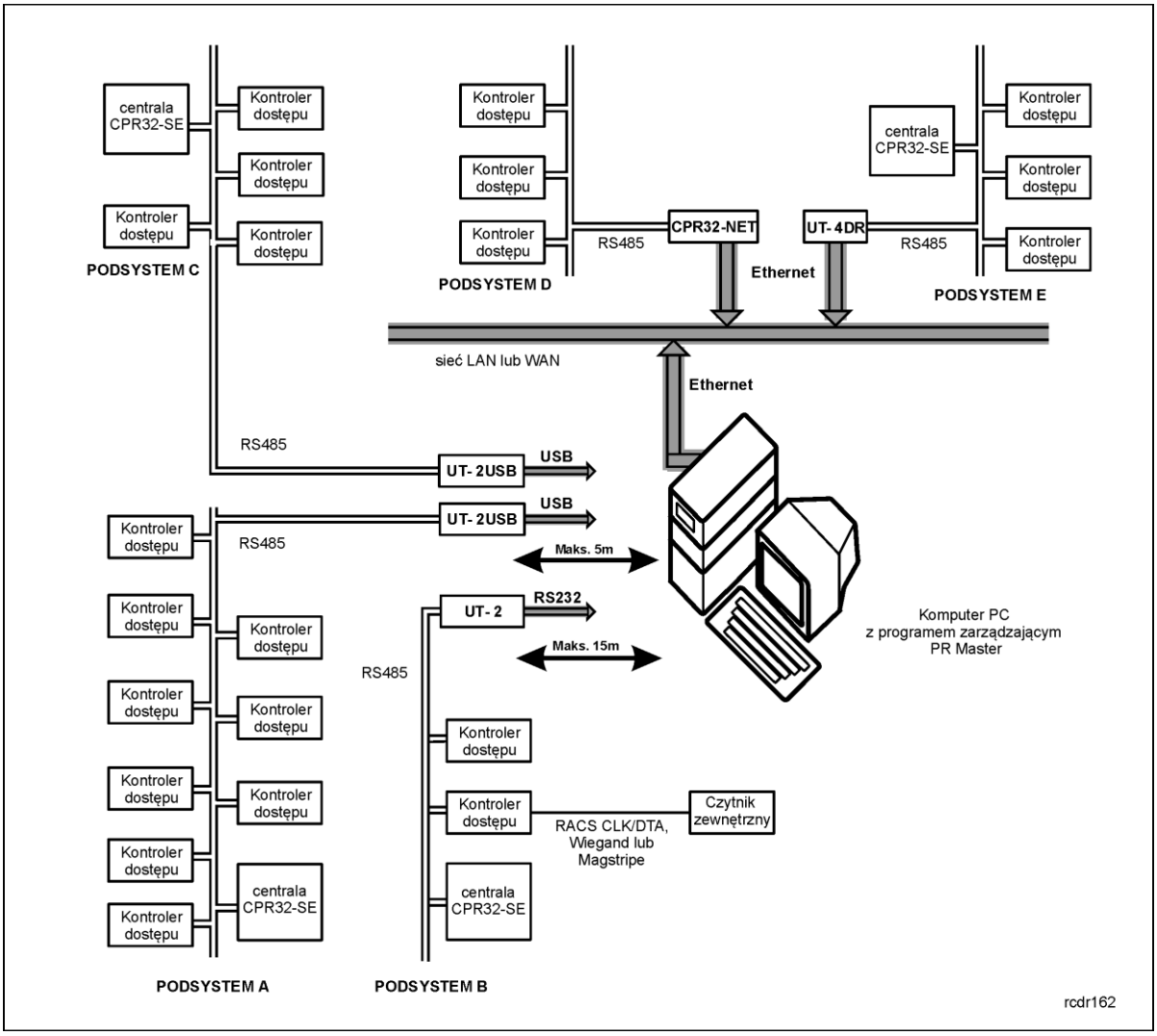
- Programową integrację z centralą alarmową INTEGRA (SATEL) oraz zamkami bezprzewodowymi systemu SALLIS (SALTO) lub APERIO (ASSA ABLOY)
- Wbudowany interfejs komunikacyjny Ethernet-RS485
- Bufor zdarzeń na opcjonalnej karcie pamięci AX-9 (33 milionów)
- Szyfrowanie komunikacji w oparciu o standard AES128 CBC
- Synchronizacja z serwerami czasu NTP

W przypadku awarii centrali CPR system kontroli dostępu automatycznie przełącza się do Trybu Autonomicznego Online i działa w tym trybie dopóki komunikacja z centralą CPR nie zostanie przywrócona. W przypadku takiej awarii system kontroli dostępu nadal działa prawidłowo tj.

rozpoznaje użytkowników i zna ich prawa dostępu, prawidłowo otwiera drzwi i zapisuje zdarzenia w buforach wewnętrznych kontrolerów.



Rys. 4 Praca w Trybie Sieciowym (z centralą CPR)



Rys. 5 Przykładowy schemat architektury systemu RACS 4 w Trybie Sieciowym

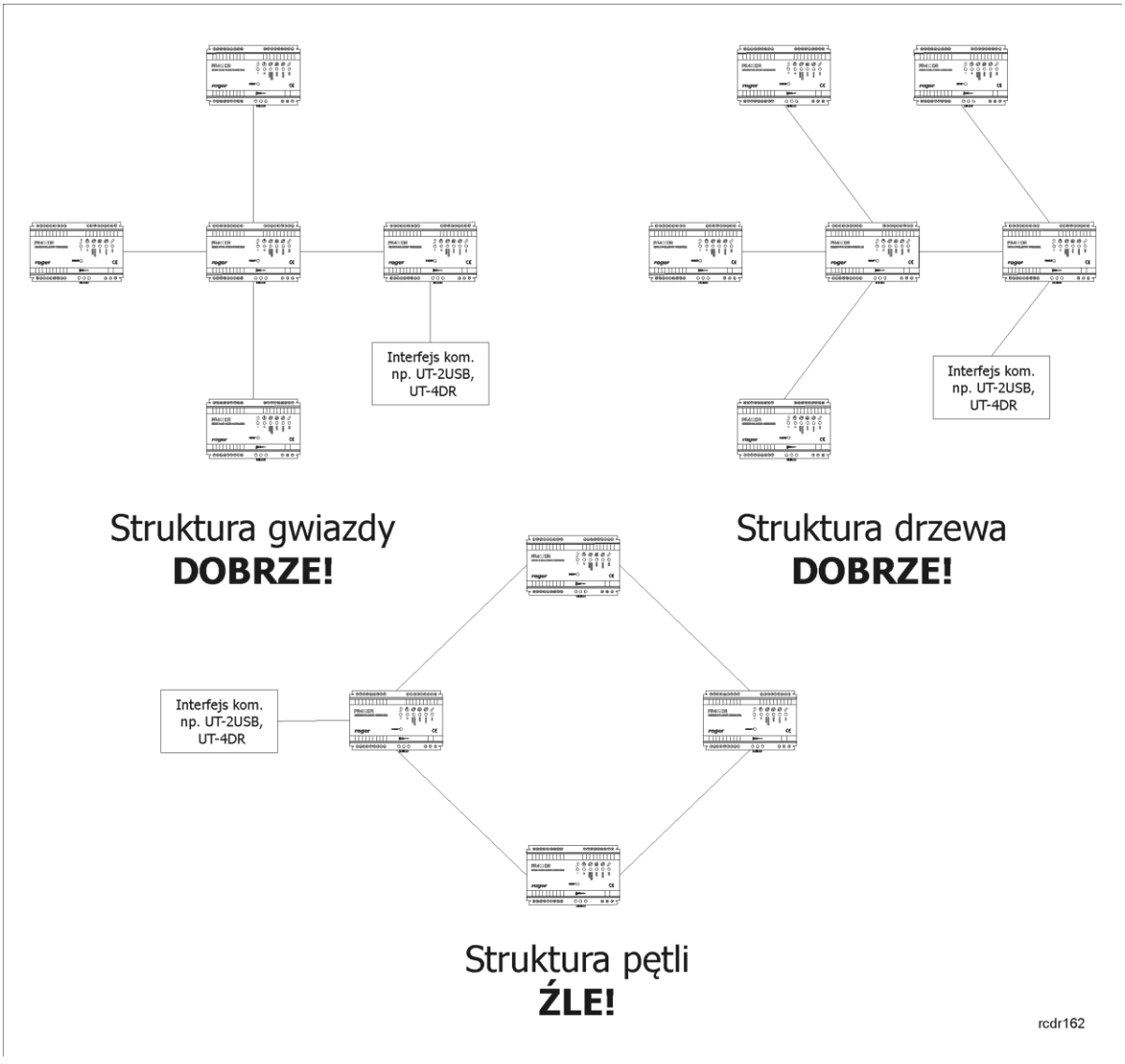
W ramach architektury systemu RACS 4 przedstawionej na rys. 5 obowiązują następujące zasady:

- Maksymalna ilość podsystemów podłączonych do komputera z oprogramowaniem PR Master to 250, a maksymalna ilość kontrolerów w podsystemie to 32 urządzenia,
- Każdy podsystem jest podłączany do komputera z oprogramowaniem PR Master przez osobny interfejs sprzętowy (ilość portów USB można zwiększyć za pomocą rozgałęźnika, w przypadku Ethernetu można zastosować switch lub ruter),
- Wszystkie kontrolery dostępu są kontrolerami jednego przejścia (jedno lub dwustronnie nadzorowanego) i można do nich podłączać zewnętrzne czytniki,
- Centrale CPR są opcjonalnymi urządzeniami poszerzającymi możliwości systemu RACS 4,
- Komputer z oprogramowaniem PR Master nie musi być na stałe włączony czy też podłączony, aby system kontroli dostępu realizował swoje funkcje. Jest ono potrzebne wtedy, gdy użytkownik chce monitorować zdarzenia i alarmy w systemie KD oraz ręcznie ingerować w działanie systemu KD,
- Wszystkie połączenia kablowe pomiędzy urządzeniami kontroli dostępu można zrealizować za pomocą skrętki nieekranowanej (UTP Kat. 5) lub dowolnych innych kabli sygnałowych.

3.2 Komunikacja

3.2.1 Interfejs RS485

Kontrolery PRxx2 są wyposażone w interfejs komunikacyjny pracujący w standardzie RS485. Interfejs ten może być wykorzystywany do programowania kontrolera oraz do komunikacji z nim. Każdy kontroler podłączony do magistrali komunikacyjnej musi posiadać swój niepowtarzalny adres (numer ID=00..99). Do jednej magistrali komunikacyjnej można dołączyć maksymalnie 32 kontrolery dostępu oraz jedną centralę (centrala nie wymaga ustawienia adresu) tworząc w ten sposób podsystem RACS 4.



Rys. 6 Topologia połączenia kontrolerów na magistrali R485

Topologia magistrali komunikacyjnej w systemie RACS 4 może być kształtowana bardzo elastycznie, dopuszczalne są struktury typu „drzewo", „gwiazda" a także dowolne ich kombinacje, nie dopuszcza się jednak stosowania topologii typu „pętla" (patrz rys. 6). Magistrala komunikacyjna może być zrealizowana przy użyciu dowolnego typu kabli sygnałowych, niemniej zaleca się używanie skrętki komputerowej bez ekranu (U/UTP kat. 5). Kable w ekranie należy stosować tylko w warunkach silnych zakłócających pól elektromagnetycznych. W systemie RACS 4 nie ma konieczności stosowania rezystorów terminujących na końcach magistrali komunikacyjnej.
Maksymalne odległości liczone po kablu w systemie RACS 4:

- pomiędzy dowolnym kontrolerem a centralą CPR32-NET: 1200m,
- pomiędzy dowolnym kontrolerem a interfejsem komunikacyjnym: 1200m,
- pomiędzy centralą CPR32-SE a interfejsem komunikacyjnym: 1200m.

Uwaga: Wszystkie urządzenia podłączone do magistrali komunikacyjnej RS485 powinny mieć wspólny potencjał masy zasilania. Warunek ten jest automatycznie spełniony, gdy wszystkie urządzenia są zasilane z tego samego źródła (np. z jednego zasilacza). W przypadku, gdy zasilanie jest realizowane z wielu źródeł (tzw. zasilanie rozproszone) to minusy wszystkich zasilaczy należy połączyć ze sobą używając do tego celu osobnego przewodu sygnałowego, a jeśli jest to niemożliwe to minusy wszystkich zasilaczy należy uziemić, przy czym konieczne jest aby różnica potencjałów uziemienia w różnych punktach instalacji (obiektu) nie była większa niż +/-2V. Pod żadnym warunkiem nie można zwierać plusów zasilania wbudowanych zasilaczy (dotyczy PR402).

Struktura złożona z magistrali komunikacyjnej, kontrolerów dostępu (maks. 32) oraz centrali CPR nosi nazwę Podsystemu Kontroli Dostępu lub krótko Podsystemu. Każdy podsystem w systemie RACS 4 jest podłączony do komputera za pośrednictwem osobnego portu komunikacyjnego. Port komunikacyjny może być rzeczywistym portem szeregowym (COM), wirtualnym portem szeregowym (Virtual Com Port - VCP) lub portem Ethernetowym. W przypadku portu VCOM stosuje się takie interfejsy jak np. RUD-1 czy UT-2USB a w przypadku portu Ethernet można użyć UT-4, CPR32-NET lub UT-4DR.
Każdy kontroler serii PRxx2 może zarządzać pojedynczym przejściem kontrolowanym jedno lub dwustronnie. W ramach jednego systemu RACS 4 można zintegrować do 250 Podsystemów, w każdym do 32 kontrolerów (ale maksymalna ilość kontrolerów w systemie to 1000). Komputer zarządzający komunikuje się z każdym z podsystemów za pośrednictwem osobnego interfejsu komunikacyjnego, dzięki czemu możliwa jest integracja podsystemów podłączonych do komputera za pośrednictwem portów COM, USB lub sieci komputerowej LAN/WAN a także sieci bezprzewodowych Wi-Fi.

Uwaga: Interfejsy komunikacyjne można stosować tymczasowo na czas programowania kontrolera bądź też można podłączyć je na stałe po to by umożliwić zarządzanie systemem KD (patrz 3.1 Tryby pracy kontrolerów serii PRxx2). Do pierwszego programowania pojedynczych kontrolerów można wykorzystać interfejs RUD-1, ponieważ posiada on wyjście zasilające 12VDC, które może być użyte do tymczasowego zasilenia programowanego urządzenia.

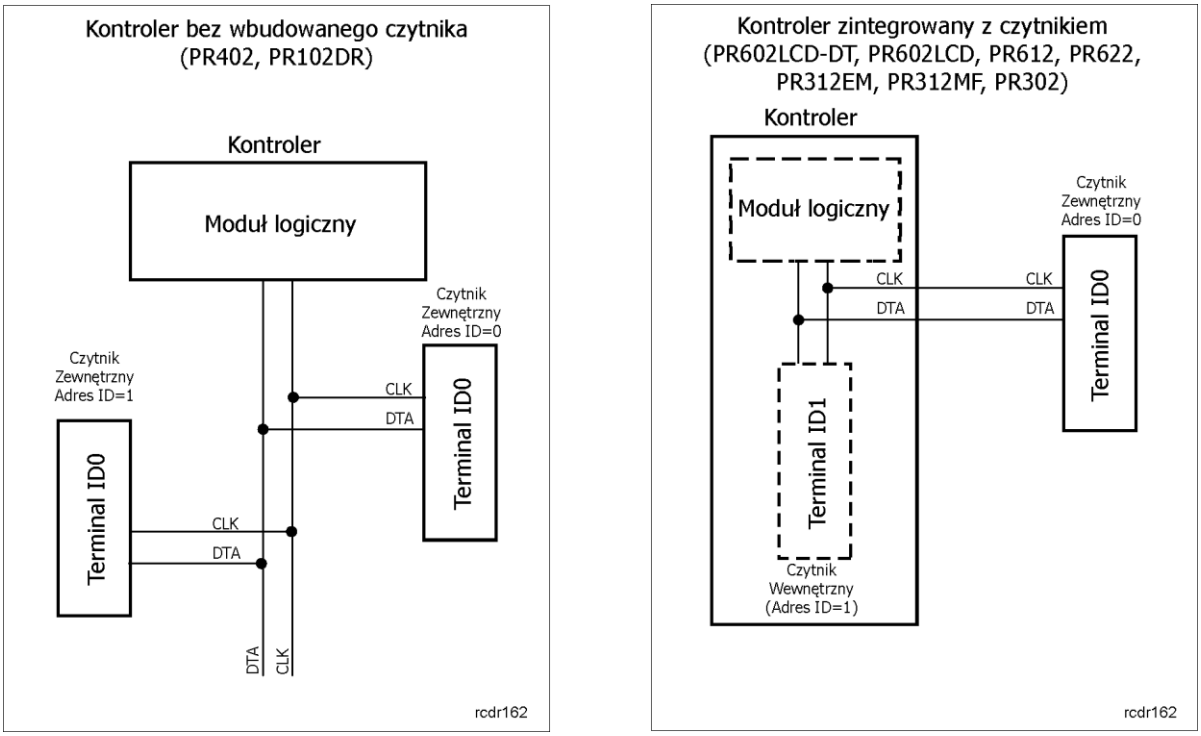
3.2.2 Adresy kontrolerów

Każdy kontroler podłączony do magistrali komunikacyjnej RS485 w ramach danego podsystemu musi posiadać swój niepowtarzalny adres z zakresu 00-99, przy czym każdy nowy fabrycznie kontroler ma ustawiony adres ID=00. O ile zachodzi taka potrzeba to adres ten można zmienić z poziomu programu zarządzającego (PR Master), manualnie w czasie procedury resetu pamięci (patrz instrukcja instalacyjna danego kontrolera), za pomocą zworek (PR402DR, PR102DR) lub poprzez zaprogramowania stałego adresu ID kontrolera (tzw. FixedID). Stały adres ID można ustawić w trakcie procesu aktualizacji oprogramowania wbudowanego (firmware) urządzenia, za pomocą programu Roger ISP. W przypadku kontrolerów PR402DR i PR102DR, adres ID można również ustawić za pomocą zworek umieszczonych na płycie/obudowie modułu. Całkowity zakres adresów ID dla takiego ustawienia mieści się w przedziale 0..127. Przy czym jeśli ustawiony adres zawiera się w przedziale 00..99 to czytnik nie zezwala na zmianę swojego adresu ID inną metodą. Szczegółowe informacje na temat różnych sposobów ustawień adresu dostępne są w instrukcjach instalacyjnych poszczególnych kontrolerów.

3.2.3 Interfejs RACS CLK/DTA

Oprócz interfejsu RS485 kontroler PRxx2 jest wyposażony w interfejs komunikacyjny RACS CLK/DTA. Interfejs ten jest przeznaczony do komunikacji kontrolera z urządzeniami peryferyjnymi firmy ROGER i składa się z on dwóch linii: CLK i DTA. Do tych linii można dołączyć następujące urządzenia zewnętrzne:

- podstawowy czytnik dostępu Terminal ID0, adres ID=0,
- podstawowy czytnik dostępu Terminal ID1, adres ID=1,
- dodatkowy czytniki po stronie Terminala ID0, adres ID=2 – patrz 3.17.3 Tryb High Security,
- dodatkowy czytniki po stronie Terminala ID1, adres ID=3 - patrz 3.17.3 Tryb High Security,
- ekspander XM-2, adres ID=5 – patrz 3.2.4 Współpraca z ekspanderem WE/WY XM-2,
- ekspander XM-8, adresy ID=8…11 – patrz 3.2.5 Współpraca z ekspanderem WE/WY XM-8,
- moduł PSAM-1, adres ID=4 – patrz 3.2.6 Współpraca z modułem PSAM-1.
- panel klawiszy funkcyjnych HRT82MF, adres ID=12 – patrz 3.2.7 Współpraca z panelem HRT82FK



Rys. 7 Interfejs RACS CLK/DTA

Maksymalna odległość liczona po kablu pomiędzy kontrolerem a dowolnym czytnikiem/modułem dołączonym do magistrali RACS CLK/DTA nie może przekraczać 150m. Struktura oraz rodzaje kabli stosowane w tej magistrali są całkowicie dowolne (np. U/UTP kat.5), jedynym warunkiem stawianym kablom jest to aby ich całkowita rezystancja mierzona pomiędzy kontrolerem a dołączonym urządzeniem nie była większa niż 50Ω. Podobnie jak w przypadku magistrali RS485 wszystkie urządzenia podłączone do linii CLK i DTA powinny mieć wspólny minus zasilania. Warunek ten jest zwykle automatycznie zapewniony, ponieważ urządzenia te są najczęściej zasilane bezpośrednio z kontrolera (PR402). Gdyby jednak wystąpiła sytuacja, że którekolwiek z nich byłoby zasilane z innego źródła to należy minus tego zasilacza połączyć z zaciskiem GND lub COM kontrolera, do którego dane urządzenie jest podłączone.

3.2.4 Współpraca z ekspanderem WE/WY XM-2

Kontroler PRxx2 może współpracować z jednym ekspanderem XM-2 o adresie ID=5. Zastosowanie tego modułu powoduje z jednej strony zwiększenie ogólnej ilości wszystkich linii we/wy jak również umożliwia fizyczne odseparowanie linii we/wy od kontrolera. Potrzeba takiej separacji może zachodzić głównie w odniesieniu do kontrolerów z wbudowanymi czytnikami (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302), które w przypadku instalacji w miejscach ogólnodostępnych mogą być narażone na ingerencję osób postronnych. W wyniku tego zagrożenia osoby, które uzyskały dostęp do wnętrza kontrolera omijając alarm antysabotażowy mogą zewrzeć styki wewnętrznego przekaźnika i odblokować drzwi. Komunikacja pomiędzy kontrolerem a ekspanderem XM-2 odbywa się na drodze cyfrowej po magistrali RACS CLK/DTA. Więcej informacji można znaleźć w instrukcji instalacyjnej ekspandera XM-2 dostępnej na stronie www.roger.pl.

3.2.5 Współpraca z ekspanderem WE/WY XM-8

Kontroler PRxx2 może współpracować z maksymalnie 4 ekspanderami XM-8 o adresach z przedziału ID=8…11. Ekspander XM-8 jest stosowany do kontroli dostępu w windach. Obsługuje on 8 wyjść przekaźnikowych i w przypadku zastosowania 4 takich modułów można obsłużyć windę o maksymalnie 32 piętrach. Komunikacja pomiędzy kontrolerem a ekspanderem XM-8 odbywa się na drodze cyfrowej po magistrali RACS CLK/DTA. Więcej informacji można znaleźć w instrukcji instalacyjnej ekspandera XM-8 dostępnej na stronie www.roger.pl.

3.2.6 Współpraca z modułem PSAM-1

Kontroler PRxx2 może współpracować z jednym modułem dozoru zasilania typu PSAM-1 o adresie ID=4. Moduł jest opcjonalnym wyposażeniem zasilaczy PS10, PS20 i PS15v24 (ROGER) ale może również współpracować z powszechnie dostępnymi zasilaczami innych producentów. Moduł PSAM-1 może pracować w trybie autonomicznym lub sieciowym. Gdy pracuje w trybie autonomicznym stany alarmowe zasilacza są sygnalizowane na jego tranzystorowych liniach wyjściowych. W trybie sieciowym moduł PSAM-1 przesyła dane o stanie zasilacza drogą cyfrową za pośrednictwem magistrali RACS CLK/DTA do urządzenia nadrzędnego (kontrolera). W trybie autonomicznym moduł PSAM-1 może współpracować ze wszystkimi kontrolerami serii PRxx1 i PRxx2 firmy ROGER. W trybie sieciowym jedynie z kontrolerami serii PRxx2. Moduł PSAM-1 umożliwia dozorowanie następujących stanów:

- Niski poziom baterii rezerwowej,
- Awaria baterii rezerwowej,
- Brak napięcia sieciowego 230VAC,
- Aktualny stan napięcia na wyjściu zasilacza (tylko w trybie sieciowym).

Więcej informacji można znaleźć w instrukcji instalacyjnej modułu PSAM-1 dostępnej na stronie www.roger.pl.

3.2.7 Współpraca z panelem HRT82FK

Kontroler PRxx2 może współpracować z jednym dotykowym panelem klawiszy funkcyjnych HRT82FK o adresie ID=12. Panel jest opcjonalnym urządzeniem pozwalającym uzyskać obsługę dodatkowych czterech klawiszy funkcyjnych w ramach pojedynczego kontrolera. Do każdego klawisza można przypisać dwie różne funkcję wywoływane odpowiednio przez krótkie oraz długie naciśnięcie klawisza. Listę możliwych funkcji podano w podpunkcie 3.15 Klawisze funkcyjne. Wskaźniki LED poszczególnych klawiszy także mogą być konfigurowane poprzez przypisanie funkcji. W praktyce wskaźnikom przypisuje się funkcje związane z funkcjami klawiszy po to by sygnalizować załączenie/wyłączenie klawisza. Obsługa panelu przez kontroler PRxx2 wymaga jego załączenie we właściwościach kontrolera za pomocą programu PR Master – patrz 4.17 Zakładki HRT82FK. Komunikacja pomiędzy kontrolerem a panelem odbywa się na drodze cyfrowej po magistrali RACS CLK/DTA. Więcej informacji można znaleźć w instrukcji instalacyjnej panelu HRT82FK dostępnej na stronie www.roger.pl.

3.2.8 Dołączanie czytników Wiegand oraz Magstripe

Niektóre kontrolery serii PRxx2 (patrz tabela 1) mogą współpracować zarówno z czytnikami serii PRT jak i z dowolnymi czytnikami zewnętrznymi pracującymi w standardzie Wiegand lub Magstripe. Sposób dołączania czytników jest przedstawiony w instrukcjach poszczególnych kontrolerów. Do komunikacji wykorzystywane są linie wejściowe kontrolera (PR402DR) lub magistrala RACS CLK/DTA (PR402-BRD, PR602LCD-DT i PR602LCD).
Aby kontroler mógł prawidłowo współpracować z czytnikiem należy w programie zarządzającym PR Master, we właściwościach kontrolera, w zakładce **Terminal ID1** i/lub zakładce **Terminal ID0** (patrz 4.2 Zakładka Terminal ID1) z listy rozwijanej poprawnie wybrać typ dołączanego czytnika, przy czym należy zwrócić uwagę na trzy parametry charakteryzujące dołączany czytnik:

- Standard elektryczny,
- Typ transmitowanych danych,
- Sposób kodowania danych.

Standard elektryczny czytników opisuje charakterystykę elektryczną sygnału stosowanego do komunikacji pomiędzy kontrolerem a czytnikiem. Kontrolery PRxx2 akceptują następujące standardy elektryczne:

- Wiegand,
- Magstripe (ABA Track II Emulation),
- RACS CLK/DTA (ROGER).

Uwaga: Wszystkie urządzenia podłączone do linii RACS CLK/DTA (w tym czytniki dostępu) powinny mieć wspólny minus zasilania.

Kontrolery PRxx2 obsługują formaty Wiegand o długości transmisji od 26 do 66 bitów, z lub bez bitów kontrolnych (tzw. bity parzystości). Nie jest konieczne wskazywanie długości transmitowanych przekazów, kontroler samoczynnie rozpoznaje i dopasowuje się do ilości bitów transmitowanych przez czytnik.
Typ danych określa, jakie dane są przesyłane przez czytnik. Czytnik może przesyłać:

- Kod karty lub kod PIN,
- Tylko kod karty,
- Tylko kod PIN,
- Tylko numer ID użytkownika.

W pierwszym z wymienionych przypadków kontroler samoczynnie rozpoznaje czy dane transmitowane przez czytnik reprezentują kod karty czy kod PIN i stosownie do tego je interpretuje. W pozostałych przypadkach dane odbierane są zawsze interpretowane w jeden i ten sam sposób wskazany w ustawieniach kontrolera tzn. jako kod karty, kod PIN lub jako numer ID użytkownika. Sposób kodowania określa, w jaki sposób następuje przesyłanie cyfr i liczb. Spotyka się następujące systemy:

- BIN, czytnik transmituje liczby w postaci binarnej,
- HEX, czytnik transmituje liczby w postaci szesnastkowej,
- BCD, czytnik transmituje liczby w postaci dziesiętnej kodowanej binarnie.

3.2.9 Dołączanie czytników biometrycznych

Wszystkie kontrolery serii PRxx2 mogą współpracować z czytnikami linii papilarnych RFT1000. Komunikacja pomiędzy kontrolerem a czytnikiem jest realizowana za pomocą interfejsu RACS CLK/DTA lub Wiegand, natomiast komunikacja pomiędzy komputerem a czytnikiem jest realizowana za pomocą interfejsu Ethernet lub RS485.
Więcej informacji można znaleźć w instrukcjach czytnika RFT1000 dostępnych na stronie www.roger.pl.

3.2.10 Dołączanie czytników dalekiego zasięgu

Niektóre kontrolery serii PRxx2 (patrz tabela 1) mogą współpracować z czytnikami dalekiego zasięgu GP60 i GP90 dostępnymi w ofercie ROGER. Komunikacja z ww. czytnikami odbywa się za pomocą interfejsu Magstripe (zalecane) z ustawieniem funkcji **[31]: Magstripe, podaje kod Karty** w programie PR Master (patrz 4.2 Zakładka Terminal ID1) lub za pomocą interfejsu Wiegand z ustawieniem funkcji **[4]: Wiegand 26...66 bit, podaje kod karty**. W przypadku podłączenia dwóch czytników do jednego kontrolera może być konieczne zastosowanie interfejsu PR-GP (ROGER).
Więcej informacji można znaleźć w instrukcjach czytników dalekiego zasięgu GP60 i GP90 dostępnych na stronie www.roger.pl.

3.3 Użytkownicy

Użytkownicy kontroli dostępu

W kontrolerach PRxx2 można zarejestrować do 4000 użytkowników. Każdy z użytkowników posiada swój numer identyfikacyjny (ID=0000-3999) oraz kartę zbliżeniową i/lub kod PIN, który może się

składać z od 3 do 6 cyfr. W kontrolerze PRxx2 wyposażonym w klawiaturę a także na czytnikach serii PRT skonfigurowanych do trybu RACS CLK/DTA wprowadzanie kodu PIN zawsze należy zakończyć klawiszem [#]. W czytnikach Wiegand i Magstripe spotyka się również inne metody wprowadzania kodu np. bez klawisza [#] lub każdy naciśnięty klawisz jest natychmiast transmitowany do kontrolera.
Użytkownicy mogą należeć do 4 typów (klas): NORMAL, SWITCHER Full, SWITCHER Limited oraz MASTER. 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 (patrz 4.5 Zakładka Przezbrajanie). Każda klasa użytkowników charakteryzuje się innymi uprawnieniami w zakresie funkcji programowania oraz przezbrajania kontrolera.

Tabela 2. Typy użytkowników

Nazwa	Numer ID	Opis
MASTER	000	Uprawnienie do otwierania drzwi i przezbrajania kontrolera. Użytkownik ten może być zdefiniowany w trakcie Resetu Pamięci lub z poziomu programu PR Master. Zdefiniowanie użytkownika MASTER umożliwia wstępne przetestowanie kontrolera poprzez sprawdzenie poprawności sterowania elementem wykonawczym i ewentualnie przezbrojenie kontroler. Przezbrojenia kontrolera wymaga dwukrotnego użycia karty Master lub kodu PIN przypisanego do użytkownika MASTER. Użytkownik MASTER jest użytkownikiem przypisywanym do tzw. Bez Grupy, co oznacza, że uzyskuje dostęp wszędzie i bez względu na aktualnie obowiązujące harmonogramy dostępu (chyba że jest to ograniczone innymi ustawieniami specjalnymi).
SWITCHER Full	ID=001-049	Uprawnienie do otwierania drzwi oraz do przezbrajania kontrolera. Przezbrojenie kontrolera wymaga dwukrotnego użycia identyfikatora natomiast przyznanie dostępu następuje z chwilą pierwszego użycia tego identyfikatora.
SWITCHER Limited	ID=050-099	Uprawnienie tylko do przezbrajania kontrolera, przezbrojenie następuje w następstwie jednokrotnego użycia identyfikatora.
NORMAL	ID=100-999	Uprawnienie tylko do otwierania drzwi zgodnie z ustawionymi prawami dostępu. Użytkownicy typu NORMAL o numerze ID większym niż 1000 mogą posiadać dodatkowo atrybut Local SWITCHER, który uprawnia ich również do przezbrajania określonego kontrolera. W odróżnieniu od pozostałych klas użytkowników, atrybut Local SWITCHER przydziela się indywidualnie każdemu użytkownikowi na każdym kontrolerze. Tak jak w przypadku użytkowników SWITCHER Full, przezbrojenie kontrolera przez użytkowników NORMAL posiadających atrybut Local SWITCHER wymaga dwukrotnego użycia identyfikatora.

Grupy Dostępu

Użytkownicy kontrolera mogą być przypisywani do jednej z predefiniowanych grup tj. Bez Grupy, Grupy bez Dostępu lub przynależeć do dowolnej Grupy Dostępu zdefiniowanej przez administratora systemu za pomocą opcji **Grupy** w oknie głównym programu PR Master. W kontrolerach PRxx2 można zdefiniować maksymalnie 250 Grup Dostępu. Przynależność do danej Grupy Dostępu determinuje prawa użytkownika w ramach danego systemu KD. Wszyscy użytkownicy należący do tej samej Grupy Dostępu mają takie same (identyczne) uprawnienia dostępu. Grupa Dostępu może się składać tylko z jednego użytkownika. Członkowie grupy uzyskują dostęp do określonych obszarów zwanych Strefami Dostępu zgodnie z indywidualnie zdefiniowanymi Harmonogramami. Użytkownicy posiadający status Bez Grupy posiadają dostęp do wszystkich Stref Dostępu bez żadnych ograniczeń czasowych – tzn. mają dostęp do wszystkich pomieszczeń będących pod kontrolą systemu przez całą dobę i w każdym dniu tygodnia. Natomiast użytkownicy przypisani do Grupy bez Dostępu nie mają prawo otwierać żadnych drzwi.

Uwaga: W systemie RACS 4 dany użytkownik może być przypisany do jednej Grupy Dostępu.

3.4 Tryby Identyfikacji

W celu identyfikacji (potwierdzenia tożsamości) użytkownika, kontroler przejścia może stosować jeden z czterech podanych poniżej Trybów Identyfikacji.

Tabela 3. Tryby Identyfikacji	
Nazwa	Opis
Karta lub PIN	Kontroler wymaga odczytu karty lub podania kodu PIN.
Karta i PIN	Kontroler wymaga odczytu karty i podania kodu PIN, kolejność nie gra roli.
Tylko Karta	Kontroler akceptuje tylko karty.
Tylko PIN	Kontroler akceptuje tylko kody PIN.

Tryby Identyfikacji definiuje się niezależnie dla każdej strony przejścia. O ile Tryb Identyfikacji nie zostanie zmieniony podczas konfiguracji systemu to stosowany jest tryb Karta lub PIN jako Domyślny Tryb Identyfikacji. Tryb Identyfikacji dotyczy wszystkich użytkowników niezależnie od ich typu lub kategorii. Sterowanie Trybami Identyfikacji może odbywać się z poziomu:

- Harmonogramu - opcja **Harmonogramy** w oknie głównym programu PR Master i zakładka **Terminal ID1** lub **Terminal ID0** (patrz 4.2 Zakładka Terminal ID1) we właściwościach kontrolera
- Linii wejściowej kontrolera - patrz 3.13 Linie wejściowe kontrolera
- Klawisza funkcyjnego kontrolera - patrz 3.15 Klawisze funkcyjne
- Komendy z klawiatury kontrolera lub dołączonego do niego czytnika PRT z klawiaturą - patrz 3.18 Komendy z klawiatury

3.5 Tryby Drzwi

Tryb Drzwi to zbiór zasad (scenariuszy), na bazie których kontroler blokuje i odblokowuje kontrolowane przejście (drzwi). Rozróżnia się cztery Tryby Drzwi:

Tabela 4. Tryby Drzwi	
Tryb Drzwi	Opis
Normalny	Normalnie drzwi są zablokowane, zwolnienie drzwi następuje tylko na czas przyznania dostępu.
Odblokowane	Drzwi są odblokowane na stałe, wejście może się odbywać bez użycia identyfikatorów i przejście jest niekontrolowane.
Warunkowo Odblokowane	Początkowo drzwi są w stanie Normalnym, z chwilą przyznania dostępu pierwszej osobie drzwi przechodzą samoczynnie do trybu Odblokowane.
Zamknięte	Drzwi są permanentnie zablokowane niezależnie od tego czy użytkownik, który próbuje wejść jest uprawniony do wejścia czy nie.

Podstawowym a jednocześnie domyślnym Trybem Drzwi jest tryb Normalny (drzwi zostają odblokowane wyłącznie w momencie przyznania dostępu). Sterowanie Trybami Drzwi może odbywać się z poziomu:

- Harmonogramu czasowego - opcja **Harmonogramy** w oknie głównym programu PR Master i zakładka **Dostęp** (patrz 4.4 Zakładka Dostęp) we właściwościach kontrolera,
- Linii wejściowej - patrz 3.13 Linie wejściowe kontrolera,
- Klawisza funkcyjnego - patrz 3.15 Klawisze funkcyjne,
- Komendy z klawiatury kontrolera lub dołączonego do niego czytnika PRT z klawiaturą - patrz 3.18 Komendy z klawiatury,

- Komendy zdalnej z programu PR Master - opcje dostępne po kliknięciu kontrolera prawym przyciskiem myszy w oknie głównym programu PR Master.

3.6 Tryby Uzbrojenia

Koncepcja Trybów Uzbrojenia

Kontroler PRxx2 posiada dwa stany uzbrojenia: uzbrojony i rozbrojony. Aktualny stan uzbrojenia kontrolera jest sygnalizowany na dwukolorowym wskaźniku LED STATUS przy czym stanowi uzbrojenia odpowiada kolor czerwony natomiast stanowi rozbrojenia odpowiada kolor zielony. Stan uzbrojenia jest również sygnalizowany za pomocą LED na czytniku serii PRT o ile został on podłączony do kontrolera.
Sterowanie trybem uzbrojenia kontrolera może być realizowane na kilka sposobów:

- Manualnie przy pomocy identyfikatorów użytkowników - Karta zbliżeniowa i/lub kod PIN, patrz 3.3 Użytkownicy,
- Automatycznie z poziomu Harmonogramu Przezbrajania - Opcja **Harmonogramy** w oknie głównym programu PR Master i zakładka **Przezbrajanie** we właściwościach kontrolera,
- Z linii wejściowej - patrz 3.13 Linie wejściowe kontrolera,
- Z klawisza funkcyjnego - patrz 3.15 Klawisze funkcyjne,
- Manualnie komendą z klawiatury kontrolera lub dołączonego do niego czytnika PRT z klawiaturą - patrz 3.18 Komendy z klawiatury,
- Zdalnie z poziomu centrali CPR32 - logika Stref Alarmowych, patrz 3.12 Strefy Alarmowe,
- Zdalnie z komputera zarządzającego z programem PR Master - opcje dostępne po kliknięciu kontrolera prawym przyciskiem myszy w oknie głównym programu PR Master.

Wszystkie wymienione sposoby przezbrajania mogą być stosowane współbieżnie (mają taki sam priorytet). Wyjątkiem od tej zasady jest sytuacja, gdy stan uzbrojenia jest sterowany z poziomu linii wejściowej z funkcją **[03]: Przezbrajanie – klucz stały**. Gdy linia wejściowa z tą funkcją jest załączona to kontroler jest w stanie rozbrojenia a gdy nie jest załączona to kontroler jest w stanie uzbrojenia. Gdy do jednego z wejść kontrolera przypisana jest funkcja **[03]** to stan uzbrojenia zależy tylko od stanu tej linii i inne metody przezbrajania nie działają.

Tryby uzbrojenia zostały wprowadzone do systemu RACS 4 w celu zapewnienia:

- dodatkowego poziomu kontroli dostępu,
- integracji z centralami alarmowymi.

Dodatkowy poziom dostępu wiąże się z opcją **Blokuj dostęp gdy kontroler jest stanie uzbrojenia** (patrz 4.4 Zakładka Dostęp), po której załączeniu do uzyskania dostępu na danym przejściu najpierw konieczne jest rozbrojenie kontrolera a następnie użycie identyfikatora posiadającego prawa dostępu. Jeżeli opcja jest wyłączona to użytkownik z odpowiednimi prawami dostępu uzyskuje dostęp bez względu na stan uzbrojenia. W przypadku kontrolera rozbrojonego dostęp może uzyskać jedynie użytkownik z odpowiednimi prawami dostępu (bez względu na powyższą opcję). Domyślnie wspomniana opcja jest odznaczona.
Do integracji z centralami alarmowymi wykorzystuje się linie wejściowe i wyjściowe kontrolera, które można połączyć z wejściami i wyjściami centrali alarmowej. Można również zastosować logikę Stref Alarmowych (patrz 3.12 Strefy Alarmowe).

Manualne przezbrajanie kontrolera przez użytkownika

Kontroler może być przezbrajany przy pomocy identyfikatorów użytkowników kart/PIN kodów: MASTER, SWITCHER Full, SWITCHER Limited i NORMAL z atrybutem Local Switcher (patrz 3.3 Użytkownicy).
Sposób przezbrajania dla użytkowników SWITCHER Full, MASTER i NORMAL z atrybutem Local SWITCHER:

- Zalogować się (tzn. odczytać kartę lub wprowadź PIN w zależności od aktualnego Trybu Identyfikacji – patrz 3.4 Tryby Identyfikacji),
- Poczekać aż wskaźnik LED SYSTEM zacznie pulsować,

- Gdy wskaźnik LED SYSTEM pulsuje dokonać powtórnego logowania, przy czym jeśli na kontrolerze obowiązuje w danej chwili Tryb Karta i PIN to wystarczy użyć tylko jednej z form identyfikacji tzn. karty lub PIN-u.

W przypadku przezbrojenia przez użytkownika o statusie SWITCHER Limited wystarczy zalogować się jednokrotnie.

Przezbrajanie kontrolera przez harmonogram

Kontroler może zmieniać stan uzbrojenia samoczynnie wg zdefiniowanego harmonogramu czasowego zwanego Harmonogramem Przezbrajania. Harmonogram Przezbrajania jest w istocie zwykłym harmonogramem czasowym czyli Harmonogramem Ogólnego Przeznaczenia zastosowanym do sterowania trybem uzbrojenia kontrolera. Algorytm przezbrajania przez harmonogram działa w taki sposób, że o czasie wskazanym przez parametr Od.. kontroler przechodzi do stanu rozbrojenia natomiast o czasie wskazanym przez parametr Do.. kontroler powraca do stanu uzbrojenia. Możliwe jest opóźnianie uzbrojenia (patrz 4.5 Zakładka Przezbrajanie). Wszystkie harmonogramy w systemie RACS 4 ustawia się w oknie głównym programu PR Master za pomocą opcji **Harmonogramy**.
Przezbrajanie może się odbywać w oparciu o harmonogram dla Strefy Alarmowej, do której należy dany kontroler lub w oparciu o harmonogram bezpośrednio przypisany do danego kontrolera.. Wskazanie wbudowanego harmonogramu Nigdy powoduje, że kontroler na stałe będzie przebywał w trybie uzbrojenia po przesłaniu ustawień lub resecie ustawień, natomiast wskazanie wbudowanego harmonogramu Zawsze spowoduje, że kontroler przez cały czas po przesłaniu ustawień lub resecie ustawień będzie w trybie rozbrojenia.

Uwaga: Samo wybranie Harmonogramu Przezbrajania nie oznacza, że kontroler będzie na bieżąco kontrolował zgodność swojego stanu uzbrojenia z harmonogramem. Harmonogram decyduje jedynie o momentach czasowych, w których następuje zmiana uzbrojenia. Aby kontroler samoczynnie uzbrajał się po ręcznym rozbrojeniu w czasie, gdy zgodnie z harmonogramem powinien być on uzbrojony, konieczne jest zastosowanie opcji **Samoczynnie przywróć tryb uzbrojenia po czasie** (patrz 4.5 Zakładka Przezbrajanie).

Moment uzbrojenia wynikającego z Harmonogramu Przezbrajania jak również moment samouzbrajania może być odwlekany przez użytkownika, przy czym ma on do dyspozycji następujące metody:

- Użycie klawisza funkcyjnego – patrz 3.15 Klawisze funkcyjne,
- Wyzwolenie linii wejściowej – patrz 3.13 Linie wejściowe kontrolera,
- Manualnie przy pomocy komendy wprowadzonej na klawiaturze kontrolera lub dołączonego czytnika z klawiaturą – patrz 3.18 Komendy z klawiatury,
- Automatycznie z chwilą przyznania dostępu.

Ta zwłoka w automatycznym uzbrajaniu może być definiowana przez administratora w przedziale od 5 do 99 minut. Możliwe jest również ustawienie czasu ostrzegania użytkowników przed nadchodzącym uzbrojeniem w przedziale od 1 do 99 minut. Ostrzeżenie ma postać sygnału akustycznego generowanego przez kontroler/czytnik.
Więcej informacji szczegółowych na temat ustawień dotyczących przezbrajania automatycznego jest podane w opisie opcji programu PR Master – patrz 4.5 Zakładka Przezbrajanie.

3.7 Definiowanie Praw Dostępu

Definiowanie praw dostępu w systemie RACS 4 polega na wskazaniu kto, gdzie i kiedy ma mieć prawo dostępu. Proces ustalania zasad dostępu za pomocą oprogramowania PR Master najlepiej realizować w następujących krokach:

- Zdefiniowanie Grup Użytkowników za pomocą opcji **Grupy** w oknie głównym programu PR Master,
- Dodanie lub zaimportowanie użytkowników i przypisanie ich do Grup Użytkowników za pomocą opcji **Użytkownicy** w oknie głównym programu PR Master,

- Zdefiniowanie Stref Dostępu za pomocą opcji **Strefy Dostępu** w oknie głównym programu PR Master,
- Przydzielenie punktów identyfikacji (terminali ID1 i ID0) we właściwościach kontrolerów jako wejść do konkretnych Stref Dostępu (patrz 4.2 Zakładka Terminal ID1),
- Zdefiniowanie Harmonogramów (tzw. kalendarzy) za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master,
- Powiązanie Grup Użytkowników ze Strefami Dostępu oraz Harmonogramami w oknie otwieranym za pomocą opcji **Grupy**. Etap ten polega na wskazaniu Harmonogramu, który określi przedziały dni/godzin kiedy użytkownicy danej grupy będą mieli prawo dostępu do wybranej Strefy Dostępu,
- Skorzystanie z opcji **Mapa praw dostępu** w oknie głównym programu PR Master w celu weryfikacji wcześniejszych ustawień,
- Opcjonalnie skonfigurowanie dodatkowych mechanizmów odpowiedzialnych za dostęp (np. definiowanie Trybów Drzwi, definiowanie linii wejściowych zwalniających/blokujących dostęp, funkcja APB itp.).

Proces przyznawania dostępu przez kontroler przebiega następująco:

- Identyfikacja użytkownika (logowanie),
- Określenie Grupy Użytkowników, do której należy osoba,
- Określenie czy dana Grupa Użytkowników ma w tej chwili prawo dostępu do wybranej Strefy Dostępu, w skład której wchodzi dany punkt identyfikacji (czytnik),
- Sprawdzenie dodatkowych mechanizmów sterujących dostępem (APB, opcje specjalne, Tryb Drzwi itd.),
- Decyzja o dostępie,
- Odblokowanie drzwi.

Uwaga: W systemie RACS 4 definiowanie praw dostępu polega na wskazaniu kto, gdzie i kiedy ma mieć dostęp. Nowo dopisany użytkownik przypisany do Grupy bez Dostępu nie może otwierać żadnych drzwi. Z kolei Użytkownik przypisany do grupy Bez Grupy ma prawa dostępu do wszystkich przejść bez żadnych limitów czasowych.

Kontroler nie przyznaje dostępu, gdy:

- Odczytany identyfikator nie jest znany,
- Odczytany identyfikator nie jest pełny np. wprowadzono tylko PIN, choć na czytniku obowiązuje Tryb Identyfikacji Karta i PIN,
- Wprowadzony identyfikator należy do użytkownika typu SWITCHER Limited,
- Z harmonogramu czasowego wynika, że użytkownik danej Grupy Użytkowników nie ma aktualnie prawa dostępu do danej Strefy Dostępu,
- Gdy kontroler jest uzbrojony oraz obowiązuje na nim opcja **Blokuj dostęp gdy kontroler jest w stanie uzbrojenia** (patrz 4.4 Zakładka Dostęp),
- W przypadku gdy dostęp jest blokowany z poziomu linii wejściowej skonfigurowanej do funkcji **[11]: Blokada dostępu.**

Uwaga: Gdy odczytany identyfikator nie jest zarejestrowany w kontrolerze to czytnik generuje długi sygnał akustyczny, gdy użytkownik do którego należy identyfikator jest zarejestrowany lecz w danej chwili nie ma prawa wejścia to czytnik generuje dwa długie tony akustyczne.

Zawsze, kiedy kontroler przyznaje dostęp zapala się wskaźnik LED OPEN i pozostaje on zapalony tak długo jak drzwi są w stanie odblokowania.

Sterowanie elementem wykonawczym

Za pomocą programu PR Master (patrz 4.4 Zakładka Dostęp) dla danego przejścia (kontrolera) możliwe jest ustawianie następujących parametrów:

- **CZAS NA WEJŚCIE** (inaczej czasu zwolnienia zamka drzwi),

- **OPÓŹNIENIE OTWARCIA DRZWI** (zwłoki, po której nastąpi zwolnienie zamka drzwi),
- **CZAS NA ZAMKNIĘCIE** (inaczej czasu po którym niedomknięcie drzwi będzie sygnalizowane alarmem DRZWI OTWARTE – wymaga podłączenia czujnika otwarcia drzwi).

Opcjonalnie, sterowanie zamkiem drzwiowym może być realizowane w trybie zatrzask (tryb bistabilny), wtedy drzwi zostają odblokowane na czas nieograniczony tzn. aż do momentu wystąpienia kolejnego przyznania dostępu.
W praktyce spotyka się cztery podstawowe sposoby sterowania elementem wykonawczym:

- Przez podanie zasilania (np. elektrozaczep),
- Przez odjęcie zasilania (np. zwora magnetyczna lub elektrozaczep rewersyjny),
- Przez podanie impulsu do układu automatyki (np. sterowanie szlabanem),
- Przez sterowanie silnikiem wykonawczym.

Kontroler może sterować elementem wykonawczym (zamkiem) za pośrednictwem trzech różnych funkcji, które zwykle przypisuje się wyjściom przekaźnikowym REL1 i/lub REL2 kontrolera:

- **[97]:Zamek drzwi (term. ID0)**
- **[98]:Zamek drzwi (term. ID1)**
- **[99]:Zamek drzwi**

Kontroler aktywuje wyjście **[99]** bez względu na to, czy dostęp został przyznany z Terminala ID0, czy Terminala ID1. Natomiast wyjścia **[97]** i **[98]** są aktywowane w zależności od tego, na którym czytniku (ID0 czy ID1) nastąpiło logowanie użytkownika. W praktyce, wyjścia **[97]** i **[98]** znajdują zastosowanie do sterowania bramką obrotową w sytuacji, gdy wymagane jest rozróżnienie kierunku obrotu bramki. W momencie przyznania dostępu drzwi zostają odblokowane na czas określony przez parametr **CZAS NA WEJŚCIE**.

3.8 Kod Obiektu (ang. Facility Code)

Kod Obiektu to charakterystyczna część kodu karty, która wskazuje na przynależność danej karty do pewnej (większej) grupy kart wytworzonych zwykle dla konkretnego systemu lub klienta. W kontrolerze PRxx2 kod obiektu to bity na pozycjach 16-24 numeru karty, które po przetworzeniu na postać dziesiętną dają liczbę z zakresu od 000-255.

Przykład:
Kod karty w postaci binarnej: 00010000000000001110111000100010010110111, gdzie podkreślona część kodu 11101110 jest traktowana jako Kod Obiektu.

Załączenie opcji Kod Obiektu powoduje, że kontroler przyznaje dostęp wszystkim kartom, które mają ten sam Kod Obiektu. Dzięki tej funkcji kontroler może umożliwiać dostęp do pomieszczenia dla znacznie większej ilości użytkowników pod warunkiem, że użytkownicy ci posiadają karty ze wspólnym Kodem Obiektu. Opcje związane z Kodem Obiektu są dostępne we właściwościach kontrolera w programie PR Master (patrz 4.4 Zakładka Dostęp).

3.9 Alarm Drzwi

Przez pojęcie Alarm Drzwi w kontrolerach PRxx2 rozumie się wystąpienie przynajmniej jednego z trzech wymienionych poniżej stanów:

- PREALARM
- DRZWI OTWARTE
- WEJŚCIE SIŁOWE

Sygnalizacja każdego z wymienionych stanów alarmowych może być realizowana indywidualnie na osobnych liniach wyjściowych lub zbiorczo na linii wyjściowej z funkcją **[256]: Alarm drzwi**. W przypadku, gdy alarm drzwi jest sygnalizowany na jednym wyjściu **[256]** to rozróżnienie typu sygnalizowanego alarmu następuje poprzez rozpoznanie sposobu modulacji linii wyjściowej, przy czym w przypadku wystąpienia więcej niż jednego alarmu kontroler sygnalizuje alarm o najwyższym priorytecie.

Istnieje również możliwość sygnalizowania Alarmu Drzwi na wewnętrznym głośniku. Logika takiej sygnalizacji jest taka sama jak w przypadku sygnału elektrycznego na linii wyjściowej kontrolera. Opcje związane z Alarmem Drzwi są dostępne we właściwościach kontrolera w programie PR Master (patrz 4.6 Zakładka Opcje).

Tabela 5. Alarmy Drzwi

Stan	Opis	Priorytet	Metoda sygnalizacji
PREALARM	Stan ten występuje w następstwie wystąpienia pięciu kolejnych prób użycia nieznanego identyfikatora na kontrolerze w ciągu pięciu minut. Identyfikator istniejący w systemie ale nie posiadający praw dostępu do danego przejścia nie wywołuje stanu PREALARM.	Niski	Pojedynczy impuls trwający 0,5 sek. powtarzany z okresem 4 sek.
DRZWI OTWARTE	Stan powstaje w momencie, gdy drzwi nie zostaną domknięte po upływie czasu określonego przez: **CZAS NA ZAMKNIĘCIE** (patrz 4.4 Zakładka Dostęp). Wymagane zainstalowanie czujnika otwarcia drzwi.	Średni	Podwójne impulsy (każdy impuls 0.5s) powtarzane z okresem 4 sek.
WEJŚCIE SIŁOWE	Stan występuje w przypadku wykrycia otwarcia drzwi bez udziału kontrolera lub na skutek wprowadzenia kodu PIN pod przymusem (patrz 4.6 Zakładka Opcje). Wymagane zainstalowanie czujnika otwarcia drzwi.	Najwyższy	Impuls trwający 2 sek. a potem 2 sek. przerwy

3.10 Flagi Systemowe (Tajmery)

Flagi Systemowe to stany logiczne w pamięci kontrolera, które odzwierciedlają pewne określone stany (sytuacje) występujące w kontrolerze. Niektóre flagi posiadają ściśle zdefiniowane znaczenie i są związane z określonymi zdarzeniami (np. ŚWIATŁO, TAMPER, WŁAMANIE) inne, mają charakter uniwersalny i mogą być użyte do dowolnie wybranych celów (np. AUX1, AUX2).
Normalnie domyślnym stanem każdej flagi jest stan wyłączenia. Załączenie flagi może nastąpić jedynie w następstwie wystąpienia pewnych, specyficznych dla danej flagi przyczyn. Powrót flagi do stanu normalnego następuje samoczynnie po upływie czasu określonego przez jej Tajmer lub pod wpływem innego, charakterystycznego dla danej flagi zdarzenia. Tajmery niektórych flag mogą być ustawiane w tryb pracy bistabilnej (praca typu zatrzask), wtedy zmiana stanu flagi następuje na czas nieograniczony tzn. do momentu wystąpienia następnego zdarzenia, które zmieni jej stan.
Aktualny stan każdej flagi może być sygnalizowany na linii wyjściowej, gdy przypisana jest do niej określona funkcja.
Czasy załączania flag systemowych mogą być ustawiane we właściwościach kontrolera w programie PR Master (patrz 4.9 Zakładka Tajmery).

Tabela 6. Flagi Systemowe (Tajmery)		
Załączenie flagi	Wyłączenie flagi	Skutek załączenia flagi
Flaga ŚWIATŁO		
- Linie wejściowe: **[68]:Załącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** - Klawisze funkcyjne: **[68]:Załącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** - Komendy z klawiatury: **[F21]:Załącz ŚWIATŁO** **[F23]:Przełącz ŚWIATŁO**	- Automatycznie z chwilą upłynięcia czasu określonego przez Tajmer ŚWIATŁO; - Linie wejściowe: **[69]:Wyłącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** - Klawisze funkcyjne: **[69]:Wyłącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** - Komendy z klawiatury: **[F22]:Wyłącz ŚWIATŁO** **[F23]:Przełącz ŚWIATŁO**	- Linia wyjściowa: **[64]: ŚWIATŁO**
Flaga TAMPER		
- Linia wejściowa: **[08]:TAMPER**	- Z chwilą upłynięcia czasu określonego przez Tajmer TAMPER - Rozbrojenie kontrolera - Klawisz funkcyjny: **[77]: Wyłącz WŁAMANIE i TAMPER** - Komenda z klawiatury: **[F31]: Wyłącz WŁAMANIE i TAMPER**	- Flaga: WŁAMANIE - Linie wyjściowe: **[65]: TAMPER** **[68]: WŁAMANIE** - Zdarzenia alarmowe: **[540]: Alarm Tamper** **[052]: Załączono WŁAMANIE**
Flaga AUX1		
- Linie wejściowe: **[71]:Załącz AUX1** **[73]:Przełącz AUX1** - Klawisze funkcyjne: **[71]:Załącz AUX1** **[73]:Przełącz AUX1** - Komendy z klawiatury: **[F24]:Załącz AUX1** **[F26]:Przełącz AUX1**	- Z chwilą upłynięcia czasu określonego przez Tajmer AUX1 - Linie wejściowe: **[72]:Wyłącz AUX1** **[73]:Przełącz AUX1** - Klawisze funkcyjne: **[72]:Wyłącz AUX1** **[73]:Przełącz AUX1** - Komendy z klawiatury: **[F25]:Wyłącz AUX1** **[F26]:Przełącz AUX1**	- Linia wyjściowa **[66]: AUX1**

Flaga AUX2		
- Linie wejściowe: **[74]:Ustaw AUX2** **[76]:Przełącz AUX2** - Klawisze funkcyjne: **[74]:Załącz AUX2** **[76]:Przełącz AUX2** - Komendy z klawiatury: **[F27]:Załącz AUX2** **[F29]:Przełącz AUX2**	- Z chwilą upłynięcia czasu określonego przez Tajmer AUX2 - Linie wejściowe: **[75]:Wyłącz AUX2** **[76]:Przełącz AUX2** - Klawisze funkcyjne: **[75]:Wyłącz AUX2** **[76]:Przełącz AUX2** - Komendy z klawiatury: **[F28]:Wyłącz AUX2** **[F29]:Przełącz AUX2**	- Linia wyjściowa **[67]: AUX2**
Flaga WŁAMANIE		
- Linie wejściowe: **[08]:TAMPER** **[09]:WŁAMANIE** - Klawisz funkcyjny: **[09]:WŁAMANIE** - Komenda z klawiatury: **[F30]: Załącz WŁAMANIE**	- Z chwilą upłynięcia czasu określonego przez Tajmer WŁAMANIE - Rozbrojenie kontrolera - Klawisz funkcyjny: **[77]: Wyłącz WŁAMANIE i TAMPER** - Komenda z klawiatury: **[F31]: Wyłącz WŁAMANIE i TAMPER**	- Linia wyjściowa: **[68]: WŁAMANIE** - Zdarzenie alarmowe: **[052]: Załączono WŁAMANIE**
Flaga WEJŚCIE SIŁOWE		
- Linia wejściowa **[01]: Czujnik otwarcia drzwi** gdy kontroler nie udzielił dostępu - wprowadzenie kodu PIN różniącego się o +/-1 na ostatniej pozycji od kodu prawidłowego (patrz 4.6 Zakładka Opcje)	- Z chwilą upłynięcia czasu określonego przez Tajmer WEJŚCIE SIŁOWE - Użycie uprawnionego identyfikatora (karta i/lub kod PIN) - Rozbrojenie/uzbrojenie kontrolera	- Linie wyjściowe: **[28]: WEJŚCIE SIŁOWE** **[256]: ALARM DRZWI** - Zdarzenie alarmowe: **[005]: WEJŚCIE SIŁOWE** lub **[017]: Wejście pod przymusem**
Flaga PREALARM		
- pięciokrotne użycie nieznanego identyfikatora (karta i/lub kod PIN) na danym kontrolerze w ciągu 5 minut	- Z chwilą upłynięcia czasu określonego przez Tajmer PREALARM - Użycie uprawnionego identyfikatora (karta i/lub kod PIN) - Rozbrojenie/uzbrojenie kontrolera	- Linie wyjściowe: **[29]: PREALARM** **[256]: ALARM DRZWI** - Zdarzenie alarmowe: **[003]: PREALARM**

Flaga DRZWI OTWARTE		
- Linia wejściowa: **[01]: Czujnik otwarcia drzwi** gdy minął czas określony przez opcję CZAS NA WEJŚCIE a linia jest nadal aktywna (czujnik wykrywa otwarcie drzwi)	- Z chwilą zaniku sygnału na linii wejściowej: **[01]: Czujnik otwarcia drzwi** - Z chwilą upłynięcia czasu określonego przez Tajmer DRZWI OTWARTE - Użycie uprawnionego identyfikatora (karta i/lub kod PIN) - Rozbrojenie/uzbrojenie kontrolera Uwaga: Najwyższy priorytet ma załączenie linii wejściowej **[01]: Czujnik otwarcia drzwi**. Tajmer DRZWI OTWARTE jest aktywny tak długo jak wspomniana linia wejściowa jest załączona. Gdy wykryte zostanie zamknięcie drzwi to flaga DRZWI OTWARTE jest od razu wyłączona bez względu na jej Tajmer.	- Linie wyjściowe: **[30]: DRZWI OTWARTE** **[256]: ALARM DRZWI** - Zdarzenie alarmowe: **[004]: DRZWI OTWARTE**

Uwaga: Występowanie sygnałów na linii wyjściowej **[256]: ALARM DRZWI** może być zablokowane za pomocą opcji dostępnych w programie PR Master (patrz 4.6 Zakładka Opcje).

3.11 Antypowrót (ang. Anti-passback)

W przypadku załączenia funkcji Anti-passback użytkownik jest zobligowany do logowania się naprzemiennie raz na wejściu raz na wyjściu z pomieszczenia/strefy. Kontroler w sposób ciągły rejestruje, na którym czytniku użytkownik się ostatnio zalogował i dane te przechowuje w tzw. Rejestrze APB. Stan tego rejestru wskazuje ostatnie miejsce logowania użytkowników. Zasady APB mogą być stosowane w odniesieniu do pojedynczego przejścia lub większego obszaru zwanego Strefą Anti-passback (Strefa APB). Strefy APB są definiowane niezależnie od istniejących w systemie stref innego typu (np. Stref Dostępu czy Stref Alarmowych), aczkolwiek mogą się z nimi pokrywać. Ze względu na to czy funkcja APB odnosi się do pojedynczego przejścia czy też obszaru złożonego z wielu przejść rozróżnia się:

- APB Lokalny,
- APB Globalny.

APB Lokalny dotyczy sytuacji, kiedy zasady APB są stosowane w odniesieniu do pojedynczego przejścia (pojedynczego kontrolera). Gdy obowiązuje lokalny APB użytkownik musi się logować naprzemiennie raz na czytniku wejściowym raz na wyjściowym z pomieszczenia przy czym obydwa czytniki muszą być podłączone do tego samego kontrolera. Domyślnie czytnik o adresie ID=0 jest traktowany jako czytnik wejściowy natomiast czytnik o adresie ID=1 jako czytnik wyjściowy, przyporządkowanie to może być jednak zmienione we właściwościach kontrolera (patrz 4.2 Zakładka Terminal ID1).
APB Globalny dotyczy sytuacji kiedy zasady APB nie są stosowane w odniesieniu do pojedynczego przejścia lecz w odniesieniu do większego obszaru zwanego Strefą APB. W skład Strefy APB mogą wchodzić czytniki podłączone do różnych kontrolerów w ramach danego podsystemu. Gdy obowiązuje APB Globalny to aby wyjść z danej Strefy APB użytkownik musi najpierw do niej wejść i

vice versa. APB Globalny może być stosowany w systemach posiadających minimum dwa kontrolery, dodatkowo w systemie musi być zainstalowana centrala CPR
Ze względu na sposób reakcji kontrolera na naruszanie zasad APB rozróżnia się:

- APB Twardy,
- APB Miękki.

Gdy na kontrolerze obowiązuje Anti-passback Miękki to każda próba naruszenia zasad APB wywołuje jedynie rejestrację zdarzenia **[509]: Naruszenie zasad APB**, które informuje o fakcie naruszenia zasad APB, ale kontroler nie blokuje dostępu. Gdy na kontrolerze obowiązuje Anti-passback Twardy to próba naruszenia zasad APB wywołuje odmowę dostępu (dwa długie sygnały dźwiękowe) oraz rejestrację zdarzenia **[509]: Naruszenie zasad APB**.
Oprócz tego wyróżnia się jeszcze APB z obsługą czujnika otwarcia drzwi (ang. True APB). Normalnie po przyznaniu dostępu, kontroler uznaje, że dany użytkownik wszedł (wyszedł) z pomieszczenia i stosownie do tego uaktualnia Rejestr APB. W przypadku zastosowania APB z obsługą czujnika otwarcia drzwi, aktualizacja Rejestru APB jest dokonywana dopiero wtedy gdy kontroler rozpozna, że po przyznaniu dostępu drzwi zostały otwarte, z kolei gdy to nie nastąpi to kontroler nie zmienia stanu Rejestru APB i uznaje, że użytkownik nie wszedł pomimo tego, że kontroler przyznał mu dostęp. Działanie tej opcji wymaga, podłączenia czujnika otwarcia drzwi do jednej z linii wejściowych kontrolera i ustawienia funkcji **[01]: Czujnik otwarcia drzwi** dla tej linii.
Opcje związane z APB są dostępne we właściwościach kontrolera w programie PR Master (patrz 4.8 Zakładka APB).

Uwaga: Po wykonaniu operacji zerowania Rejestru APB każdy użytkownik może dokonać logowania na dowolnym z czytników (wejściowym lub wyjściowym), lecz potem, od momentu pierwszego logowania musi się już stosować do zasad APB, czyli logować się naprzemiennie na wejściu i wyjściu

---

Strefy Anti-passback (Strefy APB)

Przez pojęcie Strefy APB rozumie się pewien wybrany obszar systemu kontroli dostępu, do którego dostęp jest nadzorowany przez wiele punktów identyfikacji (czytników). Definicja Strefy APB składa się z listy czytników, które kontrolują wejście do niej oraz listy czytników wyjściowych z danej Strefy APB. Jako że każdy kontroler serii PRxx2 może nadzorować tylko jedno przejście dwustronne to musi być on zlokalizowany na granicy dwóch Stref APB. Jeśli jeden z czytników dołączonych do kontrolera dozoruje wejście do Strefy APB, to drugi z nich dozoruje wyjście z niej. Nie dopuszcza się sytuacji, aby obydwa czytniki dołączone do tego samego kontrolera kontrolowały wejście do tej samej Strefy APB.

Uwaga: Nie jest konieczne, aby każdy kontroler serii PRxx2 leżący na granicy dwóch Stref APB posiadał dwa czytniki, wejście i wyjście ze strefy APB może być dozorowane przez osobne kontrolery.

W każdym systemie KD występuje jedna, predefiniowana Strefa APB zwana strefą publiczną. Strefa publiczna to teren otaczający obszar nadzorowany przez system kontroli dostępu. Na przykład, jeśli system KD jest zainstalowany w budynku, wówczas wychodząc z budynku przechodzi się do strefy publicznej i odwrotnie, wchodząc do budynku opuszcza się strefę publiczną.

Uwaga: W systemie RACS 4 Strefa APB może obejmować tylko kontrolery należące do tego samego Podsystemu. Nie można zdefiniować Strefy APB zawierającej kontrolery zlokalizowane w różnych Podsystemach.

W przypadku Strefy APB możliwe jest zdefiniowanie przejścia wewnętrznego poprzez przypisanie danego kontrolera (wraz z czytnikami) to danej Strefy APB w zakładce **APB** (patrz 4.8 Zakładka APB). Użytkownikowi może zostać udzielony dostęp na takim przejściu jedynie wtedy gdy przebywa on już w danej Strefie APB tzn. wszedł do niej poprzez jeden z punktów/terminali wejściowych. W praktycznych zastosowaniach kontroler pełniący przejścia wewnętrznego wcale nie musi być zlokalizowany w pomieszczeniu lub obszarze podlegającym kontroli APB. Można sobie więc

wyobrazić zastosowanie mechanizmu przejścia wewnętrznego także do kontrolowania trasy poruszania się użytkowników w budynku.

Rejestr APB

Rejestr APB to obszar pamięci kontrolera, w której przechowywane są informacje wskazujące, po której stronie przejścia (na którym czytniku, wejściowym czy wyjściowym) miało miejsce ostatnie logowanie użytkowników.
Zerowanie Rejestru APB powoduje, że każdy użytkownik może dokonać pierwszego logowania na dowolnym z czytników (wejściowym lub wyjściowym), lecz potem, od momentu pierwszego logowania musi się już stosować do zasad APB, czyli logować się naprzemiennie raz na wejściu raz na wyjściu.
Zerowanie Rejestru APB jest wykonywane automatycznie po włączeniu zasilania, może być również wykonane następującymi metodami:

- Z poziomu linii wejściowej – patrz 3.13 Linie wejściowe kontrolera,
- Z klawisza funkcyjnego - patrz 3.15 Klawisze funkcyjne,
- Zdalnie z komputera zarządzającego z programem PR Master – polecenie **Zeruj Rejestr APB** jest dostępne po kliknięciu kontrolera prawym przyciskiem myszy w oknie głównym programu PR Master,
- Zdalnie z komputera zarządzającego z programem PR Master – polecenie **Zeruj Globalny Rejestr APB** jest dostępne po kliknięciu podsystemu prawym przyciskiem myszy w oknie głównym programu PR Master,
- Manualnie przy pomocy komendy z klawiatury kontrolera lub dołączonego do niego czytnika PRT z klawiaturą - patrz 3.18 Komendy z klawiatury,
- Automatycznie za pomocą Harmonogramu – opcja **Harmonogramy** w oknie głównym programu PR Master i zakładka **APB** – patrz 4.8 Zakładka APB.

Hierarchia Stref APB

Hierarchia Stref APB odzwierciedla relacje terytorialne pomiędzy różnymi Strefami APB zdefiniowanymi w ramach jednego podsystemu KD. Gdy jest ona załączona to użytkownicy mogą przemieszczać się tylko pomiędzy sąsiednimi Strefami APB. Strefy sąsiednie w rozumieniu zasad globalnego APB to takie strefy, pomiędzy którymi istnieją przejścia. W rezultacie działania hierarchii APB system KD nie pozwala na wejście do danej Strefy APB inaczej jak tylko ze strefy bezpośrednio z nią sąsiadującej. Hierarchię APB można programowo wyłączyć, wtedy użytkownik może opuścić daną Strefę APB i wejść do innej Strefy APB, niezależnie od tego, czy obie strefy są połączone bezpośrednim przejściem czy nie. Hierarchia Stref APB może być załączona i wyłączona w oknie otwieranym za pomocą opcji **Strefy APB** w oknie głównym programu PR Master.

Uwagi:
1. Pod pojęciem przejścia rozumie się kontroler, który leży na granicy dwóch Stref APB.
2. Sąsiednie Strefy APB to strefy, pomiędzy którymi istnieje przejście dozorowane przez jeden kontroler (jeden czytnik kontrolera należy do jednej strefy a drugi czytnik do drugiej strefy).
3. Hierarchia Stref APB powstaje automatycznie w wyniku przypisania poszczególnych czytników do istniejących w systemie Stref APB. Modyfikacji hierarchii Stref APB można dokonać jedynie poprzez reorganizację przypisania czytników do poszczególnych Stref APB.

Procedura ustawienia APB lokalnego za pomocą programu PR Master

1. We właściwościach kontrolera (program PR Master) przejść do zakładki **Zaawansowane** a następnie zaznaczyć opcję **Załącz APB (Anti-passback)**.
2. W razie potrzeby w zakładce **Zaawansowane** zaznaczyć czy stosowany będzie True APB z obsługą czujnika otwarcia drzwi, przypisać harmonogram APB Twardy/Miękki, harmonogram zerowania Rejestru APB oraz limit osób przebywających w pomieszczeniu. Można przypisać jeden z harmonogramów wbudowanych lub zdefiniować własny za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.

3. We właściwościach kontrolera, w zakładce **Terminal ID1**, w polu **Lokalizacja czytnika** w zależności od potrzeb wybrać opcję **Wejście do pomieszczenia** lub **Wyjście z pomieszczenia**.
4. Przesłać ustawienie do kontrolerów za pomocą programu PR Master.
5. Rejestr APB można wyzerować klikając kontroler prawym przyciskiem myszy w oknie głównym programu PR Master i wybierając opcję **Zeruj Rejestr APB**. Można również przejrzeć rejestr wybierając opcję **Lista zalogowanych na czytniku wejściowym**.

Procedura ustawienia APB Globalnego za pomocą programu PR Master

1. Zdefiniować nazwy stref za pomocą opcji **Strefy APB** w oknie głównym programu PR Master i w razie potrzeby zaznaczyć opcję **Hierarchia APB** oraz ustalić limit użytkowników w Strefach APB.
2. We właściwościach kontrolera przejść do zakładki **APB** a następnie zaznaczyć opcję **Załącz APB (Anti-passback)**.
3. W razie potrzeby w zakładce **APB** zaznaczyć czy stosowany będzie True APB z obsługą czujnika otwarcia drzwi, przypisać harmonogram APB Twardy/Miękki oraz harmonogram zerowania Rejestru APB. Można przypisać jeden z harmonogramów wbudowanych lub zdefiniować własny za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
4. Przypisać czytniki kontrolera do Stref APB przechodząc do właściwości kontrolera a następnie zakładki **Terminal ID1**. W polu **Strefa APB (Globalny APB)** wybrać strefę z listy rozwijanej. Terminal ID1 stanie się terminalem wejściowym do tej strefy. Przejść do zakładki **Terminal ID0** we właściwościach tego samego kontrolera i analogicznie w polu **Strefa APB (Globalny APB)** wybrać strefę, dla której Terminal ID0 będzie terminalem wejściowym. W ustawieniach można wykorzystać wbudowaną Strefę APB o nazwie Strefa Domyślna. Po tym ustawieniu odpowiednie czytniki będą wyświetlane dla określonych Stref APB w oknie opcji **Strefy APB**, dostępnej w oknie głównym programu PR Master.
5. Analogiczną operację wykonać dla kolejnych kontrolerów Strefy Globalnego APB w ramach tego samego podsystemu oraz dla kolejnych Stref APB jeżeli są one stosowane.
6. Zweryfikować ustawienia terminali w oknie opcji **Strefy APB** dostępnej w oknie głównym programu PR Master.
7. Przesłać ustawienie do kontrolerów i centrali CPR za pomocą programu PR Master.
8. Rejestr APB można wyzerować klikając kontroler prawym przyciskiem myszy i wybierając opcję **Zeruj Rejestr APB.** Można również przejrzeć rejestr wybierając opcję **Odczytaj Rejestr APB**. Zerowanie i odczyt można również zrealizować globalnie klikając prawym przyciskiem myszy Podsystem w oknie głównym programu PR Master i wybierając odpowiednią opcję z listy.

3.12 Strefy Alarmowe

Mechanizm Stref Alarmowych jest wykorzystywany w integracji systemu kontroli dostępu RACS 4 z centralami alarmowymi. Strefa Alarmowa to grupa kontrolerów współbieżnie zmieniających swój aktualny stan uzbrojenia. Gdy dowolny kontroler należący do danej Strefy Alarmowej zmieni swój stan uzbrojenia (przy czym nie jest istotne co było przyczyną zmiany trybu uzbrojenia) reszta kontrolerów wchodzących w skład tej samej Strefy Alarmowej zostaje automatycznie przezbrojona w ten sam sposób. Mechanizm Stref Alarmowych wymaga instalacji centrali CPR, która w sposób ciągły monitoruje stany uzbrojenia wszystkich kontrolerów w systemie i gdy jeden z nich zmieni swój stan uzbrojenia centrala przezbraja w ten sam sposób pozostałe kontrolery wchodzące w skład tej samej Strefy Alarmowej. W efekcie działania tego mechanizmu wszystkie kontrolery wchodzące w skład tej samej Strefy Alarmowej posiadają w każdej chwili działania systemu ten sam stan uzbrojenia.

Uwaga: Stosowanie mechanizmu Stref Alarmowych nie blokuje innych metod przezbrajania kontrolerów.

Uwaga: W systemie RACS 4 możliwa jest obsługa maksymalnie 32 Stref Alarmowych.

Gdy sterowanie stanem uzbrojenia kontrolera jest realizowane za pośrednictwem linii wejściowej **[03]:Przezbrajanie – klucz stały**, to stan uzbrojenia danego kontrolera nie może być

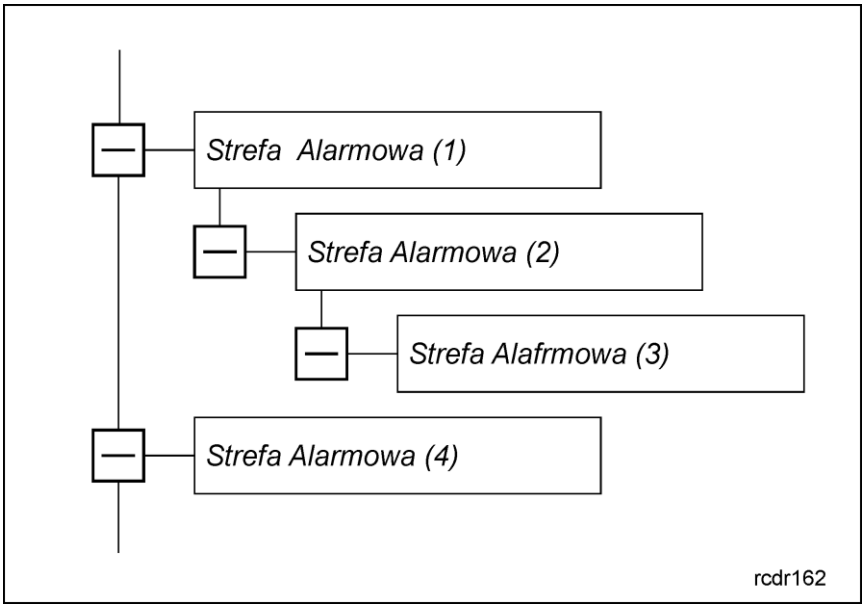
zmieniany innymi metodami. Jeżeli kontroler z wejściem **[03]** zostałby przypisany do jakiejś Strefy Alarmowej to i tak stan jego uzbrojenia będzie zależał jedynie od stanu linii wejściowej.

Hierarchia Stref Alarmowych

W systemie RACS 4 można zdefiniować jedną lub więcej Stref Alarmowych. Strefy Alarmowe mogą być zupełnie niezależne od siebie lub tworzyć pewną zhierarchizowaną strukturę gdzie występuje zasada nadrzędności i podrzędności. Gdy Strefy Alarmowe są niezależne, to zmiana stanu uzbrojenia dowolnej z nich (uzbrojenie lub rozbrojenie) nie ma wpływu na stan uzbrojenia stref pozostałych. Gdy między strefami jest zdefiniowania hierarchia to między strefami może zachodzić relacja podrzędności lub nadrzędności. Jeśli taka relacja została zdefiniowana to zachodzą następujące zależności:

- Uzbrojenie strefy nadrzędnej powoduje uzbrojenie wszystkich stref względem niej 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.

W systemie RACS 4 definiowanie hierarchii stref alarmowych następuje za pomocą struktury drzewa, które odzwierciedla wzajemne zależności pomiędzy strefami alarmowymi.



Rys. 8 Hierarchia stref alarmowych

W przedstawionym przykładzie strefa (4) jest niezależna od wszystkich pozostałych stref alarmowych. Strefa (2) jest podrzędna względem strefy (1) natomiast strefa (3) jest podrzędna względem strefy (2). Uzbrojenie strefy (1) powoduje uzbrojenie stref (2) i (3), natomiast uzbrojenie strefy (2) powoduje uzbrojenie strefy (3).

Procedura ustawienia Stref Alarmowych

1. Zdefiniować nazwy stref za pomocą opcji **Strefy Alarmowe** w oknie głównym programu PR Master wybierając jednocześnie podsystem, harmonogram oraz opcjonalnie załączając Hierarchę Stref Alarmowych. Wybranie wbudowanego harmonogramu Zawsze lub harmonogramu Nigdy w istocie oznacza rezygnację z automatycznego uzbrajania/rozbrajania Stref Alarmowych i decyduje jedynie o domyślnym stanie uzbrojenia kontrolera/-ów. Własny harmonogram można utworzyć za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
2. We właściwościach kontrolera przejść do zakładki **Przezbrajanie** a następnie zaznaczyć opcję **Załącz Harmonogram Przezbrajania**.
3. W tej samej zakładce można zdefiniować dodatkowe parametry samouzbrajania związane z opóźnianiem i ostrzeżeniami akustycznymi.

4. W przypadku Stref Alarmowych jej obszar jest definiowany poprzez przypisanie kontrolerów a nie poszczególnych terminali (ID1, ID0). Przypisanie kontrolera polega na załączeniu Harmonogramu Przezbrajania.
5. Zweryfikować ustawienia w oknie opcji **Strefy Alarmowe** dostępnej w oknie głównym programu PR Master.
6. Przesłać ustawienia do kontrolerów i centrali CPR.

Opcje związane z przezbrajaniem i samouzbrajaniem są dostępne we właściwościach kontrolera w programie PR Master (patrz 4.5 Zakładka Przezbrajanie).

3.13 Linie wejściowe kontrolera

Ilość dostępnych programowalnych linii wejściowych zależy od typu kontrolera – patrz tabela 1. Opcjonalnie kontrolery serii PRxx2 mogą obsługiwać dwa dodatkowe wejścia znajdujące się na zewnętrznym ekspanderze XM-2. Każdą linię wejściową można indywidualnie skonfigurować co do funkcji, harmonogramu, warunków dodatkowych, sposobu wyzwalania (NO/NC) oraz domyślnego Trybu RCP we właściwościach kontrolera w programie PR Master (patrz 4.11 Zakładki Wejście IN1…IN8). Wyzwolenie linii NO następuje przez zwarcie jej z minusem zasilania, linia typu NC musi być normalnie zwarta z minusem zasilania, wyzwolenie jej następuje przez odjęcie minusa zasilania. Dodatkowo funkcje linii dzielą się na funkcje typu klucz stały i klucz chwilowy. Rodzaj klucza linii określa czy kontroler reaguje jedynie w chwili wyzwolenia linii (klucz chwilowy) czy na każdą zmianę jej stanu (klucz stały). Dla przykładu linia z funkcją **[01]: Czujnik otwarcia drzwi** jest linią typu klucz stały i kontroler reaguje zarówno na jej wyzwolenie jak i powrót do stanu normalnego, linia z funkcją **[02]: Przycisk wyjścia** jest linią typu klucz chwilowy – kontroler reaguje tylko na jej wyzwolenie.

Tabela 7 Funkcje linii wejściowych

Kod	Nazwa funkcja	Klucz	Opis działania
[00]	**Wejście wyłączone**	Brak	Linia wyłączona.
[01]	**Czujnik otwarcia drzwi**	Stały	Linia jest dedykowana do podłączenia czujnika otwarcia drzwi. Gdy linia jest wyzwolona kontroler uznaje, że drzwi są otwarte a gdy linia jest w stanie normalnym uznaje, że drzwi są zamknięte.
[02]	**Przycisk wyjścia**	Chwilowy	Wejście jest przeznaczone do podłączenia tzw. przycisku wyjścia od środka lub innego typu kontaktu, którego użycie ma zwalniać drzwi. Wyzwolenie linii powoduje zwolnienie drzwi na zasadach identycznych jak po przyznaniu dostępu.
[03]	**Przezbrajanie - klucz stały**	Stały	Linia ta służy do sterowania aktualnym stanem uzbrojenia. Gdy linia jest załączona to kontroler jest utrzymywany w stanie rozbrojenia a gdy nie jest załączona to kontroler jest utrzymywany w stanie uzbrojenia. Uwaga: W kontrolerze może być zdefiniowana tylko jedna linia tego typu. Ta linia ma najwyższy priorytet spośród wszystkich metod przezbrajania.

[05]	**Dozór napięcia sieci AC**	Stały	Gdy linia jest w stanie normalnym to jest to informacja dla kontrolera, że zasilanie sieciowe 230VAC zewnętrznego zasilacza z wyjściem 12VDC jest obecne. Gdy linia jest wyzwolona to oznacza to, że zasilania sieciowego nie ma. Wejście **[05]** może być wykorzystywane do połączenia z liniami wyjściowymi modułu PSAM-1 współpracującego z zasilaczami PS20 lub z liniami wyjściowymi zasilaczy innych producentów o ile oferują one funkcjonalność dozorowania napięcia sieciowego. Uwaga: Niezależnie od wejścia **[05]**, kontroler PR402 dozoruje obecność napięcia zasilającego 18VAC o ile jest ono doprowadzone do jego zacisków poprzez transformator.
[06]	**Dozór stanu akumulatora**	Stały	Gdy linia jest w stanie normalnym to jest to informacja dla kontrolera, że stan akumulatora rezerwowego w zewnętrznym zasilaczu jest właściwy. Gdy linia jest wyzwolona to oznacza to, że stan tego akumulatora jest niezadowalający. Wejście **[06]** może być wykorzystywane do połączenia z liniami wyjściowymi modułu PSAM-1 współpracującego z zasilaczami PS20 i akumulatorami lub z liniami wyjściowymi urządzeń innych producentów o ile oferują one funkcjonalność dozorowania stanu akumulatora. Uwaga: Niezależnie od wejścia **[06]** kontroler PR402 dozoruje stan akumulatora rezerwowego, jeżeli jest on dołączony bezpośrednio do jego zacisków.
[07]	**Dzwonek**	Stały	Wyzwolenie linii załącza sygnał dźwiękowy dzwonka na wewnętrznym głośniku kontrolera (4 sek.) i opcjonalnie na linii wyjściowej z funkcją **[15]:Dzwonek** (4 sek.).
[08]	**TAMPER**	Chwilowy	Wyzwolenie linii jest interpretowane jako naruszenie obwodu antysabotażowego i powoduje załączenie Flag Systemowych TAMPER oraz WŁAMANIE. Styk antysabotażowy w kontrolerach PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302 jest podłączony do osobnych przewodów lub zacisków, które można z kolei połączyć z linią wejściową kontrolera z funkcją **[08]** albo połączyć z dowolnym urządzeniem zewnętrznym np. syreną alarmową.
[09]	**WŁAMANIE**	Chwilowy	Wyzwolenie linii jest interpretowane jako zadziałanie podłączonego do niej czujnika alarmowego i powoduje załączenie Flagi Systemowej WŁAMANIE.
[11]	**Blokada dostępu**	Stały	Gdy linia jest wyzwolona kontroler bezwarunkowo blokuje możliwość przyznania dostępu.

[13]	**Blokada uzbrojenia**	Stały	Gdy linia jest wyzwolona to kontroler nie może być uzbrajany za pomocą identyfikatora (karty, kodu PIN) oraz wejścia czy klawisza funkcyjnego. Z kolei uzbrajanie na bazie harmonogramu jest opóźniane (patrz 4.5 Zakładka Przezbrajanie).
[14]	**Zwolnij drzwi - klucz stały**	Stały	Przez cały okres wyzwolenia linii kontroler ustawia drzwi w Trybie Odblokowane tzn. udziela dostępu każdemu.
[44]	**Chwilowa emulacja terminala ID1**	Chwilowy	W wyniku samego przypisania funkcji **[44]** do jednego z wejść, przyznanie dostępu osobie uprawnionej za pomocą karty/kodu PIN skutkuje zdarzeniem **[547]: Przyznanie dostępu – tryb specjalny** zamiast domyślnego zdarzenia **[001]: Przyznanie dostępu**. Zdarzenie **[547]** jest ignorowane w Raporcie Obecności programu PR Master. W wyniku wyzwolenia linii **[44]**, tryb emulacji ID1 trwa do momentu najbliższego logowania, lecz nie dłużej niż 8 sekund a logowanie uprawnionego użytkownika skutkuje zdarzeniem **[001]: Przyznanie dostępu**. Uwaga: Funkcja **[44]** nie jest dostępna dla kontrolerów PR402 i PR102DR.
[45]	**Chwilowa emulacja terminala ID0 przez terminal ID1**	Chwilowy	W wyniku wyzwolenia linii kontroler z wbudowanym czytnikiem Terminal ID1 przełącza się do trybu emulacji Terminala ID0. Tryb emulacji trwa do momentu najbliższego logowania, lecz nie dłużej niż 8 sekund a logowanie uprawnionego użytkownika skutkuje zdarzeniem **[001]: Przyznanie dostępu**. Uwaga: Funkcja **[45]** nie jest dostępna dla kontrolerów PR402 i PR102DR.
[46]	**Losowa kontrola - potwierdzenie**	Chwilowy	Wyzwolenie linii powoduje skasowanie sygnalizacji żądania losowej kontroli użytkownika. Linia jest wykorzystywana tylko przy załączonej opcji: **Losowa kontrola użytkownika wymaga potwierdzenia** (patrz 4.7 Zakładka Zaawansowane).
[47]	**Przycisk wejścia**	Chwilowy	Wyzwolenie linii powoduje zwolnienie drzwi na zasadach identycznych jak po przyznaniu dostępu. Wejście takie jest przeznaczone do podłączenia tzw. przycisku wejścia lub innego typu kontaktu, którego użycie ma zwalniać drzwi. Funkcja **[47]** działa podobnie jak funkcja **[02].**
[48]	**Wybierz tryb RCP z klawiatury - zmiana trwała**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[49]	**Wybierz tryb RCP z klawiatury - zmiana chwilowa**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).

[50]	**Następny tryb RCP - zmiana trwała**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master). Funkcja **[50]** jest dostępna jedynie w kontrolerach PR602LCD-DT i PR602LCD.
[51]	**Następny tryb RCP - zmiana chwilowa**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master). Funkcja **[51]** jest dostępna jedynie w kontrolerach PR602LCD-DT i PR602LCD.
[56]	**Ustaw predefiniowany tryb RCP – zmiana trwała**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[57]	**Ustaw predefiniowany tryb RCP – zmiana chwilowa**	Chwilowy	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[58]	**Załącz zwłokę przed samouzbrojeniem**	Chwilowy	Wyzwolenie linii przesuwa moment samouzbrojenia o czas określony przez parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem** (patrz 4.5 Zakładka Przezbrajanie).
[59]	**Kasuj zwłokę przed samouzbrojeniem**	Chwilowy	Wyzwolenie linii kasuje parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem** – kontroler natychmiast podejmuje próbę samouzbrojenia zgodnie z Harmonogramem Przezbrajania (patrz 4.5 Zakładka Przezbrajanie).
[60]	**Zeruj Rejestr APB**	Chwilowy	Wyzwolenie linii zeruje Rejestr APB. W efekcie wszyscy użytkownicy systemu mogą zalogować się na wejściu lub wyjściu Strefy APB ale w następnych krokach muszą przestrzegać zasad APB
[61]	**Przezbrajanie - klucz chwilowy**	Chwilowy	Wyzwolenie linii powoduje trwałe przełączenie aktualnego stanu uzbrojenia kontrolera.
[62]	**Wyłącz wyjścia na modułach XM-8**	Chwilowy	Wyzwolenie linii wyłącza wszystkie wyjścia przekaźnikowe ekspanderów XM-8 dołączonych do kontrolera.
[63]	**Załącz wyjścia na modułach XM-8**	Chwilowy	Wyzwolenie linii załącza wszystkie wyjścia przekaźnikowe ekspanderów XM-8 dołączonych do kontrolera.
[64]	**Ustaw drzwi w tryb Normalny**	Chwilowy	Wyzwolenie linii ustawia Tryb Drzwi Normalny.
[65]	**Ustaw drzwi w tryb Odblokowane**	Chwilowy	Wyzwolenie linii ustawia Tryb Drzwi Odblokowane.
[66]	**Ustaw drzwi w tryb War. Odblokowane**	Chwilowy	Wyzwolenie linii ustawia Tryb Drzwi Warunkowo Odblokowane.
[67]	**Ustaw tryb drzwi Zablokowane**	Chwilowy	Wyzwolenie linii ustawia Tryb Drzwi Zablokowane.
[68]	**Załącz ŚWIATŁO**	Chwilowy	Wyzwolenie linii załącza Flagę (Tajmer) ŚWIATŁO.
[69]	**Wyłącz ŚWIATŁO**	Chwilowy	Wyzwolenie linii wyłącza Flagę (Tajmer) ŚWIATŁO.

[70]	**Przełącz ŚWIATŁO**	Chwilowy	Wyzwolenie linii przełącza Flagę (Tajmer) ŚWIATŁO do stanu przeciwnego.
[71]	**Załącz AUX1**	Chwilowy	Wyzwolenie linii załącza Flagę (Tajmer) AUX1.
[72]	**Wyłącz AUX1**	Chwilowy	Wyzwolenie linii wyłącza Flagę (Tajmer) AUX1.
[73]	**Przełącz AUX1**	Chwilowy	Wyzwolenie linii przełącza Flagę (Tajmer) AUX1 do stanu przeciwnego.
[74]	**Załącz AUX2**	Chwilowy	Wyzwolenie linii załącza Flagę (Tajmer) AUX2.
[75]	**Wyłącz AUX2**	Chwilowy	Wyzwolenie linii wyłącza Flagę (Tajmer) AUX2.
[76]	**Przełącz AUX2**	Chwilowy	Wyzwolenie linii przełącza Flagę (Tajmer) AUX2 do stanu przeciwnego.
[78]	**Ustaw tryb Rozbrojony**	Chwilowy	Wyzwolenie linii przełącza trwale kontroler do trybu rozbrojenia.
[79]	**Ustaw tryb Uzbrojony**	Chwilowy	Wyzwolenie linii przełącza trwale kontroler do trybu uzbrojenia.
[84]	**Ustaw tryb Karta lub PIN dla terminala ID0**	Chwilowy	Wyzwolenie linii ustawia tryb Karta lub PIN dla terminala ID0.
[85]	**Ustaw tryb Tylko Karta dla term.ID0**	Chwilowy	Wyzwolenie linii ustawia tryb Tylko Karta dla terminala ID0.
[86]	**Ustaw tryb Tylko PIN dla term.ID0**	Chwilowy	Wyzwolenie linii ustawia tryb Tylko PIN dla terminala ID0.
[87]	**Ustaw tryb Karta i PIN dla term.ID0**	Chwilowy	Wyzwolenie linii ustawia tryb Karta i PIN dla terminala ID0.
[88]	**Ustaw tryb Karta lub PIN dla term.ID1**	Chwilowy	Wyzwolenie linii ustawia tryb Karta lub PIN dla terminala ID1.
[89]	**Ustaw tryb Tylko Karta dla term.ID1**	Chwilowy	Wyzwolenie linii ustawia tryb Tylko Karta dla terminala ID1.
[90]	**Ustaw tryb Tylko PIN dla term.ID1**	Chwilowy	Wyzwolenie linii ustawia tryb Tylko PIN dla terminala ID1.
[91]	**Ustaw tryb Karta i PIN dla term.ID1**	Chwilowy	Wyzwolenie linii ustawia tryb Karta i PIN dla terminala ID1.

Uwaga: Zdefiniowanie linii wejściowej do funkcji **[01]:Czujnik otwarcia drzwi, [03]:Przezbrajanie – klucz stały, [05]:Dozór napięcia sieci AC** oraz **[06]:Dozór stanu akumulatora** blokuje możliwość skonfigurowania kolejnego wejścia kontrolera do tej samej funkcji.

3.14 Linie wyjściowe kontrolera

Ilość programowalnych linii wyjściowych (przekaźnikowych i tranzystorowych) zależy od typu kontrolera – patrz tabela 1. Opcjonalnie kontrolery serii PRxx2 mogą obsługiwać dwa dodatkowe wyjścia przekaźnikowe znajdujące się na zewnętrznym ekspanderze XM-2. Każdą linię wyjściową można indywidualnie skonfigurować co do funkcji, harmonogramu oraz warunków dodatkowych we

właściwościach kontrolera w programie PR Master (patrz 4.13 Zakładki Wyjście REL1…REL2 oraz 4.12 Zakładki Wyjście IO1…IO2). Wyjścia przekaźnikowe REL1 i REL2 udostępniają po jednym izolowanym styku NO/NC/COM (w stanie normalnym kontakty NO-COM są rozwarte a kontakty NC-COM zwarte). Wyjścia tranzystorowe w stanie normalnym reprezentują stan wysokiej impedancji (rozwarcia), gdy wyzwolone podają minus zasilania. Każde z wyjść tranzystorowych może przełączać prąd o wartości do 1A i napięciu do 15VDC. Linie tranzystorowe posiadają wewnętrzne zabezpieczenia, które automatycznie wyłączają linie po przekroczeniu dopuszczalnego prądu. Domyślną funkcją wyjścia REL1 jest funkcja **[99]: Zamek drzwi**, która steruje elementem wykonawczym (zamkiem drzwi).

Tabela 8. Funkcje linii wyjściowych

Kod	Nazwa funkcji	Opis działania
[00]	**Tryb Rozbrojony**	Gdy kontroler jest w stanie uzbrojenia to linia ta jest wyłączona, gdy kontroler jest stanie rozbrojenia linia ta jest załączona. Funkcja działa odwrotnie niż funkcja **[35] Tryb Uzbrojony.**
[08]	**Sterowanie z PC**	Wyjście z funkcją **[08]** może być sterowane komendami z poziomu programu PR Master poprzez kliknięcie kontrolera prawym przyciskiem myszki i wybranie polecenia **Załącz/wyłącz linię wyjściową** albo poprzez wybranie polecenia **Sterowanie wyjściami** w Trybie Monitorowania programu PR Master. Można sterować jedynie wyjściami ogólnego przeznaczenia (IO1...IO2) i tylko tymi, do których przypisana jest funkcja **[08]** lub **[13]**.
[09]	**Przyznanie dostępu**	Wyjście jest załączone przez cały czas otwarcia drzwi za pomocą karty i/lub kodu PIN czyli przez czas ustawiony za pomocą opcji **CZAS NA WEJŚCIE** we właściwościach kontrolera (program PR Master).
[10]	**Status drzwi**	Wyjście to przechodzi do stanu załączenia w momencie otwarcia drzwi i pozostaje w tym stanie tak długo jak drzwi pozostają otwarte. Funkcja **[10]** w praktyce powtarza stan linii wejściowej kontrolera podłączonej do czujnika otwarcia i skonfigurowanej do funkcji **[01]: Czujnik otwarcia drzwi.**
[11]	**Odmowa dostępu**	Wyjście to jest załączane na czas około 2 sekund każdorazowo, gdy kontroler odmówi przyznania dostępu.
[12]	**Harmonogram czasowy**	Wyjście to przechodzi do stanu załączenia w przedziałach czasowych zdefiniowanych przez przypisany do niego harmonogram czasowy, przy czym przedziały Od… Do… wskazują kiedy linia ma być załączona. Harmonogram można zdefiniować za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
[13]	**Harmonogram czasowy + komenda zdalna z PC**	Działa jaki linia z funkcją **[12]**. Dodatkowo linia wyjściowa z funkcją **[13]** może być sterowana komendami z poziomu programu PR Master poprzez kliknięcie kontrolera prawym przyciskiem myszki i wybranie polecenia **Załącz/wyłącz linię wyjściową** albo poprzez wybranie polecenia **Sterowanie wyjściami** w Trybie Monitorowania programu PR Master. Można sterować jedynie wyjściami ogólnego przeznaczenia (IO1...IO2) i tylko tymi, do których przypisana jest funkcja **[13]** lub **[08]**.

[14]	**Logowanie na terminalu ID0**	Wyjście zostaje załączone w momencie logowania na terminalu ID0 i trwa w tym stanie do momentu logowania na terminalu ID1. Zazwyczaj funkcja ta jest wykorzystywana do sterowania kierunkiem obrotu bramki typu obrotowej (tripod) lub sterowania przejściem dwukierunkowym wtedy wskazuje ono kierunek przejścia.
[15]	**Dzwonek**	Wyjście jest załączane na czas 5 sekund w momencie wystąpienia sygnalizacji stanu Dzwonek. Sygnalizację dzwonka można wyzwolić przy pomocy klawisza funkcyjnego bądź z linii wejściowej z funkcją dzwonka.
[16]	**Pomieszczenie nie jest puste**	Wyjście załącza się w momencie wejścia pierwszej osoby do nadzorowanego pomieszczenia (Strefy APB) i pozostaje w tym stanie do momentu, kiedy ostatnia osoba opuści to pomieszczenie. Liczba użytkowników przebywających w pomieszczeniu jest wyznaczana na podstawie zawartości Rejestru APB, w którym są przechowywane dane o osobach, które weszły i wyszły z pomieszczenia.
[17]	**Osiągnięto limit osób w pomieszczeniu**	Wyjście zostaje załączone w momencie, gdy liczba osób znajdujących się w pomieszczeniu (Strefie APB) osiągnie limit. Wyjście zostaje wyłączone, gdy liczba osób wewnątrz pomieszczenia spadnie poniżej zdefiniowanego maksimum.
[18]	**Tryb Drzwi Normalny**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Normalny.
[19]	**Tryb Drzwi Odblokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Odblokowane.
[20]	**Tryb Drzwi War. Odblokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: War. Odblokowane.
[21]	**Tryb Drzwi Zablokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Zablokowane.
[22]	**Zwłoka przed samouzbrojeniem w toku**	Wyjście sygnalizuje, że kontroler jest w trakcie odliczania zwłoki czasowej przed samoczynnym uzbrojeniem. Linia jest załączana na czas określony przez parametr **Domyślna zwłoka czasowa przed samouzbrojeniem** oraz przez parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem** (patrz 4.5 Zakładka Przezbrajanie) i pozostaje załączona do momentu uzbrojenia kontrolera.
[23]	**Głośnik zewnętrzny**	Wyjście jest przeznaczone do podłączenia zewnętrznego głośnika z wbudowanym generatorem akustycznym, który będzie sterowany na identycznych zasadach, co wewnętrzny głośnik kontrolera.
[24]	**Restart terminala**	Wyjście jest wyzwalane na czas ok. 2s za każdym razem jak kontroler rozpozna, że utracono komunikację z podłączonym do niego czytnikiem. Linię tego typu można wykorzystać do chwilowego zdjęcia zasilania z zewnętrznego czytnika w celu jego zresetowania. Uwaga: Kontroler może nadzorować poprawność komunikacji tylko z czytnikami serii PRT skonfigurowanymi do formatu RACS CLK/DTA (funkcja nie działa w przypadku czytników Wiegand i Magstripe).

[25]	**Impuls na rozbrojenie**	Wyjście jest wyzwalane na czas ok. 2s za każdym razem, gdy kontroler przejdzie do stanu rozbrojenia.
[26]	**Impuls na uzbrojenie**	Wyjście jest wyzwalane na czas ok. 2s za każdym razem, gdy kontroler przejdzie do stanu uzbrojenia.
[27]	**Żądanie uzbrojenia**	W ogólnym ujęciu wyjście **[27]** działa tak samo jak wyjście **[0]: Tryb rozbrojony** tj. linia załączona, gdy kontroler rozbrojony i wyłączona, gdy kontroler uzbrojony z tą różnicą, że linia **[27]** zmienia swój stan również podczas nieudanej próby uzbrojenia. Przykładowo, jeżeli kontroler jest rozbrojony i załączona jest linia wejściowa z funkcją **[13]: Blokada uzbrojenia** to próba uzbrojenia jedną z dostępnych metod będzie skutkować wyłączeniem linii **[27]** pomimo tego, że sam kontroler nie zmieni swojego stanu uzbrojenia.
[28]	**WEJŚCIE SIŁOWE**	Wyjście powtarza stan flagi WEJŚCIE SIŁOWE. Gdy flaga jest załączona to wyjście jest załączone, gdy flaga jest wyłączona to wyjście też jest wyłączone.
[29]	**PREALARM**	Wyjście powtarza stan flagi PREALARM. Gdy flaga jest załączona to wyjście jest załączone, gdy flaga jest wyłączona to wyjście też jest wyłączone.
[30]	**DRZWI OTWARTE**	Wyjście powtarza stan flagi DRZWI OTWARTE. Gdy flaga jest załączona to wyjście jest załączone, gdy flaga jest wyłączona to wyjście też jest wyłączone.
[31]	**Gong**	Wyjście załącza się na czas ok. 2s każdorazowo, gdy kontroler rozpozna, że drzwi zostały otwarte. Rozpoznanie wymaga dołączenia czujnika otwarcia drzwi do linii wejściowej kontrolera z funkcją **[01]: Czujnik otwarcia drzwi**. Samo przyznanie dostępu przez kontroler nie skutkuje wyzwoleniem linii wyjściowej z funkcją **[31].**
[32]	**Naruszenie APB**	Wyjście załącza się na czas około 2s w momencie naruszenia zasad APB. Nie dotyczy opcji limitu osób w pomieszczeniu, który jest ustawiany dla danej strefy APB. Do tego służy funkcja **[17].**
[33]	**Alert przed samouzbrojeniem - wyjście niemodulowane**	Wyjście jest wyzwalane gdy do momentu samouzbrojenia pozostał czas ustawiony za pomocą opcji **Alert przed samouzbrojeniem** (patrz 4.5 Zakładka Przezbrajanie). Wyjście jest wyłączane z chwilą, gdy czas ustawiony za pomocą wspomnianej opcji upłynie i kontroler zgodnie z harmonogramem przezbrajania przejdzie do stanu uzbrojenia.
[34]	**Alert przed samouzbrojeniem - wyjście modulowane**	Wyjście funkcjonuje tak samo jak wyjście z funkcją **[33]** z tą różnicą, że nie jest ono załączane na stałe. W przypadku załączenia funkcji **[34]** generowany jest podwójny impuls co 8 sekund.
[35]	**Tryb Uzbrojony**	Gdy kontroler jest w stanie uzbrojenia to linia ta jest załączona, gdy kontroler jest stanie rozbrojenia linia ta jest wyłączona. Funkcja działa odwrotnie niż funkcja **[00] Tryb Rozbrojony.**
[36]	**Impuls na przyznanie dostępu**	Wyjście jest wyzwalane na okres 1 sek. po przyznaniu dostępu przez kontroler.

[37]	**Utrata napięcia sieci AC**	Wyjście jest wyzwalane po około 8 minutach od momentu utraty zasilania 18VAC i powraca do stanu normalnego po około 40 sekundach od wykrycia powrotu zasilania.
[38]	**Niski stan akumulatora**	Wyjście jest wyzwalane po około 9 minutach od momentu wykrycia niskiego stanu akumulatora i po takim samym czasie powraca do stanu normalnego po wykryciu odpowiedniego stanu naładowania akumulatora.
[39]	**Żądanie losowej kontroli**	Wyjście to przechodzi na 2s do stanu załączenia w momencie wytypowania osoby do kontroli. Jeśli jednak we właściwościach kontrolera załączona jest opcja **Losowa kontrola użytkownika wymaga potwierdzenia** (patrz 4.7 Zakładka Zaawansowane) to wyjście z funkcją **[39]** pozostaje załączone do momentu potwierdzenia kontroli za pomocą linii wejściowej z funkcją **[46]: Losowa kontrola - potwierdzenie** lub za pomocą klawisza funkcyjnego z funkcją **[46]: Losowa kontrola – potwierdzenie.**
[64]	**ŚWIATŁO**	Wyjście powtarza stan Flagi ŚWIATŁO. Jeśli flaga jest załączona to wyjście jest załączone, jeśli flaga jest wyłączona to wyjście też jest wyłączone.
[65]	**TAMPER**	Wyjście powtarza stan Flagi TAMPER. Jeśli flaga jest załączona to wyjście jest załączone, jeśli flaga jest wyłączona to wyjście też jest wyłączone.
[66]	**AUX1**	Wyjście powtarza stan Flagi AUX1. Jeśli flaga jest załączona to wyjście jest załączone, jeśli flaga jest wyłączona to wyjście też jest wyłączone.
[67]	**AUX2**	Wyjście powtarza stan Flagi AUX2. Jeśli flaga jest załączona to wyjście jest załączone, jeśli flaga jest wyłączona to wyjście też jest wyłączone.
[68]	**WŁAMANIE**	Wyjście powtarza stan Flagi WŁAMANIE. Jeśli flaga jest załączona to wyjście jest załączone, jeśli flaga jest wyłączona to wyjście też jest wyłączone.
[74]	**Przełączanie obwodów antenowych term. ID1 i ID0**	Wyjście służy do naprzemiennego załączania i wyłączania cewek obwodów antenowych kontrolera oraz czytnika zewnętrznego. Podłączenie tego wyjścia do wejścia czytnika zewnętrznego poprawia odczyt kart gdy czytniki i kontroler są zamontowane zbyt blisko w ramach danego przejścia kontrolowanego dwustronnie. To wyjście jest dostępne jedynie dla kontrolerów z wbudowanym czytnikiem tj. PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302.
[84]	**Tryb Karta lub PIN dla terminala ID0**	Wyjście jest załączone gdy na terminalu ID0 obowiązuje tryb Karta lub PIN.
[85]	**Tryb Tylko Karta dla terminala ID0**	Wyjście jest załączone gdy na terminalu ID0 obowiązuje tryb Tylko Karta.
[86]	**Tryb Tylko PIN dla terminala ID0**	Wyjście jest załączone gdy na terminalu ID0 obowiązuje tryb Tylko PIN.
[87]	**Tryb Karta i PIN dla terminala ID0**	Wyjście jest załączone gdy na terminalu ID0 obowiązuje tryb Karta i PIN.

[88]	**Tryb Karta lub PIN dla terminala ID1**	Wyjście jest załączone gdy na terminalu ID1 obowiązuje tryb Karta lub PIN.
[89]	**Tryb Tylko Karta dla terminala ID1**	Wyjście jest załączone gdy na terminalu ID1 obowiązuje tryb Tylko Karta.
[90]	**Tryb Tylko PIN dla terminala ID1**	Wyjście jest załączone gdy na terminalu ID1 obowiązuje tryb Tylko PIN.
[91]	**Tryb Karta i PIN dla terminala ID1**	Wyjście jest załączone gdy na terminalu ID1 obowiązuje tryb Karta i PIN.
[92]	**Zmiana chwilowa trybu RCP**	Wyjście jest załączane na 8 sek. w momencie użycia wejścia lub klawisza funkcyjnego z funkcją tymczasowej zmiany trybu RCP tj. **[49]**, **[51]** lub **[57]**. Funkcja **[92]** może być użyta do blokowania dostępu w sytuacji gdy użytkownik nie wybierze żadnego trybu RCP. Wystarczy w ramach tego samego kontrolera wyjście z funkcją **[92]** podłączyć do wejścia z funkcją **[11]**. Wejście z funkcją **[11]** musi być skonfigurowane jako NC.
[93]	**DRZWI OTWARTE - prealert**	Wyjście jest załączane w połowie czasu powodującego załączenie Flagi DRZWI OTWARTE czyli w połowie czasu definiowanego za pomocą parametru **CZAS NA ZAMKNIĘCIE**. Wyjście jest wyłączane gdy drzwi zostaną domknięte lub upłynie czas załączenia Flagi DRZWI OTWARTE. Po podłączeniu urządzenia akustycznego wyjściez funkcją **[93]** może być użyte do ostrzegania użytkowników przed zbliżającym się alarmem DRZWI OTWARTE.
[97]	**Zamek drzwi (term. ID0)**	Wyjście jest wyzwalane na czas określony przez parametr **CZAS NA WEJŚCIE** (patrz 4.4 Zakładka Dostęp), gdy dostęp został przyznane z poziomu terminala ID0. Wyjście przeznaczone jest do sterowania przejściem dwustronnym z rozróżnieniem kierunku wejście – wyjście (np. bramka obrotowa).
[98]	**Zamek drzwi (term ID1)**	Wyjście jest wyzwalane na czas określony przez parametr **CZAS NA WEJŚCIE** (patrz 4.4 Zakładka Dostęp), gdy dostęp został przyznane z poziomu terminala ID1 lub z poziomu przycisku wyjścia. Wyjście przeznaczone jest do sterowania przejściem dwustronnym z rozróżnieniem kierunku wejście – wyjście (np. bramka obrotowa).
[99]	**Zamek drzwi**	Wyjście jest wyzwalane na czas określony przez parametr **CZAS NA WEJŚCIE** (patrz 4.4 Zakładka Dostęp) bez względu na to, z którego terminala został przyznany dostęp. Funkcja **[99]** jest domyślnym ustawieniem wyjścia przekaźnikowego REL1 w kontrolerze i służy do sterowania zamkiem drzwi.
[256]	**Alarm drzwi**	Wyjście sygnalizuje wystąpienie stanu Alarm Drzwi (patrz 3.9 Alarm Drzwi) Uwaga: Funkcja **[256]** jest funkcją zespoloną składającą się z trzech typów alarmów szczegółowych: DRZWI OTWARTE, PREALARM oraz WEJŚCIE SIŁOWE. Sygnalizacja każdego z alarmów jest realizowana przez inny rodzaj modulowania (impulsowania) linii wyjściowej. W przypadku jednoczesnego wystąpienia więcej niż jednego alarmu kontroler sygnalizuje alarm o najwyższym priorytecie.

3.15 Klawisze funkcyjne

Kontrolery serii PRxx2 dopuszczają zdefiniowanie do czterech klawiszy funkcyjnych dla każdej strony przejścia. Każdy klawisz funkcyjny można indywidualnie skonfigurować co do funkcji, harmonogramu, domyślnego trybu RCP oraz warunków dodatkowych we właściwościach kontrolera w programie PR Master (patrz 4.16 Zakładki Klawisz F1…F4). Program PR Master dopuszcza oprogramowanie wszystkich czterech klawiszy funkcyjnych dla każdego z czytników (Terminali ID0 i ID1) bez względu czy fizycznie istnieją one w danym kontrolerze/czytniku czy nie. W przypadku czytników zewnętrznych serii PRT, klawisze funkcyjne działają tylko wtedy, gdy czytniki komunikują się z kontrolerem w standardzie RACS CLK/DTA. W przypadku komunikacji Wiegand czy Magstripe klawisze funkcyjne nie są obsługiwane. Z punktu widzenia użytkownika, klawisze funkcyjne na klawiaturze działają jak przyciski dołączone do linii wejściowych kontrolera.

Tabela 9. Klawisze funkcyjne

Kod	Nazwa funkcji	Opis działania
[00]	**Brak funkcji**	Klawisz funkcyjny, do którego nie przypisano żadnych funkcji.
[02]	**Zwolnij drzwi**	Użycie klawisza zwalnia kontrolowane drzwi na identycznych zasadach jak w przypadku przyznania dostępu.
[04]	**Tylko rejestracja**	Każde użycie klawisza zostaje rejestrowane w historii zdarzeń, lecz kontroler nie podejmuje żadnych dodatkowych działań.
[09]	**WŁAMANIE**	Klawisz z funkcją **[09]** działa analogicznie jak linia wejściowa z funkcją **[09]** i powoduje załączenie Flagi (Tajmera) WŁAMANIE.
[44]	**Chwilowa emulacja terminala ID1**	W wyniku samego przypisania funkcji **[44]** do jednego z klawiszy funkcyjnych, przyznanie dostępu osobie uprawnionej za pomocą karty/kodu PIN skutkuje zdarzeniem **[547]: Przyznanie dostępu – tryb specjalny** zamiast zdarzeniem **[001]: Przyznanie dostępu**. Zdarzenie **[547]** jest ignorowane w Raporcie Obecności programu PR Master. W wyniku użycia tego klawisza tryb emulacji trwa do momentu najbliższego logowania, lecz nie dłużej niż 8 sekund a logowanie uprawnionego użytkownika skutkuje zdarzeniem **[001]: Przyznanie dostępu**. Uwaga: Funkcja **[44]** nie jest dostępna dla kontrolerów PR402 i PR102DR.
[45]	**Chwilowa emulacja terminala ID0 przez terminal ID1**	W wyniku użycia klawisza kontroler z wbudowanym czytnikiem Terminal ID1 przełącza się do trybu emulacji Terminala ID0. Tryb emulacji trwa do momentu najbliższego logowania, lecz nie dłużej niż 8 sekund a logowanie uprawnionego użytkownika skutkuje zdarzeniem **[001]: Przyznanie dostępu**. Uwaga: Funkcja **[45]** nie jest dostępna dla kontrolerów PR402 i PR102DR.
[46]	**Losowa kontrola - potwierdzenie**	Użycie klawisza powoduje skasowanie sygnalizacji żądania losowej kontroli użytkownika. Klawisz jest wykorzystywany tylko przez załączonej opcji: **Losowa kontrola użytkownika wymaga potwierdzenia** (patrz 4.7 Zakładka Zaawansowane).

[48]	**Wybierz tryb RCP z klawiatury - zmiana trwała**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[49]	**Wybierz tryb RCP z klawiatury - zmiana chwilowa**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[50]	**Następny tryb RCP - zmiana trwała**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master). Funkcja **[50]** jest dostępna jedynie w kontrolerze PR602LCD-DT i PR602LCD.
[51]	**Następny tryb RCP - zmiana chwilowa**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master). Funkcja **[51]** jest dostępna jedynie w kontrolerze PR602LCD-DT i PR602LCD.
[56]	**Ustaw predefiniowany tryb RCP – zmiana trwała**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[57]	**Ustaw predefiniowany tryb RCP – zmiana chwilowa**	Linia wejściowa związana z rejestracją czasu pracy (program RCP Master).
[58]	**Załącz zwłokę przed samouzbrojeniem**	Użycie klawisza przesuwa moment samouzbrojenia o czas określony przez parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem** (patrz 4.5 Zakładka Przezbrajanie).
[59]	**Kasuj zwłokę przed samouzbrojeniem**	Użycie klawisza kasuje parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem** – kontroler natychmiast podejmuje próbę samouzbrojenia zgodnie z Harmonogramem Przezbrajania (patrz 4.5 Zakładka Przezbrajanie).
[60]	**Zeruj Rejestr APB**	Użycie klawisza zeruje Rejestr APB. W efekcie wszyscy użytkownicy systemu mogą zalogować się na wejściu lub wyjściu Strefy APB ale w następnych krokach muszą przestrzegać zasad APB.
[61]	**Zmień stan uzbrojenia – klucz chwilowy**	Użycie klawisza powoduje przełączenie aktualnego stanu uzbrojenia kontrolera.
[62]	**Wyłącz wyjścia na module XM-8**	Użycie klawisza wyłącza wszystkie wyjścia na ekspanderach XM-8 dołączonych do kontrolera.
[63]	**Załącz wyjścia na module XM-8**	Użycie klawisza załącza wszystkie wyjścia na ekspanderach XM-8 dołączonych do kontrolera.
[64]	**Ustaw drzwi w tryb Normalny**	Użycie klawisza ustawia Tryb Drzwi Normalny.
[65]	**Ustaw drzwi w tryb Odblokowane**	Użycie klawisza ustawia Tryb Drzwi Odblokowane.
[66]	**Ustaw drzwi w tryb War. Odblokowane**	Użycie klawisza ustawia Tryb Drzwi Warunkowo Odblokowane.
[67]	**Ustaw drzwi w tryb Zablokowane**	Użycie klawisza ustawia Tryb Drzwi Zablokowane.
[68]	**Załącz ŚWIATŁO**	Użycie klawisza załącza Flagę (tajmer) ŚWIATŁO.

[69]	**Wyłącz ŚWIATŁO**	Użycie klawisza wyłącza Flagę (tajmer) ŚWIATŁO.
[70]	**Przełącz ŚWIATŁO**	Użycie klawisza przełącza Flagę ŚWIATŁO do stanu przeciwnego.
[71]	**Załącz AUX1**	Użycie klawisza załącza Flagę (tajmer) AUX1.
[72]	**Wyłącz AUX1**	Użycie klawisza wyłącza Flagę (tajmer) AUX1.
[73]	**Przełącz AUX1**	Użycie klawisza przełącza Flagę AUX1 do stanu przeciwnego.
[74]	**Załącz AUX2**	Użycie klawisza załącza Flagę (tajmer) AUX2.
[75]	**Wyłącz AUX2**	Użycie klawisza wyłącza Flagę (tajmer) AUX2.
[76]	**Przełącz AUX2**	Użycie klawisza przełącza Flagę AUX2 do stanu przeciwnego.
[77]	**Wyłącz WŁAMANIE i TAMPER**	Użycie klawisza wyłącza Flagi (tajmery) WŁAMANIE i TAMPER.
[78]	**Ustaw tryb Rozbrojony**	Użycie klawisza przełącza kontroler do trybu rozbrojenia.
[79]	**Ustaw tryb Uzbrojony**	Użycie klawisza przełącza kontroler do trybu uzbrojenia.
[84]	**Ustaw tryb Karta lub PIN dla term. ID0**	Użycie klawisza ustawia tryb Karta lub PIN dla terminala ID0.
[85]	**Ustaw tryb Tylko Karta dla term. ID0**	Użycie klawisza ustawia tryb Tylko Karta dla terminala ID0.
[86]	**Ustaw tryb Tylko PIN dla term. ID0**	Użycie klawisza ustawia tryb Tylko PIN dla terminala ID0.
[87]	**Ustaw tryb Karta i PIN dla term. IDO**	Użycie klawisza ustawia tryb Karta i PIN dla terminala ID0.
[88]	**Ustaw tryb Karta lub PIN dla term. ID1**	Użycie klawisza ustawia tryb Karta lub PIN dla terminala ID1.
[89]	**Ustaw tryb Tylko Karta dla term. ID1**	Użycie klawisza ustawia tryb Tylko Karta dla terminala ID1.
[90]	**Ustaw tryb Tylko PIN dla term. ID1**	Użycie klawisza ustawia tryb Tylko PIN dla terminala ID1.
[91]	**Ustaw tryb Karta i PIN dla term. ID1**	Użycie klawisza ustawia tryb Karta i PIN dla terminala ID1.
[255]	**Dzwonek**	Użycie klawisza załącza sygnał dźwiękowy dzwonka na wewnętrznym głośniku kontrolera (4 sek.) i opcjonalnie na linii wyjściowej z funkcją **[15]:Dzwonek** (4 sek.).

3.16 Harmonogramy i Warunki dodatkowe

Harmonogramy

Harmonogramy Czasowe lub w skrócie Harmonogramy to kalendarze obejmujące swoim zakresem 7 dni tygodnia (Pon. - Niedz.) plus 4 dni świąteczne (H1-H4). Każdy harmonogram może posiadać do 128 przedziałów czasowych Od… Do…. W systemie RACS 4 (program PR Master) rozróżnia się następujące typy harmonogramów czasowych:

- Harmonogramy Ogólnego Przeznaczenia, które mogą być stosowane do wielu różnych funkcji i opcji dostępnych w kontrolerze. Najczęściej znajdują swoje zastosowanie w odniesieniu do definiowania praw dostępu (patrz 3.7 Definiowanie Praw Dostępu),

- Harmonogramy Trybu RCP, które służą do automatycznej zmiany trybu RCP na terminalu ID1. Są one przeznaczone do zastosowania jedynie wtedy, gdy program PR Master współpracuje z programem RCP Master (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master),
- Harmonogramy Trybu Drzwi, które służą do automatycznej zmiany Trybu Drzwi (patrz 3.5 Tryby Drzwi)
- Harmonogramy Zerowania APB, które wskazują momenty czasu, w których kontroler samoczynnie zeruje Rejestr APB (patrz 3.11 Antypowrót (ang. Anti-passback))
- Harmonogramy Trybu Identyfikacji, które służą do automatycznej zmiany Trybu Identyfikacji (patrz 3.4 Tryby Identyfikacji).

W ramach każdego z wymienionych harmonogramów oprócz ustawienia przedziałów czasu dla dni tygodnia można również wprowadzić ustawienie świąteczne. Są to dni, w których przestają obowiązywać zwykłe ustawienia harmonogramów czasowych zdefiniowanych w ramach dni tygodnia a w miejsce nich kontroler stosuje pewne reguły zastępcze. W systemie RACS 4 można zdefiniować cztery różne harmonogramy zastępcze (H1, H2, H3 i H4) w ramach danego harmonogramu i przypisać je do konkretnych dni świątecznych w roku. Kontrolery PRxx2 umożliwiają zdefiniowanie 120 dni świątecznych.

Warunki dodatkowe

Wiele funkcji oraz opcji we właściwościach kontrolera (program PR Master) może być możliwe do stosowania jedynie w określonych przedziałach czasowych i dopiero, gdy spełnione są określone Warunki Dodatkowe. Zalicza się do nich:

- Tryb High Security,
- Opcje klawisza [#],
- Kod Obiektu,
- Wejście Komisyjne,
- Stosowanie identyfikatorów przypisanych do użytkowników typu SWITCHER,
- Losowa kontrola użytkowników,
- Dostęp Warunkowy,
- Komendy z klawiatury,
- Linie wejściowe,
- Linie wyjściowe,
- Klawisze funkcyjne,
- Wejścia i wyjścia na ekspanderze XM-2.

Warunek Dodatkowy wskazuje na dodatkową okoliczność lub stan, który musi wystąpić, aby dana funkcja/opcja do której warunek jest przypisany mogła być użytkowana (logika pozytywna np. warunek **[130]**) lub przeciwnie była zablokowana (logika negatywna np. warunek **[131]**).

Przykład:
Jeśli do klawisza F1 zostanie przypisany Warunek Dodatkowy ***[129]: Zezwól gdy kontroler uzbrojony*** *to klawisz ten będzie mógł być używany tylko wtedy gdy kontroler będzie w stanie uzbrojenia.*

Warunki Dodatkowe można również przypisywać do linii wejściowych/wyjściowych oraz klawiszy funkcyjnych. Spełnienie Warunku Dodatkowego skutkuje możliwością stosowania danej linii/klawisza (logika pozytywna) lub ich zablokowaniem (logika negatywna) w zależności od konkretnego Warunku Dodatkowego. Wystąpienie danego Warunku Dodatkowego może skutkować wyłączeniem i zablokowaniem aktualnie aktywowanej linii/klawisza.

Przykład:
Gdy linia wejściowa z funkcją ***[07]: Dzwonek*** *jest załączona i przypisany jest do niej Warunek Dodatkowy* ***[129]: Zezwól gdy kontroler uzbrojony*** *to w momencie rozbrojenie kontrolera działanie funkcji* ***[07]: Dzwonek*** *zostanie przerwane.*

Tabela 10 Warunki Dodatkowe	
Kod	Warunek
[128]	Zezwól gdy kontroler rozbrojony
[129]	Zezwól gdy kontroler uzbrojony
[130]	Zezwól gdy wejście IN1 jest wyzwolone
[131]	Blokuj gdy wejście IN1 jest wyzwolone
[132]	Zezwól gdy wejście IN2 jest wyzwolone
[133]	Blokuj gdy wejście IN2 jest wyzwolone
[134]	Zezwól gdy wejście IN3 jest wyzwolone
[135]	Blokuj gdy wejście IN3 jest wyzwolone
[136]	Zezwól gdy wejście IN4 jest wyzwolone
[137]	Blokuj gdy wejście IN4 jest wyzwolone
[138]	Zezwól gdy ostatnie logowanie na term.ID0
[139]	Blokuj gdy ostatnie logowanie na term.ID0
[140]	Zezwól gdy nikogo nie ma w pomieszczeniu
[141]	Blokuj gdy nikogo nie ma w pomieszczeniu
[142]	Zezwól gdy osiągnięto limit osób w pomieszczeniu
[143]	Blokuj gdy osiągnięto limit osób w pomieszczeniu
[144]	Zezwól gdy drzwi są w trybie Normalnym
[145]	Blokuj gdy drzwi są w trybie Normalnym
[146]	Zezwól gdy drzwi są w trybie Odblokowane
[147]	Blokuj gdy drzwi są w trybie Odblokowane
[148]	Zezwól gdy drzwi są w trybie War. Odblokowane
[149]	Blokuj gdy drzwi są w trybie War. Odblokowane
[150]	Zezwól gdy drzwi są w trybie Zablokowane
[151]	Blokuj gdy drzwi są w trybie Zablokowane
[152]	Zezwól gdy załączona flaga ŚWIATŁO
[153]	Blokuj gdy załączona flaga ŚWIATŁO
[154]	Zezwól gdy załączona flaga TAMPER
[155]	Blokuj gdy załączona flaga TAMPER
[156]	Zezwól gdy załączona flaga AUX1
[157]	Blokuj gdy załączona flaga AUX1
[158]	Zezwól gdy załączona flaga AUX2
[159]	Blokuj gdy załączona flaga AUX2
[160]	Zezwól gdy załączona flaga WŁAMANIE
[161]	Blokuj gdy załączona flaga WŁAMANIE
[162]	Zezwól gdy załączona flaga WEJŚCIE SIŁOWE

[163]	Blokuj gdy załączona flaga WEJŚCIE SIŁOWE
[164]	Zezwól gdy załączona flaga PREALARM
[165]	Blokuj gdy załączona flaga PREALARM
[166]	Zezwól gdy załączona flaga DRZWI OTWARTE
[167]	Blokuj gdy załączona flaga DRZWI OTWARTE
[255]	Brak

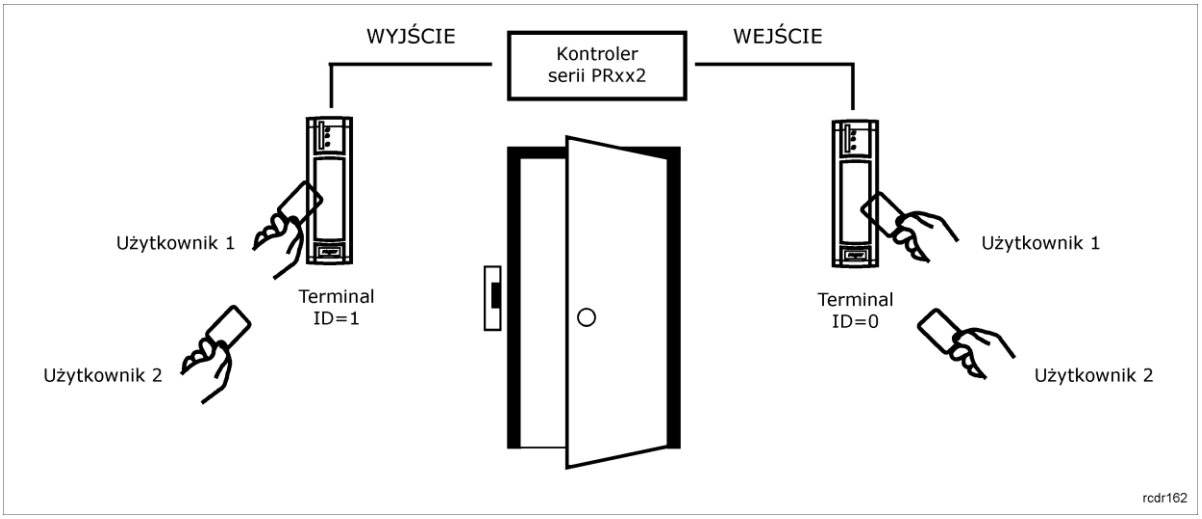
3.17 Opcje specjalne

3.17.1 Wejście Komisyjne

Jeśli ten tryb jest włączony to dostęp do pomieszczenia może być przyznany dopiero wtedy, gdy dwóch użytkowników w dowolnej kolejności, dokona poprawnej identyfikacji. Każdy z użytkowników musi dokonać identyfikacji wg tego Trybu Identyfikacji (patrz 3.4 Tryby Identyfikacji), który aktualnie obowiązuje na danym czytniku, przy czym każdy z użytkowników musi mieć w danej chwili prawo dostępu do pomieszczenia. Drugi użytkownik może zalogować się na dowolnym czytniku podłączonym do kontrolera (Terminal ID0 lub ID1) więc możliwa jest również taka sytuacja, że obaj użytkownicy są zlokalizowani po przeciwnych stronach przejścia. Załączenie trybu Wejścia Komisyjnego odnosi się do obydwu stron przejścia, nie można załączyć tego trybu indywidualnie dla każdej ze stron. Załączenie trybu Wejście Komisyjne odbywa się za pośrednictwem harmonogramu czasowego i może podlegać Warunkowi Dodatkowemu (patrz 3.16 Harmonogramy i Warunki dodatkowe).

Procedura konfiguracji Wejścia Komisyjnego

1. We właściwościach kontrolera przeznaczonego do nadzorowania wejście do pomieszczenia z Wejściem Komisyjnym (program PR Master) przejść do zakładki **Dostęp** i w obszarze **Wejście Komisyjne** wybrać Harmonogram Zawsze lub dowolny samemu ustawiony Harmonogram Ogólnego Przeznaczenia jeżeli wymagane jest by Wejście Komisyjne funkcjonowało w określonych przedziałach czasowych. Harmonogram Ogólnego Przeznaczenia można zdefiniować za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
2. Przesłać ustawienie do kontrolera.



Rys. 9 Wejście Komisyjne

3.17.2 Wejście Warunkowe

Gdy na kontrolerze obowiązuje tryb Wejście Warunkowe to prawo wejścia do pomieszczenia posiadają nie tylko osoby uprawnione ale również nieuprawnione pod warunkiem, że jest już ktoś w środku. Osoby (identyfikatory) w ogóle nie zdefiniowane w systemie RACS 4 nie mogą w żadnym wypadku uzyskać dostępu. Jeśli w pomieszczeniu nie przebywa żadna osoba (Rejestr APB wskazuje, że nikt nie jest zalogowany na czytniku wejściowym) to wejść do pomieszczenia może tylko użytkownik z odpowiednim uprawnieniem (wynikającym z jego praw dostępu). W trybie Wejście Warunkowe wyjście z pomieszczenia jest możliwe dla wszystkich użytkowników bez względu na ich uprawnienia i na ilość osób znajdujących się w wewnątrz.
Tryb Wejście Warunkowe jest oparty na Lokalnym APB (patrz 3.11 Antypowrót (ang. Anti-passback)). Załączenie trybu Wejście Warunkowe odbywa się za pośrednictwem harmonogramu czasowego i może podlegać Warunkowi Dodatkowemu (patrz 3.16 Harmonogramy i Warunki dodatkowe).

Uwaga: W momencie zresetowania Rejestru APB lista użytkowników zalogowanych w pomieszczeniu ulega wyzerowaniu, co powoduje, że wejście do pomieszczenia jest możliwe tylko dla osób z odpowiednimi prawami dostępu niemniej z chwilą wejścia pierwszej osoby inni użytkownicy automatycznie zyskują prawo dostępu aż do momentu, gdy pomieszczenie zostanie puste lub do momentu kolejnego zresetowania Rejestru APB.

Procedura konfiguracji Wejścia Warunkowego

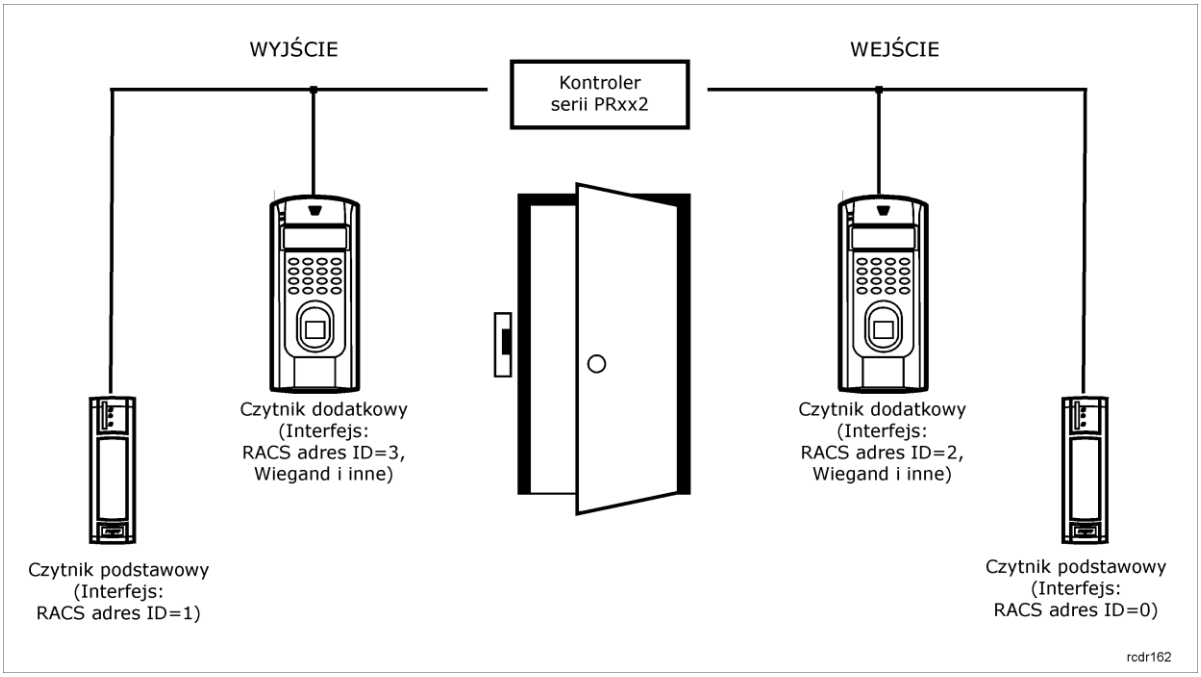
1. Zdefiniować Strefę Dostępu, do której część użytkowników ma dostęp a część nie (patrz 3.7 Definiowanie Praw Dostępu).
2. We właściwościach kontrolera przeznaczonego do nadzorowania wejście do strefy z Wejściem Warunkowym przejść do zakładki **Zaawansowane** i w obszarze **Wejście Warunkowe** wybrać Harmonogram Zawsze lub dowolny samemu ustawiony Harmonogram Ogólnego Przeznaczenia jeżeli wymagane jest by Wejście Warunkowe funkcjonowało w określonych przedziałach czasowych. Harmonogram Ogólnego Przeznaczenia można zdefiniować za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
3. W zakładce **APB** (patrz 4.8 Zakładka APB) we właściwości kontrolera zaznaczyć opcję **Załącz APB (Anti-passback).**
4. Zakładając, że Terminal ID0 jest czytnikiem wejściowym do strefy z Wejściem Warunkowym, przejść do zakładki **Terminal ID0** we właściwościach kontrolera i następnie zweryfikować czy w polu **Wejście/wyjście (Lokalny APB)** ustawiona jest opcja **Wejście do pomieszczenia**. Jeżeli to Terminal ID1 ma być czytnikiem wejściowym to wykonać analogiczne działania w zakładce **Terminal ID1** we właściwościach kontrolera.
5. Przesłać ustawienia do kontrolera.

3.17.3 Tryb High Security

Po załączeniu trybu High Security kontroler wymaga, aby użytkownik dokonał dwuetapowej identyfikacji. W pierwszym kroku użytkownik musi dokonać identyfikacji na czytniku podstawowym (ID1 lub ID0 w zależności od strony przejścia) a następnie w drugim kroku na czytniku dodatkowym zainstalowanym po tej samej stronie przejścia co czytnik podstawowy. Dopiero po wykonaniu tych obydwu kroków identyfikacji kontroler może przydzielić dostęp. Tryb High Security definiuje się dla każdej strony przejścia osobno. Działania trybu High Security może podlegać harmonogramowi czasowemu oraz Warunkowi Dodatkowemu (patrz 3.16 Harmonogramy i Warunki dodatkowe). Zwykle rolę czytnika dodatkowego pełni czytnik biometryczny (np. czytnik linii papilarnych) niemniej w ogólnym przypadku może być to dowolny typ czytnika. Wszystkie czytniki w Trybie High Security podłącza się do wspólnej magistrali RACS CLK/DTA (patrz 3.2.3 Interfejs RACS CLK/DTA). Wyjątek stanowią czytniki Wiegand (patrz 3.2.8 Dołączanie czytników Wiegand oraz Magstripe, które w przypadku kontrolera PR402DR podłącza się do jego linii wejściowych. W sytuacji korzystania z czytników komunikujących się po magistrali RACS CLK/DTA, adresy czytników (ID2 lub ID3) można ustawić w trakcie procedury Resetu Pamięci za pomocą programu RARC. Czytnik wbudowany w kontroler (PR602LCD-DT, PR602LCD,PR612, PR622, PR312EM, PR312MF i PR302) ma zawsze adres ID1. Zewnętrzny, fabrycznie nowy czytnik ma ustawiony adres domyślny ID=0.

Procedura konfiguracji trybu High Security:

1. We właściwościach kontrolera nadzorującego wejście do pomieszczenia z trybem High Security (program PR Master) przejść do zakładki **Terminal ID1** (patrz 4.2 Zakładka Terminal ID1) i w obszarze **Tryb High Security** wybrać sposób komunikacji z czytnikiem dodatkowym oraz Harmonogram Zawsze lub dowolny samemu ustawiony Harmonogram Ogólnego Przeznaczenia jeżeli wymagane jest by tryb High Security funkcjonował w określonych przedziałach czasowych. Harmonogram Ogólnego Przeznaczenia można zdefiniować za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.
2. Jeżeli wymagane jest zapewnienie trybu High Security po obu stronach drzwi to wykonać analogicznie czynności w zakładce **Terminal ID0** we właściwościach kontrolera (patrz 4.3 Zakładka Terminal ID0).
3. Przesłać ustawienie do kontrolera.



Rys. 10 Tryb High Security

3.18 Komendy z klawiatury

Kontrolery serii PRxx2 w odróżnieniu od serii PRxx1 nie mogą być całkowicie zaprogramowane pod względem wszystkich możliwych opcji i funkcji z poziomu klawiatury kontrolera czy też dołączonego do niego czytnika serii PRT z klawiaturą. Istnieje jednak zestaw komend (poleceń) obsługiwanych z poziomu klawiatury. Wszystkie komendy oraz związane z nimi ustawienia są podane we właściwościach danego kontrolera w programie PR Master (patrz 4.10 Zakładka Komendy z klawiatury).
Komenda może wymagać autoryzacji i wtedy po jej wprowadzeniu za pomocą klawiatury konieczne jest podanie uprawnionego identyfikatora. Do każdej komendy można przypisać harmonogram czasowy, który będzie dopuszczał lub blokował jej dostępność w zależności od dnia/godziny oraz Warunek Dodatkowy, który uzależni jej wykonanie od pewnych wybranych stanów kontrolera (patrz 3.16 Harmonogramy i Warunki dodatkowe).
Domyślnie kontroler akceptuje komendy wprowadzane zarówno z terminala ID1 jak i ID0 niemniej można wskazać, z których czytników (ID0 i/lub iD1) można wprowadzać komendy. Składnia każdej komendy jest podana w poniższej tabeli i jest również dostępna po wybraniu danej komendy w zakładce **Komendy z klawiatury** oraz wybraniu opcji **Właściwości** (program PR Master).
Zapis [Autoryzacja] występujący w definicji komend w tabelce zamieszczonej poniżej oznacza, że w miejscu tym należy dokonać logowania uprawnionego użytkownika (Karta i/lub kod PIN). Wymóg autoryzacji można dezaktywować indywidualnie dla każdej komendy.

Uwaga: W systemach z kontrolerami podłączonymi do wspólnej magistrali RS485 niewskazane jest modyfikowanie adresów kontrolerów za pomocą komend z klawiatury gdyż doprowadzi to do rozbieżności pomiędzy faktycznymi ustawieniami kontrolera a ustawieniami w programie PR Master.

Tabela 11 Komendy z klawiatury	
Komenda	Opis
F00: Ustaw adres (numer ID)	[*][0][0][#][Autoryzacja][nowy adres ID][#] Komenda nadaje nowy numer ID (adres) kontrolerowi, ID=00-99
F01: Ustaw datę	[*][0][1][#][Autoryzacja][DD][MM][RR][W][#] Polecenie ustawia nową datę, włącznie z rokiem i dniem tygodnia. DD: Dzień (01-31) MM: Miesiąc (00-12) RR: Rok (00-99) W: Dzień tygodnia (0-6) gdzie 0 – niedziela, 1- poniedziałek itd.
F02: Ustaw czas	[*][0][2][#][Autoryzacja][GG][MM][#] Polecenie ustawia nową godzinę GG: godzina (00-23) MM: Minuta (00-59)
F07: Ustaw drzwi w tryb Normalny	[*][0][7][#][Autoryzacja] Komenda załącza tryb drzwi Normalny
F08: Ustaw drzwi w tryb Zablokowane	[*][0][8][#][Autoryzacja] Komenda załącza tryb drzwi Zablokowane
F09: Ustaw drzwi w tryb Odblokowane	[*][0][9][#][Autoryzacja] Komenda załącza tryb drzwi Odblokowane
F10: Ustaw drzwi w tryb War. Odblokowane	[*][1][0][#][Autoryzacja] Komenda załącza tryb drzwi Warunkowo Odblokowane
F11: Ustaw kontroler w tryb Rozbrojony	[*][1][1][#][Autoryzacja] Komenda przełącza kontroler do trybu Rozbrojony
F12: Ustaw kontroler w tryb Uzbrojony	[*][1][2][#][Autoryzacja] Komenda przełącza kontroler do trybu Uzbrojony
F13: Zmień stan uzbrojenia (przezbrój kontroler)	[*][1][3][#][Autoryzacja] Komenda zmienia aktualny stan uzbrojenia
F14: Restartuj kontroler	[*][1][4][#][Autoryzacja] Komenda powoduje restart kontrolera
F15: Zeruj Rejestr APB	[*][1][5][#][Autoryzacja] Komenda powoduje inicjalizację (wyzerowanie) Rejestru APB na kontrolerze

F16: Wybierz tryb RCP z klawiatury - zmiana trwała	[*][1][6][#][Autoryzacja][NNN][#] Komenda przełącza terminal ID1 do trybu RCP wskazanego przez wartość NNN=000-255, zmiana trybu RCP ma charakter trwały i odnosi się do terminala ID1
F17: Wybierz tryb RCP z klawiatury - zmiana chwilowa	[*][1][7][#][Autoryzacja][NNN][#][Logowanie] Komenda przełącza terminal ID1 do trybu RCP wskazanego przez wartość NNN=000-255, zmiana trybu RCP ma charakter chwilowy (8 sek.) i odnosi się do terminala ID1
F18: Załącz zwłokę przed samouzbrojeniem (predefiniowaną)	[*][1][8][#][Autoryzacja] Komenda przesuwa moment samouzbrojenia o czas określony przez parametr: **Dodatkowa zwłoka czasowa przed samouzbrojeniem** (patrz 4.5 Zakładka Przezbrajanie)
F19: Załącz zwłokę przed samouzbrojeniem (definiowaną)	[*][1][9][#][Autoryzacja][NNN][#] Komenda przesuwa samouzbrojenie o czas NNN minut, poprzednie zwłoki czasowe zostają unieważnione
F20: Kasuj zwłokę przed samouzbrojeniem	[*][2][0][#][Autoryzacja] Komenda kasuje zwłokę czasową przed samouzbrojeniem (o ile jest ona w toku)
F21: Załącz flagę ŚWIATŁO	[*][2][1][#][Autoryzacja] Komenda załącza flagę ŚWIATŁO
F22: Wyłącz flagę ŚWIATŁO	[*][2][2][#][Autoryzacja] Komenda wyłącza flagę ŚWIATŁO
F23: Przełącz flagę ŚWIATŁO	[*][2][3][#][Autoryzacja] Komenda przełącza flagę ŚWIATŁO to stanu przeciwnego
F24: Załącz flagę AUX1	[*][2][4][#][Autoryzacja] Komenda załącza flagę AUX1
F25: Wyłącz flagę AUX1	[*][2][5][#][Autoryzacja] Komenda wyłącza flagę AUX1
F26: Przełącz flagę AUX1	[*][2][6][#][Autoryzacja] Komenda przełącza flagę AUX1 to stanu przeciwnego
F27: Załącz flagę AUX2	[*][2][7][#][Autoryzacja] Komenda załącza flagę AUX2
F28: Wyłącz flagę AUX2	[*][2][8][#][Autoryzacja] Komenda wyłącza flagę AUX2
F29: Przełącz flagę AUX2	[*][2][9][#][Autoryzacja] Komenda przełącza flagę AUX2 to stanu przeciwnego
F30: Załącz WŁAMANIE	[*][3][0][#][Autoryzacja] Komenda załącza flagę WŁAMANIE
F31: Wyłącz WŁAMANIE i TAMPER	[*][3][1][#][Autoryzacja] Komenda wyłącza flagi WŁAMANIE oraz TAMPER

F32: Ustaw tryb identyfikacji dla term.ID1	[*][3][2][#][Autoryzacja][N][#] Komenda przełącza terminal ID1 do trybu identyfikacji wskazanego przez cyfrę N=0..3 N=0: Tryb Karta i PIN N=1: Tryb Tylko Karta N=2: Tryb Tylko PIN N=3: Tryb Karta i PIN
F33: Ustaw tryb identyfikacji dla term.ID0	[*][3][3][#][Autoryzacja][N][#] Komenda przełącza terminal ID0 do trybu identyfikacji wskazanego przez cyfrę N=0..3, kodowanie N jak dla komendy F32

3.19 Rejestracja czasu pracy (RCP)

W systemie RACS 4 istnieją dwa rozwiązania dotyczące rejestracji czasu pracy. Oba wymagają stosowania programu PR Master do rejestrowania zdarzeń w systemie kontroli dostępu.

3.19.1 Rejestracja czasu pracy w oparciu o Obszary Obecności

To rozwiązanie oferuje bardzo uproszczoną metodę rejestracji polegającą na zliczaniu czasu przebywania użytkowników w danych obszarze kontrolowanym przez system RACS 4. Do jej zastosowania wymagane jest jedynie odpowiednie skonfigurowanie programu PR Master. Tryby RCP opisane w dalszej części instrukcji nie są w ogóle stosowane podczas rejestracji czasu pracy w oparciu o Obszary Obecności.

Procedura konfiguracji Obszarów Obecności

1. Skonfigurować system kontroli dostępu poprzez zdefiniowanie Stref Dostępu, Grup Użytkowników i Harmonogramów w oknie głównym programu PR Master (patrz 3.7 Definiowanie Praw Dostępu).
2. W oknie głównym programu PR Master wybrać opcję **Obszary Obecności.**
3. W otwartym oknie dodać nowy obszar nadając mu nazwę oraz dodać punkty wejściowe i wyjściowe do tego obszaru. Punktami wej/wyj są określone czytniki (terminale ID1 lub ID0) w systemie RACS 4. W praktyce punkty wejściowe i wyjściowe to zwykle wejścia i wyjścia do budynku czy też biur. W zależności od potrzeb można zdefiniować kilka punktów wejściowych i wyjściowych.
4. W przypadku Obszarów Obecności nie ma potrzeby ustawiać żadnych opcji we właściwościach kontrolerów. Obszary Obecności działają całkowicie niezależnie od Stref Dostępu, Stref APB czy też Stref Alarmowych.
5. Nie ma potrzeby przesyłania ustawień do kontrolerów. Działanie Obszarów Obecności polega na interpretowaniu zdarzeń rejestrowanych przez kontrolery po ich ściągnięciu do programu PR Master.
6. Podsumowanie rejestracji czasu pracy jest dostępne w oknie **Raport obecności w Obszarach**. Ten raport jest dostępny w menu górnym programu PR Master po wybraniu opcji **Raporty** a następnie opcji **Obecności**. Aktualne wyniki w Raporcie Obecności pojawią się dopiero po ściągnięciu zdarzeń z kontrolerów do programu PR Master. Można do tego użyć opcji **Odczytaj bufory zdarzeń** w oknie głównym programu PR Master.

Uwaga: Kwestia ustawień związanych z Raportem Obecności jest omówiona w instrukcji programu PR Master.

3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master

Program PR Master może rejestrować zdarzenia, które później zostaną wyeksportowane do innego, dedykowanego do tego celu programu po to by mógł on przeprowadzić szczegółowe rozliczenie czasu pracy zgodnie z obowiązującymi w danym kraju zasadami lub wymogami użytkownika. Takim

programem zewnętrznym jest m.in. oferowany przez firmę ROGER odpłatny program RCP Master. Inne programy współpracujące z PR Master to Gratyfikant, Agrobex, Symfonia, Sykom, Polman i Optima.

Uwaga: Program RCP Master 2 może ściągać zdarzenia z programu PR Master zgodnie z poniższym opisem albo funkcjonować jako oprogramowanie bezpośrednio komunikujące się z dedykowanymi kontrolerami PR602LCD-DT i PR602LCD.

Zalecanym kontrolerem do RCP jest PR602LCD, który posiada wbudowany czytnik, wyświetlacz LCD oraz klawisze funkcyjne ale w systemie RACS 4 każdy terminal (czytnik) może być punktem rejestracji zdarzeń dla systemu RCP. Kontroler PRxx2 może obsługiwać po dwa czytniki (terminale ID0 i ID1), za pomocą których może rejestrować zdarzenia **[001]: Przyznanie dostępu** z różnymi trybami RCP. W ogólnym ujęciu Tryb RCP dla czytnika ID0 jest ustawiony na stałe i nie może być zmieniany w trakcie pracy systemu. Natomiast Tryb RCP czytnika ID1 może być dynamicznie zmieniany na szereg podanych dalej sposobów.
System RACS 4 umożliwia zdefiniowanie do 255 Trybów RCP. Przeznaczeniem Trybu RCP jest rozróżnienie zdarzeń z punktu widzenia ich roli w systemie rejestracji czasu pracy. Każdy zdefiniowany w systemie tryb RCP posiada swój kod (numer 0..255) oraz może mieć przyporządkowaną nazwę (etykietę). Oprócz tego administrator do każdego trybu RCP może dopisać dodatkowo dwa dowolne parametry (informacje tekstowe) wybierając w menu górnym programu PR Master opcję **Narzędzia** a następnie **Tryby RCP**.
Tryby RCP w prawie całym zakresie mogą być swobodnie definiowane przez administratora systemu. W systemie RACS 4 istnieją następujące predefiniowane tryby RCP:

- WEJŚCIE (Kod 000),
- WYJŚCIE (Kod 016),
- WYJŚCIE SŁUŻBOWE (Kod 017),
- Przerwa śniadaniowa (Kod 018)
- Przerwa obiadowa (Kod 019),
- Nadgodziny1..5 (Kody 020..024),
- Zwolnienie się pracownika (Kod 025),
- Dyżur (Kod 026),
- BRAK (Kod 032),
- Wejście na Stanowisko 1..3 (Kody 033..035),
- Wyjście na papierosa (Kod 036)
- Przerwa (Kod 037)
- Przerwa na karmienie (Kod 038)
- Użytkownika1..5 (Kody 101..105
- Wyjście służbowe z zamknięciem (Kod 115)

Zdarzenia oznaczone trybem BRAK (Kod 032) są pomijane w rozliczeniach czasu pracy.
W celu przygotowania danych dla rozliczeń RCP należy z programu PR Master wyeksportować te zdarzenia, które posiadają jakikolwiek tryb RCP. W tym celu w oknie głównym programu PR Master wybrać opcję **Historia zdarzeń**, następnie po wybraniu parametrów filtrowania zdarzeń w oknie Historii zdarzeń wybrać opcję **Raport RCP** i następnie potwierdzić za pomocą opcji **OK**. W nowym oknie wybrać format pliku wyjściowego w zależności od tego, w jakim programie zewnętrznym będzie realizowane rozliczenie czasu pracy. W kolejnym kroku, wyeksportowany plik będzie musiał być zaimportowany przez zewnętrzny program RCP

Sterowanie trybem RCP

Domyślny Tryb RCP przypisuje się do danego czytnika (terminala) za pomocą programu PR Master. W tym celu należy przejść do właściwości danego kontrolera z podłączonymi czytnikami (kliknąć kontroler w oknie głównym programu PR Master) i przejść do zakładki **Terminal ID0** i/lub **Terminal ID1** (patrz 4.2 Zakładka Terminal ID1). W polu **Domyślny Tryb RCP** wybrać w jaki sposób dany czytnik (terminal) ma funkcjonować. Jeżeli zostanie wybrany tryb **Wejście** to dopóki nie zostanie to zmienione przez użytkownika/administratora to dany czytnik (terminal) będzie wszystkie zdarzenie typu **[001]: Przyznanie dostępu** rejestrować jako momenty rozpoczęcia

rejestracji czasu pracy dla danego użytkownika, którzy taki dostęp uzyskał. Zmiana aktualnie obowiązującego trybu RCP może być dokonywana interaktywnie przez użytkownika lub automatycznie z poziomu harmonogramu czasowego (Harmonogram Trybu RCP). Zmiana trybu RCP może mieć charakter trwały lub chwilowy. Trwała zmiana trybu RCP trwa do momentu wydania kolejnej komendy, która zmieni obowiązujący w danej chwili tryb RCP lub zmiany trybu przez harmonogram czasowy. Chwilowa zmiana trybu RCP obowiązuje tylko do momentu kolejnego logowania użytkownika a jeśli ono nie wystąpi w przeciągu 8 sekund kontroler samoczynnie przywraca poprzedni tryb RCP. Wyróżnia się następujące metody zmiany Trybu RCP danego czytnika (terminala):

- Z linii wejściowej – patrz 3.13 Linie wejściowe kontrolera,
- Z klawisza funkcyjnego (na klawiaturze) – patrz 3.15 Klawisze funkcyjne,
- Z harmonogramu czasowego – opcja **Harmonogramy** w oknie głównym programu PR Master oraz zakładka **Opcje**,
- Za pomocą komendy z klawiatury kontrolera lub klawiatury dołączonego do niego czytnika PRT – patrz 3.18 Komendy z klawiatury.

Możliwe jest zamienne stosowanie podanych powyżej metod. Zmiana Trybu RCP dotyczy Terminala ID1. Terminal ID1 to czytnik wbudowany w kontroler (Pr602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302) lub czytnik zewnętrzny podłączony do kontrolera (PR102DR, PR402). Terminal ID0, który jest zawsze czytnikiem zewnętrznym podłączonym do kontrolera może mieć jedynie ustawiony na stałe domyślny Tryb RCP.

Uwaga: W przypadku załączenia opcji **Term.ID0 przyjmuje ten sam tryb RCP co term.ID1** we właściwościach kontrolera (program PR Master) możliwe jest również dynamiczne i pośrednie sterowanie trybem RCP dla terminala ID0.

Tabela 12 Metody zmiany trybu RCP

Metoda	Funkcja	Działanie
Sterowanie z linii wejściowych	**[48]: Wybierz tryb RCP z klawiatury – zmiana trwała**	W następstwie wyzwolenia tej linii czytnik czeka na wprowadzenie trzech cyfr [NNN] zakończonych znakiem [#], które określą kod nowego trybu RCP, po czym przechodzi do wskazanego trybu RCP. Zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1, (NNN=000-255).
	[49]: Wybierz tryb RCP z klawiatury – zmiana chwilowa	W następstwie wyzwolenia tej linii czytnik czeka na wprowadzenie trzech cyfr [NNN] zakończonych znakiem [#] które określą kod nowego trybu RCP po czym przechodzi do wskazanego Trybu RCP. Zmiana trybu ma charakter chwilowy (8 sek.) i odnosi się do zdarzeń pochodzących z terminala ID1, (NNN=000-255).
	[50]: Następny tryb RCP – zmiana trwała	W następstwie wyzwolenia tej linii czytnik przechodzi do kolejnego Trybu RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1. Metoda ta jest dostępna jedynie na kontrolerze PR602LCD-DT i PR602LCD.
	[51]: Następny tryb RCP – zmiana chwilowa	W następstwie wyzwolenia tej linii czytnik przechodzi do kolejnego z Trybów RCP spośród trybów zdefiniowanych w systemie. Zmiana trybu ma charakter chwilowy (8 sek.) i odnosi się do zdarzeń pochodzących z terminala ID1. Metoda ta jest dostępna jedynie na kontrolerze PR602LCD-DT i PR602LCD.

	[56]: Ustaw predefiniowany tryb RCP – zmiana trwała	W następstwie wyzwolenia tej linii czytnik przechodzi do trybu, RCP który został zdefiniowany indywidualnie dla tej linii wejściowej. Tryb predefiniowany jest ustawiany we właściwościach kontrolera (program PR Master) w zakładce danej linii wejściowej. Zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1.
	[57]: Ustaw predefiniowany tryb RCP – zmiana chwilowa	W następstwie wyzwolenia tej linii czytnik przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej. Tryb predefiniowany jest ustawiany we właściwościach kontrolera (program PR Master) w zakładce danej linii wejściowej. Zmiana trybu ma charakter chwilowy (8 sek.) i odnosi się do zdarzeń pochodzących z terminala ID1.
Sterowanie za pomocą klawiszy funkcyjnych	**[48]: Wybierz tryb RCP z klawiatury – zmiana trwała**	Analogicznie jak funkcja **[48]** linii wejściowej.
	[49]: Wybierz tryb RCP z klawiatury – zmiana chwilowa	Analogicznie jak funkcja **[49]** linii wejściowej.
	[50]: Następny tryb RCP – zmiana trwała	Analogicznie jak funkcja **[50]** linii wejściowej. Funkcja ta jest dostępna tylko na kontrolerze PR602LCD-DT i PR602LCD.
	[51]: Następny tryb RCP – zmiana chwilowa	Analogicznie jak funkcja **[51]** dla linii wejściowej. Funkcja ta jest dostępna tylko na kontrolerze PR602LCD-DT i PR602LCD.
	[56]: Ustaw predefiniowany tryb RCP – zmiana trwała	Analogicznie jak funkcja **[56]** linii wejściowej.
	[57]: Ustaw predefiniowany tryb RCP – zmiana chwilowa	Analogicznie jak funkcja **[57]** linii wejściowej.
Komendy z klawiatury	**F16: Wybierz tryb RCP z klawiatury – zmiana trwała**	Analogicznie jak funkcja **[48]** linii wejściowej.
	F17: Wybierz tryb RCP z klawiatury – zmiana chwilowa	Analogicznie jak funkcja **[49]** linii wejściowej.
Inne metody	Harmonogram Trybu RCP	Harmonogram Trybu RCP umożliwia ustawienie automatycznej zmiany Trybu RCP dla Terminala ID1 podłączonego do kontrolera. Harmonogram ten definiuje przedziały czasu Od…Do, w których będzie obowiązywał dany Tryb RCP. Procedura definiowania tego harmonogramu jest podana poniżej.

Procedura ustawiania Harmonogramu Trybu RCP

1. W oknie głównym programu PR Master wybrać opcję **Harmonogramy** a następnie zakładkę **Harmonogramy Trybu RCP**.
2. W nowo otwartym oknie wybrać przycisk **Dodaj** i następnie nadać nazwę nowemu harmonogramowi i ustawić przedziały czasu dla poszczególnych dni tygodnia z określonymi Trybami RCP.

3. W oknie głównym programu PR Master kliknąć wybrany kontroler przechodząc do jego właściwości.
4. W zakładce **Opcje**, w polu **Sterowanie Trybem RCP** zaznaczyć opcję **Sterowanie Trybem RCP z harmonogramu** i w polu **Harmonogram** wybrać z listy rozwijanej zdefiniowany wcześniej harmonogram.
5. W razie potrzeby, w zakładkach **Terminal ID1** i/lub **Terminal ID0**, w polu **Domyślny Tryb RCP** ustawić jeden z wbudowanych Trybów RCP lub tryb zdefiniowany przez administratora. Administrator może definiować nowe Tryby RCP wybierając w menu głównym programu PR Master opcję **Narzędzia** a następnie **Tryby RCP**.
6. Oprócz ustawień związanych z Trybami RCP, konieczne jest również przypisanie poszczególnym użytkownikom numerów RCP. Można to zrobić przechodząc do opcji **Użytkownicy** w oknie głównym programu PR Master, następnie edytując bądź tworząc nowych użytkowników przejść do zakładki **Ogólne** i następnie do pola **Nr RCP**.

Uwaga: Więcej informacji na temat programu RCP Master podano w instrukcji tego oprogramowania.

3.20 Limity logowań

W przypadku kontrolerów serii PRxx2 możliwe jest określanie ile razy dany użytkownik będzie mógł mieć przyznany dostęp na danym przejściu aż do wyczerpania limitu. Możliwe jest definiowanie ręcznie odnawianego limitu logowań a w przypadku programu PR Master w wersji 4.5.6 lub nowszej oraz firmware PRxx2 w wersji x.18.6.x lub nowszej dodatkowo możliwe jest konfigurowanie automatycznie odnawianego limitu logowań. Pierwszy z limitów jest ustawiany na czas nieokreślony i wymaga ręcznego odnawiania przez administratora w przypadku jego wyczerpania natomiast drugi z nich może być automatycznie odnawiany przez kontroler w przedziałach czasu zdefiniowanych przez administratora systemu.

Procedura konfiguracji ręcznie odnawianego limitu logowań

1. Dodać użytkowników do systemu (więcej informacji w instrukcji programu PR Master).
2. Kliknąć prawym przyciskiem myszy kontroler w oknie głównym programu PR Master i następnie wybrać opcję **Limity logowań**.
3. W nowo otwartym oknie wybrać przycisk **Dodaj**.
4. W następnym oknie wybrać użytkownika z listy oraz ustawić dla niego limit logowań.
5. Zamknąć wszystkie okna i powrócić do okna głównego programu PR Master. Nowe ustawienia zostaną przesłane automatycznie.

albo

1. Podczas dodawania użytkowników za pomocą opcji **Użytkownicy** w oknie głównym programu PR Master we właściwościach danego użytkownika wybrać zakładkę **Limity logowań** a następnie wybrać przycisk **Odczyt limitów logowań**. Limity logowań można definiować zarówno dla nowych jak i istniejących użytkowników.
2. Wybrać kontroler z listy i nacisnąć przycisk **Zmień**.
3. Ustawić liczbę w polu **Limit logowań:**
4. Zamknąć okno i przesłać ustawienia za pomocą przycisku **Prześlij** (do wybranego kontrolera) albo **Aktualizuj** (do wszystkich kontrolerów).

Procedura konfiguracji automatycznie odnawianego limitu logowań

1. Kliknąć kontroler w oknie głównym programu PR Master i następnie przejść do zakładki **Opcje**.
2. W obszarze **Odnawialny limit logowań** (patrz 4.6 Zakładka Opcje) ustawić wartości dla takich parametrów jak **Okres odnawiania:** oraz **Rozpocznij odnawianie o:**
3. Dodać użytkowników do systemu (więcej informacji w instrukcji programu PR Master).
4. Kliknąć prawym przyciskiem myszy kontroler w oknie głównym programu PR Master i następnie wybrać opcję **Limity logowań**.
5. W nowo otwartym oknie wybrać przycisk **Dodaj**.
6. W następnym oknie wybrać użytkownika, ustawić dla niego limit logowań i zaznaczyć opcję **Odnawialny**.

7. Zamknąć wszystkie okna i powrócić do okna głównego programu PR Master. Nowe ustawienia zostaną przesłane automatycznie.

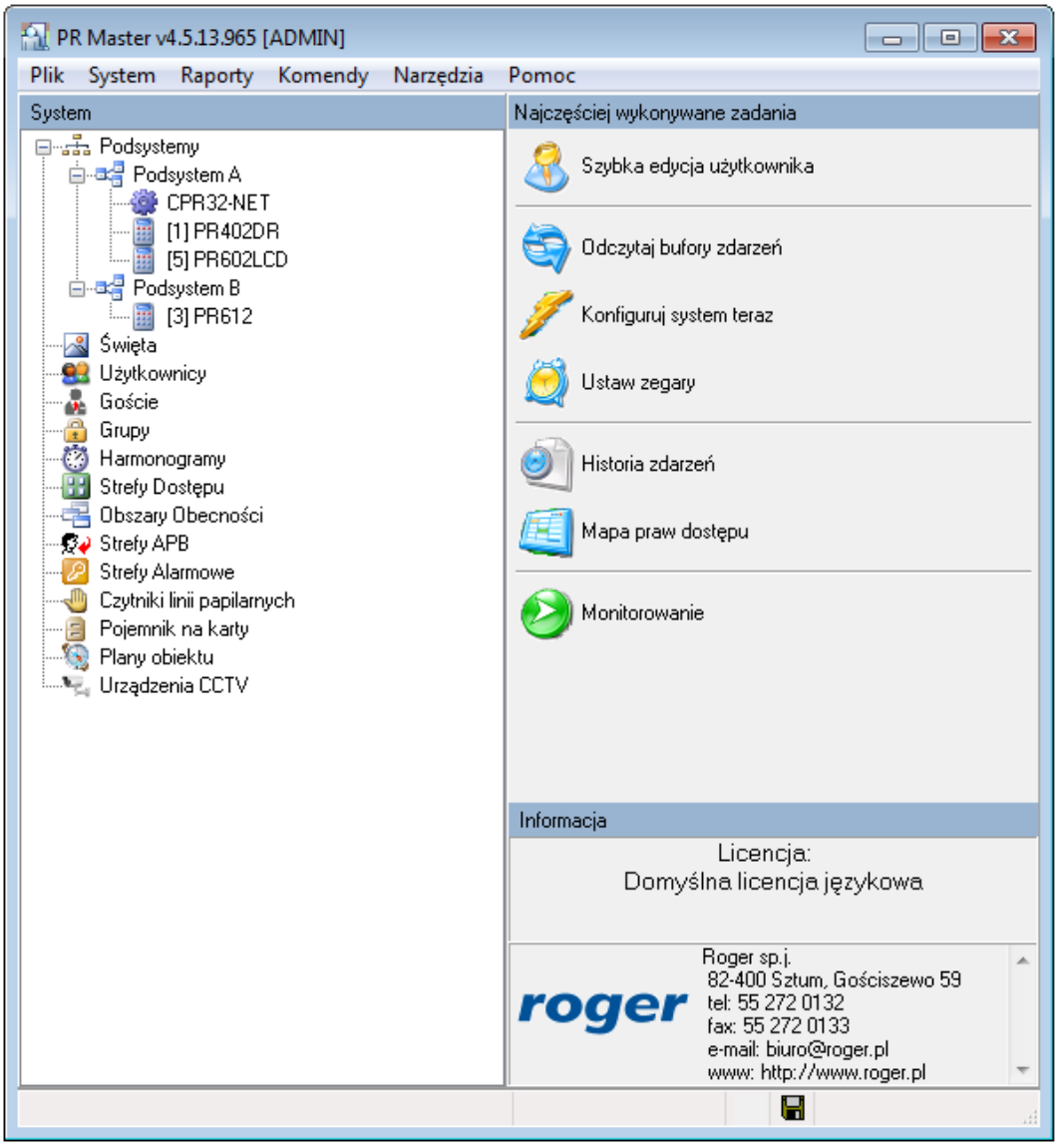
albo

1. Kliknąć kontroler w oknie głównym programu PR Master i następnie przejść do zakładki **Opcje**.
2. W obszarze **Odnawialny limit logowań** (patrz 4.6 Zakładka Opcje) ustawić wartości dla takich parametrów jak **Okres odnawiania:** oraz **Rozpocznij odnawianie o:**
3. Podczas dodawania użytkowników za pomocą opcji **Użytkownicy** w oknie głównym programu PR Master we właściwościach danego użytkownika wybrać zakładkę **Limity logowań** a następnie wybrać przycisk **Odczyt limitów logowań**. Limity logowań można definiować zarówno dla nowych jak i istniejących użytkowników.
4. Wybrać kontroler z listy i nacisnąć przycisk **Zmień**.
5. Ustawić liczbę w polu **Limit logowań:** i dodatkowo zaznaczyć opcję **Odnawialny**
6. Zamknąć okno i przesłać ustawienia za pomocą przycisku **Prześlij** (do wybranego kontrolera) albo **Aktualizuj** (do wszystkich kontrolerów).

IV. PROGRAMOWANIE

Kontrolery serii PRxx2 programuje się z poziomu aplikacji PR Master do konfiguracji i zarządzania systemem kontroli dostępu RACS 4. Program PR Master jest dostępny w pełnej wersji na stronie www.roger.pl. W niniejszym rozdziale opisane zostaną wszystkie opcje widoczne we właściwościach kontrolerów (dostępne po kliknięciu kontrolera za pomocą myszki w oknie głównym programu PR Master). Są one stosowane nie tylko do konfigurowania samych kontrolerów ale również mechanizmów kontroli dostępu. Pozostałe opcje i funkcje programu PR Master są opisane w instrukcji tego programu.
Kontrolery serii PRxx2 w odróżnieniu od serii PRxx1 nie mogą być całkowicie zaprogramowane pod względem wszystkich możliwych opcji i funkcji z poziomu klawiatury kontrolera czy też dołączonego do niego czytnika serii PRT z klawiaturą. Istnieje jednak pewien zestaw komend (poleceń) obsługiwanych z poziomu klawiatury – patrz 3.18 Komendy z klawiatury.

Uwaga: Ze wszystkimi opcjami dostępnymi w programie PR Master skojarzone są jednozdaniowe podpowiedzi. Aby wyświetlić daną podpowiedź należy ustawić wskaźnik myszy na danej opcji i odczekać 1 sekundę.

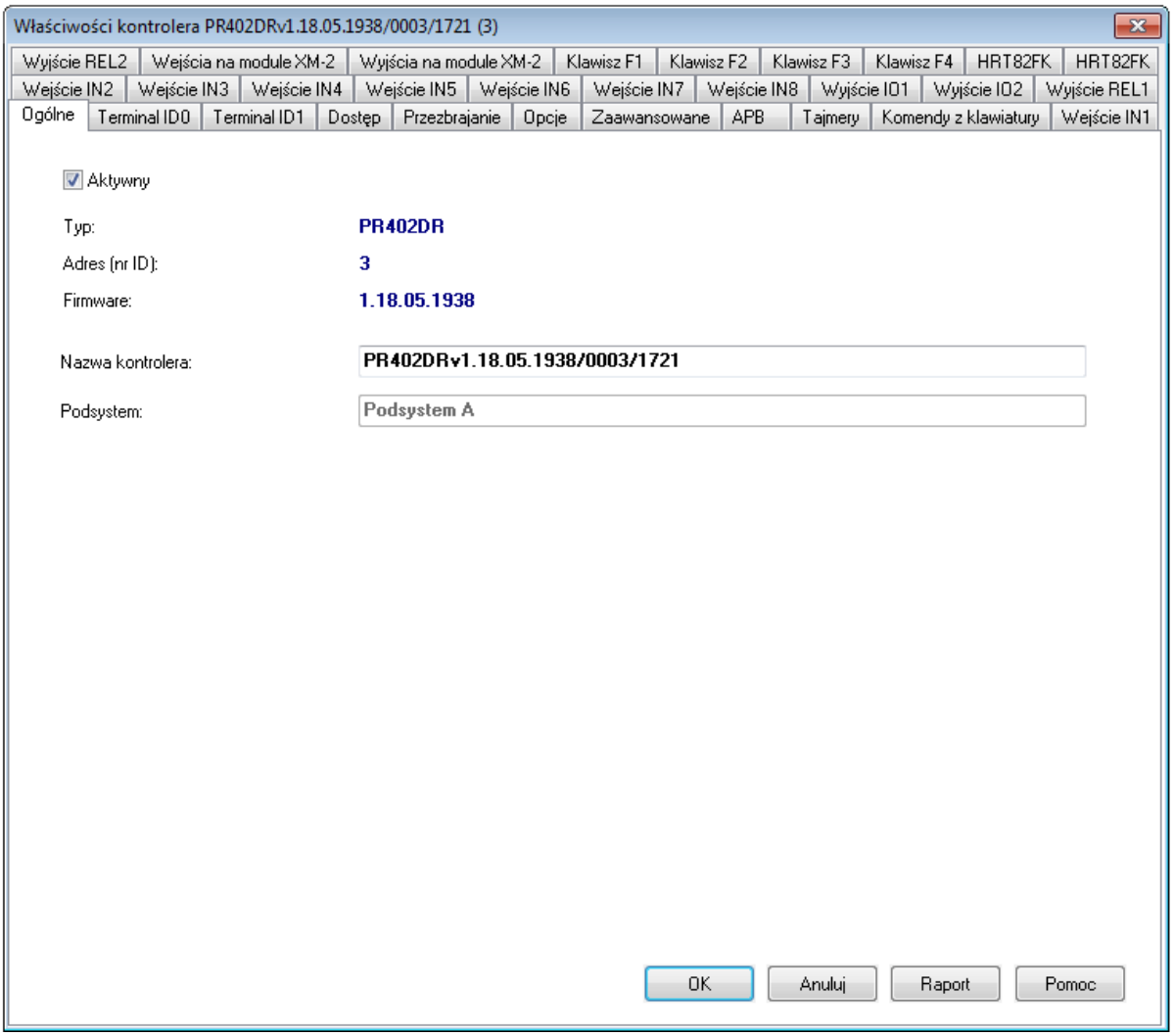


Rys. 11 Okno główne programu PR Master

4.1 Zakładka Ogólne

W zakładce **Ogólne** możliwe jest załączenie i wyłączenie danego kontrolera, zmiana wyświetlanej nazwy kontrolera oraz podane są następujące informacje ogólne:

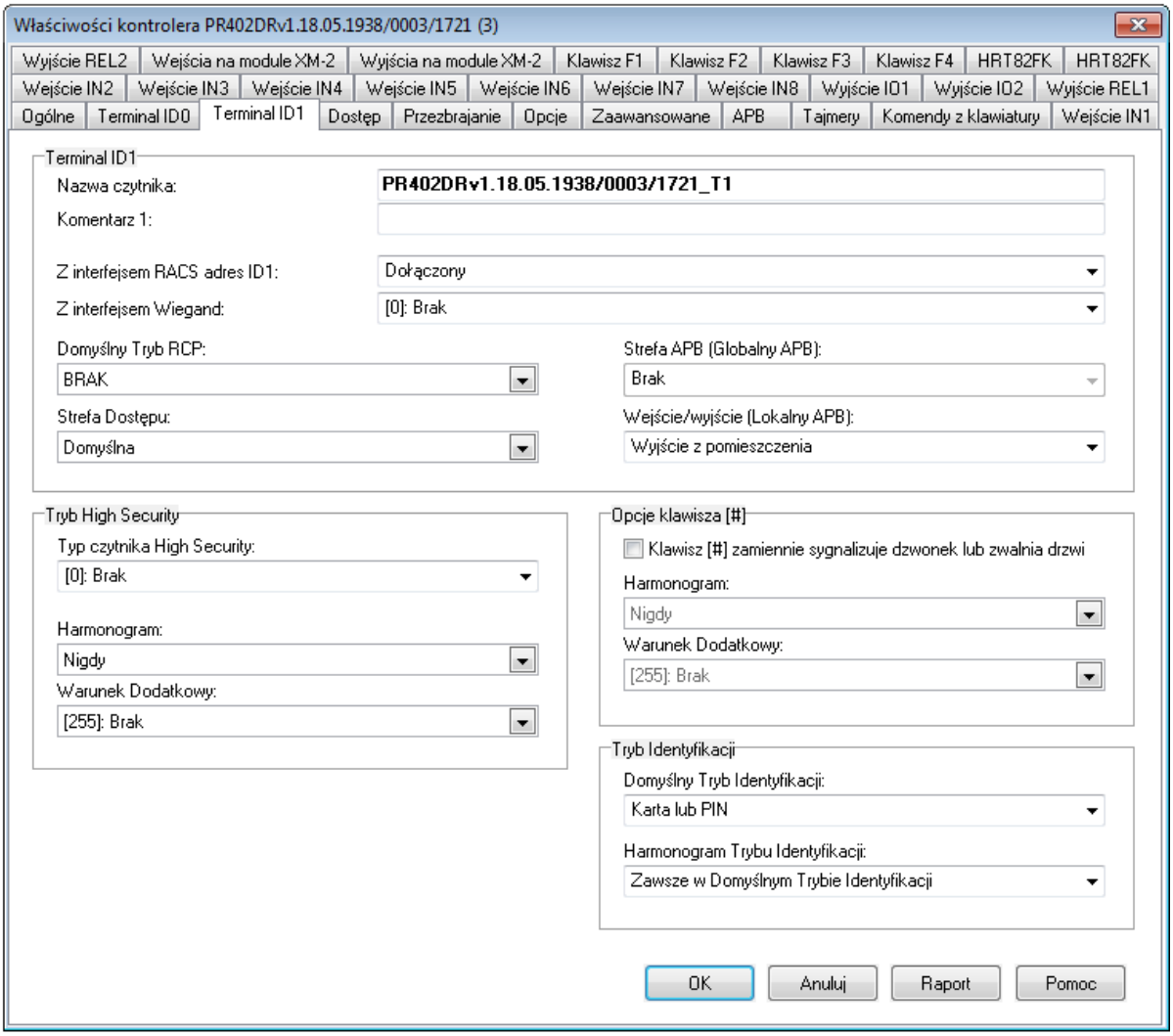
- Typ kontrolera,
- Adres (nr ID) kontrolera,
- Wersja oprogramowania wbudowanego (firmware),
- Nazwa kontrolera,
- Nazwa podsystemu, do którego należy kontroler.



Rys. 12 Zakładka Ogólne

4.2 Zakładka Terminal ID1

Terminal ID1 to czytnik wbudowany w kontroler (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302) albo czytnik zewnętrzny (PR102DR, PR402) (patrz 2.2 Budowa i przeznaczenie).



Rys. 13 Zakładka Terminal ID1

Obszar: Terminal ID1

W obszarze **Terminal ID1** możliwa jest zmiana nazwy czytnika, dodanie własnego komentarza oraz wybranie trybu pracy czytnika (patrz 3.2.3 Interfejs RACS CLK/DTA oraz 3.2.8 Dołączanie czytników Wiegand oraz Magstripe). Do poprawnej współpracy kontrolera czasami konieczne jest również skonfigurowanie samego czytnika do odpowiedniego trybu i adresu. Fabrycznie nowe czytniki serii PRT mają domyślnie ustawiony tryb RACS CLK/DTA i adres ID=0.

Opcja: Domyślny Tryb RCP – opcja umożliwia ustawienie jednego z wbudowanych lub zdefiniowanych przez administratora Trybów RCP dla czytnika. Opcja nie dotyczy rejestracji czasu pracy w oparciu o Obszary Obecności. Więcej informacji - patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master.

Opcja: Strefa Dostępu – opcja służy do wskazania danego czytnika jako wejścia do zdefiniowanej przez administratora Strefy Dostępu. Strefę Dostępu tworzy się za pomocą opcji **Strefy Dostępu** w oknie głównym programu PR Master. Więcej informacji – patrz 3.7 Definiowanie Praw Dostępu.

Opcja: Strefa APB (Globalny APB) – opcja służy do określenia danego czytnika jako wejścia do wybranej Strefy APB. Strefy APB definiuje się za pomocą opcji **Strefy APB** w oknie głównym programu PR Master. Opcja jest stosowana podczas definiowania APB Globalnego i jest

ona aktywna dopiero po załączeniu opcji **Załącz APB (Anti-passback)** w zakładce **APB** we właściwościach kontrolera. Więcej informacji – patrz 3.11 Antypowrót (ang. Anti-passback)

Opcja: Wejście/wyjście (Lokalny APB) - opcja służy do określenia danego czytnika jako wejścia lub wyjścia dla Lokalnego APB. Do funkcjonowania Lokalnego Anti-passbacku konieczne jest załączenie opcji **Załącz APB (Anti-passback)** w zakładce **APB** we właściwościach kontrolera. Więcej informacji – patrz 3.11 Antypowrót (ang. Anti-passback)

Obszar: Tryb High Security

W tym obszarze możliwe jest wybranie typu drugiego czytnika współpracującego z czytnikiem Terminal ID1 w Trybie High Security (patrz 3.17.3 Tryb High Security). Do Trybu High Security można przypisać harmonogram oraz Warunek Dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są dwa harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym Tryb High Security będzie obowiązywał. W przypadku wybrania harmonogramu Zawsze, Tryb High Security stosowany będzie przez cały czas.

Obszar: Opcje klawisza [#]

W tym obszarze można załączyć opcję **Klawisz [#] zamiennie sygnalizuje dzwonek lub zwalnia drzwi,** której działanie zależy od przypisanego harmonogramu i Warunku dodatkowego (patrz 3.16 Harmonogramy i Warunki dodatkowe). Po załączeniu opcji można wybrać wbudowany harmonogram Nigdy i wtedy klawisz [#] na klawiaturze kontrolera lub dołączonego czytnika z klawiaturą będzie przez cały czas działał tak jak klawisz funkcyjny z funkcją **[255]: Dzwonek** (patrz 3.15 Klawisze funkcyjne). Jeżeli dodatkowo zdefiniowana zostanie linia wyjściowa kontrolera z funkcją **[15]: Dzwonek** to będzie można do niej podłączyć zewnętrzne urządzenia akustyczne. Można również wybrać wbudowany harmonogram Zawsze i wtedy klawisz [#] będzie przez cały czas działał jak klawisz funkcyjny z funkcją **[02]: Zwolnij drzwi**. Można również przypisać własny harmonogram definiując Harmonogram Ogólnego Przeznaczenia za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. W przedziałach czasu Od…Do przycisk [#] będzie funkcjonował jako przycisk wyjścia a w pozostałym czasie jako dzwonek.

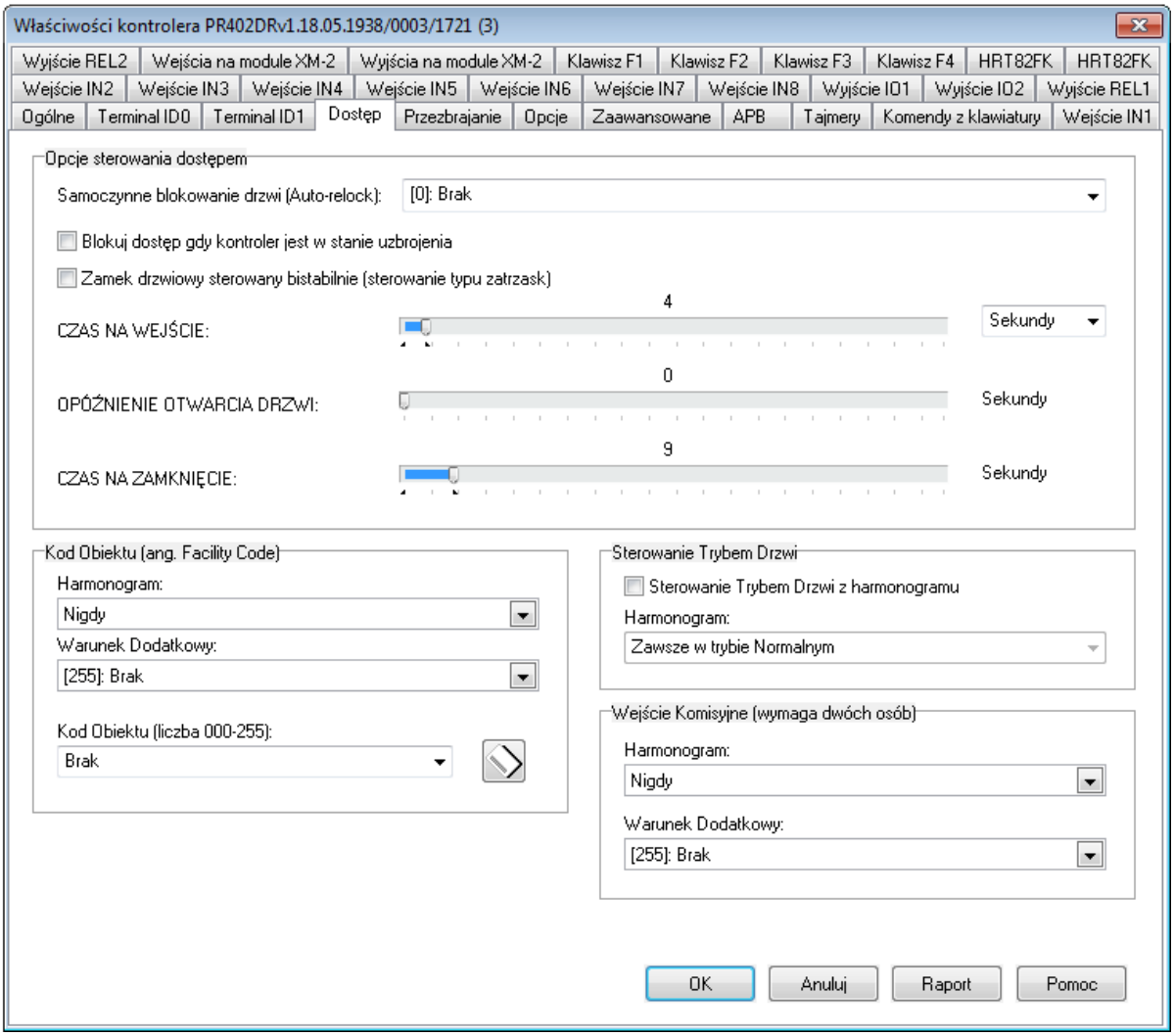
Obszar: Tryb Identyfikacji

W tym obszarze można wybrać domyślny Tryb Identyfikacji czytnika (patrz 3.4 Tryby Identyfikacji). Można również ustawić własny Harmonogram Trybu Identyfikacji, definiując go wcześniej za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.

4.3 Zakładka Terminal ID0

W zakładce **Terminal ID0** wszystkie opcje działają analogicznie jak w przypadku zakładki **Terminal ID1**. Terminal ID0 w każdej konfiguracji systemu RACS 4 jest czytnikiem zewnętrznym podłączonym do kontrolera serii PRxx2 (patrz 2.2 Budowa i przeznaczenie).

4.4 Zakładka Dostęp



Rys. 14 Zakładka Dostęp

Obszar: Opcje sterowanie dostępem

W tym obszarze definiowane są ustawienia związane ze sterowaniem zamkiem drzwi (patrz 3.7 Definiowanie Praw Dostępu).

Opcja: Samoczynne blokowanie drzwi (Auto-relock) - stosowanie tej opcji ma sens jedynie wtedy kontroler współpracuje z czujnikiem otwarcia drzwi. Jej załączenie powoduje, że kontroler może skrócić **CZAS NA WEJŚCIE**. Opcja może być wyłączona lub możliwe jest przypisanie dwóch poniższych wariantów:

- Blokuj zamek niezwłocznie po otwarciu drzwi
- Blokuj zamek niezwłocznie po zamknięciu drzwi

W pierwszym przypadku kontroler wyłącza wyjście przekaźnikowe kontrolera odpowiedzialne za sterowanie zamkiem drzwi w momencie, gdy rozpozna, że drzwi zostały już otwarte. Inaczej mówiąc zamek drzwi jest blokowany od razu po otwarciu drzwi a nie po upływie czasu ustawionego za pomocą parametru **CZAS NA WEJŚCIE**. W drugim przypadku kontroler wyłącza wyjście przekaźnikowe kontrolera odpowiedzialne za sterowanie zamkiem w momencie, gdy rozpozna, że drzwi zostały domknięte.

Opcja: Blokuj dostęp gdy kontroler jest w stanie uzbrojenia – gdy ta opcja jest załączona to kontroler może przyznać dostęp do pomieszczenia tylko wtedy gdy jest on w trybie rozbrojonym (patrz 3.6 Tryby Uzbrojenia). Jeśli kontroler jest w trybie uzbrojonym to dostęp jest permanentnie zablokowany dla wszystkich użytkowników również tych, którzy posiadają w danej chwili prawo dostępu do pomieszczenia. Dzięki opcji tej użytkownicy (typu SWITCHER) uprawnieni do przezbrajania kontrolera mogą czasowo blokować i odblokowywać dostęp dla pozostałych użytkowników systemu bez względu na ustawienia harmonogramów dostępu.

Opcja: Zamek drzwiowy sterowany bistabilnie - gdy ta opcja jest załączona to każde przyznanie dostępu przełącza wyjście sterujące elementem wykonawczym do stanu przeciwnego. Wyjście pozostaje w tym stanie do momentu, w którym kontroler ponownie przyzna komuś dostęp. Inaczej mówiąc, zamek drzwi jest albo przez cały czas otwarty albo zamknięty. Normalnie, gdy opcja nie jest załączona wyjście sterujące elementem wykonawczym jest aktywowane na pewien czas określony przez parametr **CZAS NA WEJŚCIE,** po upływie którego wyjście samoczynnie powraca do stanu wyłączenia.

Parametr: CZAS NA WEJŚCIE – w tym miejscu można ustawić czas otwarcia drzwi po przyznaniu dostępu. Zakres ustawień mieści się w przedziale od 1 sekundy do 99 minut.

Parametr: OPÓŹNIENIE OTWARCIA DRZWI – w tym miejscu można ustawić zwłokę w otwarciu drzwi po przyznaniu dostępu. Zakres ustawień mieści się w przedziale od 1 sekundy do 99 sekund.

Parametr: CZAS NA ZAMKNIĘCIE – w tym miejscu można ustawić wymagany czas domknięcia drzwi po ich otwarciu w wyniku przyznania dostępu. W przypadku zastosowania tej funkcjonalności konieczne jest podłączenie czujnika otwarcia drzwi do linii wejściowej z funkcją **[01]: Czujnik otwarcia drzwi** (patrz 3.13 Linie wejściowe kontrolera). Jeżeli po upływie **CZASU NA ZAMKNIĘCIE** drzwi są nadal otwarte to w systemie RACS 4 wzbudzany jest Alarm Drzwi o nazwie DRZWI OTWARTE (patrz 3.9 Alarm Drzwi oraz 3.10 Flagi Systemowe (Tajmery)). Zakres ustawień mieści się w przedziale od 1 sekundy do 99 sekund.

Obszar: Kod Obiektu (ang. Facility Code)

W tym obszarze można ustawić Kod Obiektu (patrz 3.8 Kod Obiektu (ang. Facility Code)) oraz przypisać do niego harmonogram i Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są harmonogramy wbudowane Zawsze i Nigdy. Można również przypisać własny harmonogram definiując Harmonogram Ogólnego Przeznaczenia za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do harmonogramu wskazuje przedział czasowy, w którym Kod Obiektu będzie stosowany. Za pomocą przycisku z ikoną karty można odczytać daną kartę zbliżeniową na podłączonym czytniku w celu ustalenia jej Kodu Obiektu (określonego fragmentu numeru karty).

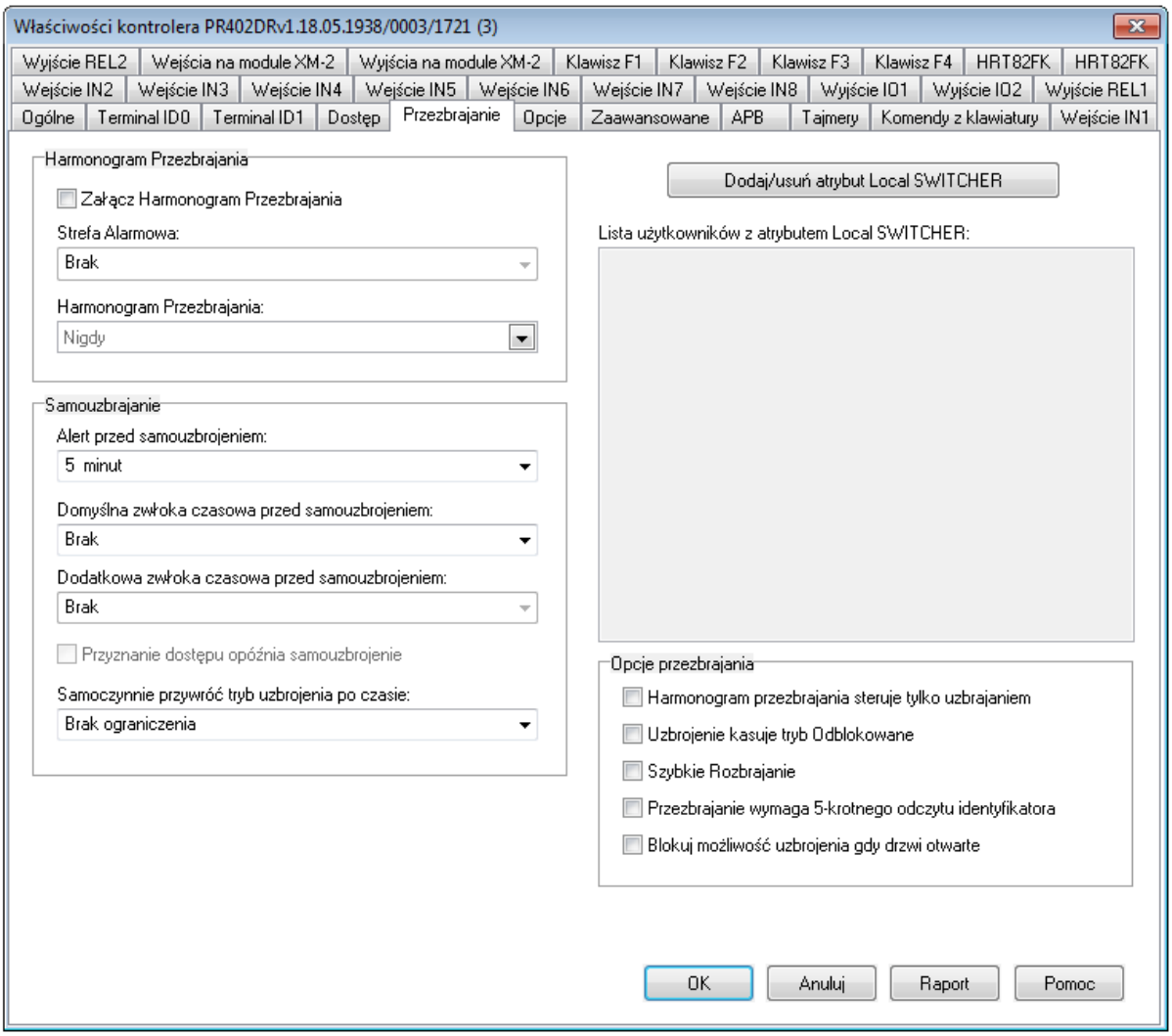
Obszar: Sterowanie Trybem Drzwi

W tym obszarze można załączyć opcję **Sterowanie Trybem Drzwi za pomocą harmonogramu** (patrz 3.5 Tryby Drzwi) oraz przypisać harmonogram domyślny Zawsze w Trybie Normalnym lub przypisać własny Harmonogram Trybu Drzwi definiując go wcześniej za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.

Obszar: Wejście Komisyjne (wymaga dwóch osób)

W tym obszarze można załączyć tryb Wejście Komisyjne (patrz 3.17.1 Wejście Komisyjne) poprzez wybranie harmonogramu wbudowanego Zawsze albo przypisanie własnego Harmonogramu Ogólnego Przeznaczenia, definiując go wcześniej za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Działanie trybu Wejście Komisyjne może być również uzależnione od Warunku Dodatkowego (patrz 3.16 Harmonogramy i Warunki dodatkowe).

4.5 Zakładka Przezbrajanie



Rys. 15 Zakładka Przezbrajanie

Obszar: Harmonogram Przezbrajania

Opcja: Załącz Harmonogram Przezbrajania – ta opcja załącza Harmonogram Przezbrajania (patrz 3.6 Tryby Uzbrojenia). Mechanizm przezbrajania można stosować w integracji systemu kontroli dostępu RACS 4 z centralami alarmowymi.

Opcja: Strefa Alarmowa – ta opcja umożliwia przypisanie kontrolera do Strefy Alarmowej w celu zdefiniowania granic tej strefy (patrz 3.12 Strefy Alarmowe). Strefy Alarmowe tworzy się za pomocą opcji **Strefy Alarmowe** w oknie głównym programu PR Master. Kontroler przypisany do danej Strefy Alarmowej może zmieniać swój stan uzbrojenia współbieżnie z innymi kontrolerami przypisanymi do tej strefy (patrz 3.6 Tryby Uzbrojenia) i zgodnie z harmonogramem ustawionym dla tej Strefy Alarmowej. Harmonogram przypisuje się do danej Strefy Alarmowej w oknie opcji **Strefy Alarmowe** dostępnej w oknie głównym programu PR Master. Dostępne są dwa harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.

Opcja: Harmonogram Przezbrajania – ta opcja umożliwia przypisanie Harmonogramu Przezbrajania (patrz 3.6 Tryby Uzbrojenia) bezpośrednio do kontrolera a nie za pośrednictwem Strefy Alarmowej. Dostępne są dwa harmonogramy wbudowane Zawsze i Nigdy. Można również

przypisać własny harmonogram definiując Harmonogram Ogólnego Przeznaczenia za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Harmonogram jest definiowany poprzez podanie parametru Od… który określa moment rozbrojenia kontrolera oraz parametru Do… który określa moment uzbrojenia kontrolera. Wybranie harmonogramu wbudowanego Zawsze oznacza, że kontroler będzie zawsze ustawiany w trybie rozbrojenia po resecie lub przesłaniu ustawień.

Obszar: Samouzbrajanie

Parametr: Alert przed Samouzbrojeniem – w tym miejscu można ustawić wyprzedzenie czasowe z jakim kontroler będzie sygnalizować fakt zbliżającego się uzbrojenia (patrz 3.6 Tryby Uzbrojenia)zgodnie z Harmonogramem Przezbrajania. Sygnalizacja może być akustyczna na wewnętrznym głośniku czytnika/kontrolera oraz na linii wyjściowej z funkcją **[33]: Alert przed samouzbrojeniem – wyjście niemodulowane** i/lub **[34]: Alert przed samouzbrojeniem – wyjście modulowane** (patrz 3.14 Linie wyjściowe kontrolera). Celem tej sygnalizacji jest ostrzeżenie osób pozostających w pomieszczeniach, że wkrótce nastąpi planowe uzbrojenie kontrolera. Dostępny zakres ustawień mieści się w przedziale od 1 do 99 minut.

Parametr: Domyślna zwłoka czasowa przed samouzbrojeniem – w tym miejscu można ustawić zwłokę w uzbrojeniu kontrolera wynikającą z Harmonogramu Przezbrajania (patrz 3.6 Tryby Uzbrojenia). Jest ona załączona, gdy w momencie planowanego uzbrojenia, linia wejściowa kontrolera z funkcją **[13]: Blokada uzbrojenia** jest wyzwolona (patrz 3.13 Linie wejściowe kontrolera). Zwłoka jest powtarzana aż do momentu gdy linia wejściowa z funkcją **[13]** przestanie być aktywna lub do momentu, gdy upłynie okres wymaganego uzbrojenia wynikający z Harmonogramu Przezbrajania. Celem tej zwłoki jest umożliwienie automatycznego opóźniania planowego uzbrojenia kontrolera przez urządzenie/system zewnętrzny. Dostępny zakres ustawień zwłoki mieści się w przedziale od 5 do 99 minut

Parametr: Dodatkowa zwłoka czasowa przed samouzbrojeniem – w tym miejscu, analogicznie jak dla powyższego parametru **Domyślnej zwłoki czasowej przed samouzbrojeniem** można ustawić zwłokę w uzbrojeniu kontrolera wynikającego z Harmonogramu Przezbrajania (patrz 3.6 Tryby Uzbrojenia). Różnica polega na metodzie załączenia zwłoki. Nie jest ona aktywowana załączeniem linii wejściowej z funkcją **[13]: Blokada uzbrojenia** ale za pomocą linii wejściowej z funkcją **[58]: Załącz zwłokę przed samouzbrojeniem**, klawisza funkcyjnego z funkcją **[58]: Załącz zwłokę przed samouzbrojeniem** albo za pomocą komendy z klawiatury **F18: Załącz zwłokę przed samouzbrojeniem (predefiniowaną)**. Zwłoka jest powtarzana i odliczana za każdym razem gdy aktywuje ją użytkownik jedną z podanych powyżej metod lub do momentu, gdy upłynie okres wymaganego uzbrojenia wynikający z Harmonogramu Przezbrajania. Celem tej zwłoki jest umożliwienie użytkownikowi ręcznego odwlekania planowego uzbrojenia kontrolera. Dostępny zakres ustawień zwłoki mieści się w przedziale od 5 do 99 minut.

Opcja: Przyznanie dostępu opóźnia moment uzbrojenia – w wyniku załączenia tej opcji wspomniana powyżej **Dodatkowa zwłoka czasowa przed samouzbrojeniem** może być dodatkowo załączana poprzez przyznanie dostępu (otwarcie zamka drzwi przez uprawnionego użytkownika za pomocą karty zbliżeniowej czy kodu PIN).

Parametr: Samoczynnie przywróć tryb uzbrojenia po czasie – w tym miejscu można ustawić zwłokę czasową, po której kontroler zostanie ponownie uzbrojony zgodnie z Harmonogramem Przezbrajania. Celem tej zwłoki jest automatyczne uzbrojenie kontrolera, gdy użytkownik ręcznie go rozbroił (patrz 3.6 Tryby Uzbrojenia) a harmonogram wskazuje, że w danym momencie kontroler powinien być uzbrojony. Samoczynne uzbrajanie może być odwlekane przez użytkownika zgodnie z parametrem **Dodatkowa zwłoka czasowa przed samouzbrojeniem**. Dostępny zakres ustawień zwłoki mieści się w przedziale od 5 do 99 minut.

Obszar: Local SWITCHER

W tym obszarze można nadać poszczególnym użytkownikom typu NORMAL z numerami ID od 1000 do 3999 możliwość przezbrajania kontrolera (patrz 3.6 Tryby Uzbrojenia). W odróżnieniu od

użytkowników typu MASTER, SWITCHER Full i SWITCHER Limited (patrz 3.3 Użytkownicy), użytkownik NORMAL z atrybutem Local SWITCHER może przezbrajać jedynie ten kontroler, na którym atrybut został mu przypisany.

Obszar: Opcje przezbrajania

Opcja: Harmonogram przezbrajania steruje tylko uzbrajaniem – gdy ta opcja jest załączona to Harmonogram Przezbrajania może automatycznie jedynie uzbrajać kontroler (patrz 3.6 Tryby Uzbrojenia) a rozbrajanie musi być dokonywane ręcznie lub zdalnie.

Opcja: Uzbrojenie kasuje tryb Odblokowane – gdy ta opcja jest załączona to w momencie uzbrojenia (patrz 3.6 Tryby Uzbrojenia) kontroler będzie kasował tryb drzwi Odblokowane i przywracał tryb Normalny (patrz 3.5 Tryby Drzwi). Opcja ta ma na celu zapobiegnięcie sytuacji, w której kontroler jest uzbrajany i jednocześnie kontroler utrzymuje zamek drzwi w stanie zwolnionym (drzwi niezablokowane).

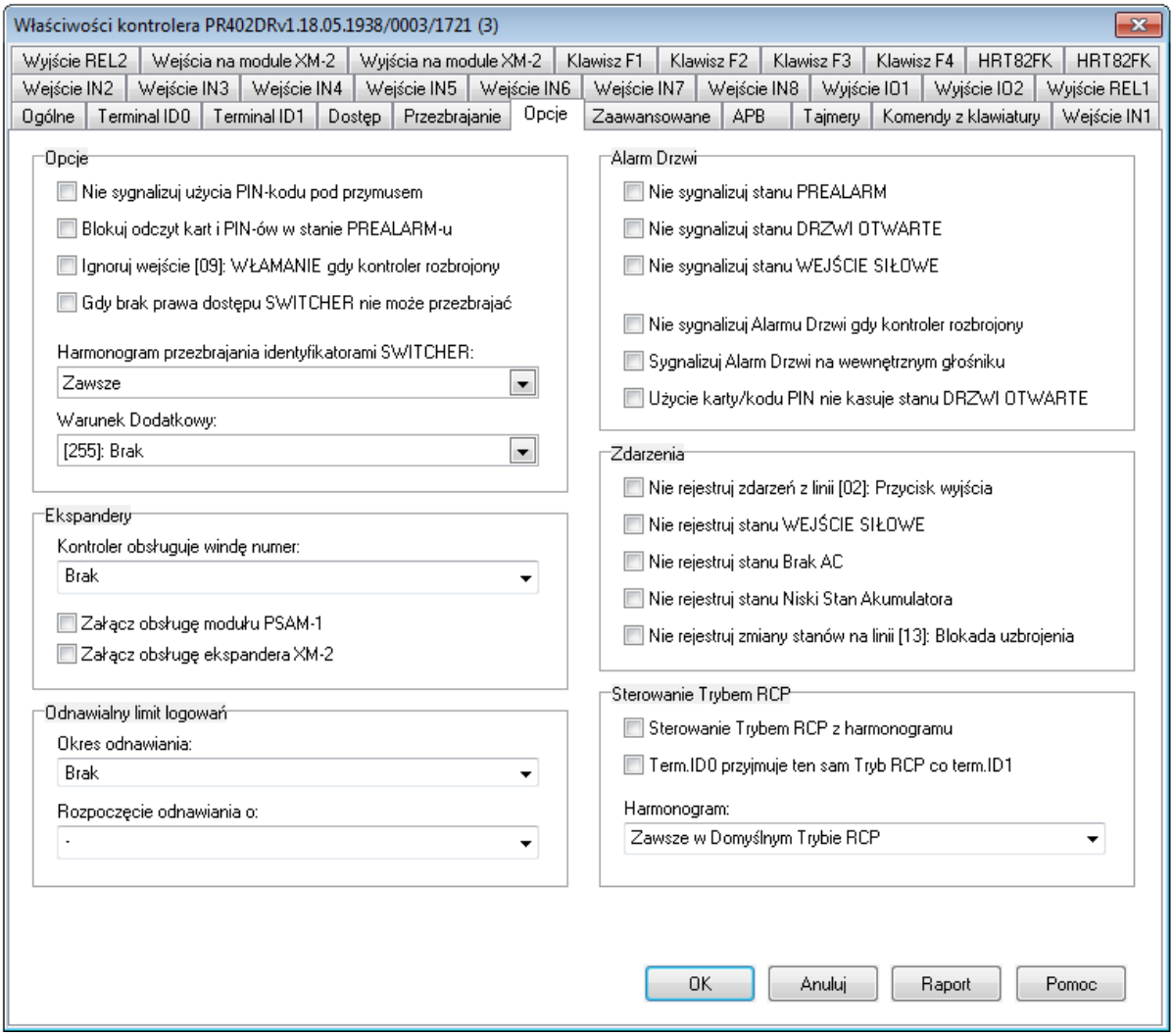
Opcja: Szybkie Rozbrajanie – gdy ta opcja jest załączona to użytkownicy typu MASTER, SWITCHER Full oraz użytkownicy NORMAL z załączonym atrybutem Local SWITCHER (patrz 3.3 Użytkownicy) mogą rozbroić kontroler (patrz 3.6 Tryby Uzbrojenia) po jednokrotnym użyciu identyfikatora (karty zbliżeniowej lub kodu PIN). Uzbrojenie nadal wymaga dwukrotnego użycia identyfikatora. Gdy ta opcja nie jest załączona to do ręcznego uzbrojenia oraz rozbrojenia kontrolera wymagane jest dwukrotne użycie tego samego identyfikatora. Użytkownik typu Switcher Limited przezbraja kontroler zawsze poprzez jednokrotne użycie identyfikatora bez względu na tą opcję.

Opcja: Przezbrajanie wymaga 5-krotnego odczytu identyfikatora – gdy opcja jest załączona to użytkownik typu SWITCHER Limited (patrz 3.3 Użytkownicy) musi pięciokrotnie użyć identyfikatora (kartę zbliżeniową lub kod PIN) by przezbroić kontroler (patrz 3.6 Tryby Uzbrojenia). Użytkownicy typu MASTER, SWITCHER Full oraz NORMAL z atrybutem Local SWITCHER muszą w rzeczywistości użyć identyfikatora sześciokrotnie gdyż pierwsze użycie jest związane z otwarciem drzwi. Identyfikator należy zbliżać w krótkich odstępach czasu w trakcie świecenia pomarańczowego wskaźnika LED SYSTEM na czytniku.

Uwaga: Jeśli na terminalu (czytniku) ustawiony jest Tryb Identyfikacji Karta i PIN (patrz 3.4 Tryby Identyfikacji) to przy załączonej ww. opcji należy najpierw wprowadzić raz kod PIN a następnie zbliżyć pięciokrotnie kartę do czytnika.

Opcja: Blokuj możliwość uzbrojenia gdy drzwi otwarte – gdy ta opcja jest załączona to uzbrajanie kontrolera jest zablokowane, w sytuacji gdy czujnik otwarcia drzwi wskazuje, że drzwi są otwarte. Czujnik otwarcia drzwi powinien być w takiej konfiguracji podłączony do linii wejściowej kontrolera z funkcją **[01]: Czujnik otwarcia drzwi.** Opcja może blokować uzbrajanie ręczne tj. za pomocą karty/kodu PIN, klawiszy funkcyjnych, komend z klawiatury ale nie blokuje uzbrajania przez harmonogram a w przypadku skonfigurowania ustawień związanych z samouzbrajaniem działa analogicznie jak funkcja **[13]: Blokada uzbrojenia** na opisany powyżej parametr **Domyślna zwłoka czasowa przed samouzbrojeniem** (tj. powoduje powtarzanie zwłoki samouzbrajania aż do skutku czyli zamknięcia drzwi lub do momentu, gdy upłynie okres wymaganego uzbrojenia wynikający z harmonogramu czasowego).

4.6 Zakładka Opcje



Rys. 16 Zakładka Opcje

Obszar: Opcje

Opcja: Nie sygnalizuj użycia kodu PIN pod przymusem – gdy ta opcja jest załączona to wprowadzenie kodu PIN różniącego się o +/-1 na ostatniej pozycji będzie traktowane jako wprowadzenie nieznanego kodu i będzie skutkować odmową dostępu. Gdy ta opcja nie jest zaznaczona to wprowadzenie kodu PIN różniącego się o +/-1 na ostatniej pozycji będzie skutkowało przyznaniem dostępu i wywołaniem stanu alarmowego WEJŚCIE SIŁOWE (patrz 3.9 Alarm Drzwi oraz 3.10 Flagi Systemowe (Tajmery)).

Przykład:
*Opcja **Nie sygnalizuj użycia kodu PIN pod przymusem** jest zaznaczona. Prawidłowy kod to [4569][#]. Wprowadzenie kodu [4568][#] bądź [4560][#] jest interpretowane jako wprowadzenie błędnego kodu. Gdy opcja **Nie sygnalizuj użycia kodu PIN pod przymusem** jest odznaczona to wprowadzenie kodu [4568][#] bądź [4560][#] będzie skutkować przyznaniem dostępu i wywołaniem stanu alarmowego WEJŚCIE SIŁOWE.*

Opcja: Blokuj odczyt kart i PIN-ów w stanie PREALARM – gdy ta opcja jest załączona to kontroler blokuje odczyt wszystkich kart oraz kodów PIN gdy aktywny jest PREALARM (patrz 3.9 Alarm Drzwi) na czas określony przez flagę PREALARM (patrz 3.10 Flagi Systemowe (Tajmery)). Stan

PREALARM występuje po pięciokrotnym użyciu nieznanego identyfikatora (karty zbliżeniowej lub kodu PIN).

Opcja: Ignoruj wejście [09]: WŁAMANIE gdy kontroler rozbrojony – gdy ta opcja jest zaznaczona to kontroler ignoruję załączenie linii wejściowej z funkcją **[09]: WŁAMANIE** (patrz 3.13 Linie wejściowe kontrolera) co oznacza, że flaga systemowa WŁAMANIE (patrz 3.10 Flagi Systemowe (Tajmery)) również nie jest załączana. Ignorowanie ww. linii wejściowej występuje tylko wtedy, gdy kontroler jest rozbrojony (patrz 3.6 Tryby Uzbrojenia).

Opcja: Gdy brak prawa dostępu SWITCHER nie może przezbrajać – gdy ta opcja jest załączona to zarówno użytkownik typu SWITCHER Full, SWITCHER Limited jak i użytkownik NORMAL z atrybutem Local SWITCHER (patrz 3.3 Użytkownicy) nie ma prawa przezbrajać danego kontrolera, jeżeli nie ma ustawionych praw dostępu w ramach tego kontrolera (przejścia). Ta opcja nie ma wpływu na użytkownika typu MASTER, która ma nieograniczone prawa dostępu.

Opcja: Harmonogram przezbrajania identyfikatorami SWITCHER – w tym miejscu można przypisać harmonogram dla użytkowników typu SWITCHER Full, SWITCHER Limited oraz użytkowników NORMAL z atrybutem Local SWITCHER (patrz 3.3 Użytkownicy) po to by określić przedziały czasowe, w których mogą oni przezbrajać kontrolera. Dostępne są harmonogramy wbudowane Zawsze i Nigdy. Można również przypisać własny harmonogram definiując Harmonogram Ogólnego Przeznaczenia za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master.

Opcja: Warunek Dodatkowy – w tym miejscu można przypisać Warunek Dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe) dla użytkowników typu SWITCHER Full, SWITCHER Limited oraz użytkowników NORMAL z atrybutem Local SWITCHER (patrz 3.3 Użytkownicy) po to by uaktywnić/zablokować ich prawa do przezbrajania.

Obszar: Ekspandery

Opcja: Kontroler obsługuje windę numer - w tym miejscu można wybrać numer windy nadzorowanej przez kontroler. Opcja jest wykorzystywana podczas konfiguracji kontroli dostępu w windach. Więcej informacji na temat takiej kontroli podano w punkcie 3.2.5 Współpraca z ekspanderem WE/WY XM-8 oraz w instrukcji ekspandera XM-8 dostępnej na stronie www.roger.pl

Opcja: Załącz obsługę modułu PSAM-1 – w tym miejscu można załączyć obsługę modułu dozoru zasilania PSAM-1. Więcej informacji na temat dozoru zasilania podano w punkcie 3.2.6 Współpraca z modułem PSAM-1 oraz w instrukcji modułu PSAM-1 dostępnej na stronie www.roger.pl

Opcja: Załącz obsługę ekspandera XM-2 – gdy ta opcja jest załączona to możliwa jest obsługa ekspandera XM-2, w tym możliwość przypisywania funkcji dla linii wejściowych i wyjściowych modułu w odpowiednich zakładkach (patrz 4.14 Zakładka Wejścia na module XM-2 oraz 4.15 Zakładka Wyjścia na module XM-2). Więcej informacji na temat ekspandera XM-2 podano w punkcie 3.2.4 Współpraca z ekspanderem WE/WY XM-2 oraz w instrukcji ekspandera XM-2 dostępnej na stronie www.roger.pl

Obszar: Automatyczne odnawianie limitu logowań

Parametr: Okres odświeżania: – w tym miejscu można ustawić okres odnawialnego limitu logowań – patrz 3.20 Limity logowań. Możliwe ustawienia to Brak, 1h, 2h, 3h, 4h, 6h, 12h oraz 24h.
Parametr: Rozpocznij odświeżanie o: – w tym miejscu można ustawić pełną godzinę od której będzie rozpoczynane odnawianie limitu logowań – patrz 3.20 Limity logowań.

Obszar: Alarm drzwi

Opcja: Nie sygnalizuj stanu PREALARM – gdy ta opcja jest załączona to kontroler nie sygnalizuje stanu PREALARM na linii wyjściowej z funkcją **[256]: Alarm drzwi** (patrz 3.9 Alarm Drzwi oraz 3.14 Linie wyjściowe kontrolera). Ta opcja nie blokuje innych metod sygnalizacji stanu PREALARM, w szczególności nie blokuje linii wyjściowej z funkcją **[29]: PREALARM** ani Flagi

Systemowej PREALARM (patrz 3.10 Flagi Systemowe (Tajmery)). Opcja nie blokuje również pozostałych Alarmów Drzwi na linii **[256]** tj. DRZWI OTWARTE i WEJŚCIE SIŁOWE. Zdarzenie związane ze stanem PREALARM jest zapisywane w historii zdarzeń oraz prezentowane w Trybie Monitorowania programu PR Master.

Opcja: Nie sygnalizuj stanu DRZWI OTWARTE – gdy ta opcja jest załączona to kontroler nie sygnalizuje stanu DRZWI OTWARTE na linii wyjściowej z funkcją **[256]: Alarm drzwi** (patrz 3.9 Alarm Drzwi oraz 3.14 Linie wyjściowe kontrolera). Ta opcja nie blokuje innych metod sygnalizacji stanu DRZWI OTWARTE, w szczególności nie blokuje linii wyjściowej z funkcją **[30]: DRZWI OTWARTE** ani Flagi Systemowej DRZWI OTWARTE (patrz 3.10 Flagi Systemowe (Tajmery)). Opcja nie blokuje również pozostałych Alarmów Drzwi na linii **[256]** tj. PREALARM i WEJŚCIE SIŁOWE. Zdarzenie związane ze stanem DRZWI OTWARTE jest zapisywane w historii zdarzeń oraz prezentowane w Trybie Monitorowania programu PR Master.

Opcja: Nie sygnalizuj stanu WEJŚCIE SIŁOWE - gdy ta opcja jest załączona to kontroler nie sygnalizuje stanu WEJŚCIE SIŁOWE na linii wyjściowej z funkcją **[256]: Alarm drzwi** (patrz 3.9 Alarm Drzwi oraz 3.14 Linie wyjściowe kontrolera). Ta opcja nie blokuje innych metod sygnalizacji stanu WEJŚCIE SIŁOWE, w szczególności nie blokuje linii wyjściowej z funkcją **[28]: WEJŚCIE SIŁOWE** ani Flagi Systemowej WEJŚCIE SIŁOWE (patrz 3.10 Flagi Systemowe (Tajmery)). Opcja nie blokuje również pozostałych Alarmów Drzwi na linii **[256]** tj. PREALARM i DRZWI OTWARTE. Zdarzenie związane ze stanem WEJŚCIE SIŁOWE jest zapisywane w historii zdarzeń oraz prezentowane w Trybie Monitorowania programu PR Master.

Opcja: Nie sygnalizuj Alarmu Drzwi gdy kontroler rozbrojony – gdy ta opcja jest załączona to żaden ze stanów Alarmu Drzwi nie jest załączany na linii wyjściowej **[256]: Alarm drzwi** (patrz 3.9 Alarm Drzwi oraz 3.14 Linie wyjściowe kontrolera) w sytuacji, gdy kontroler jest rozbrojony (patrz 3.6 Tryby Uzbrojenia). Alarmy Drzwi nie są również wtedy załączane na liniach wyjściowych z funkcjami **[29]: PREALARM, [30]: DRZWI OTWARTE, [28]: WEJŚCIE SIŁOWE** oraz na związanych z nimi Flagach (patrz 3.10 Flagi Systemowe (Tajmery)). Natomiast zdarzenia związane ze wszystkimi Alarmami Drzwi są zapisywane w historii zdarzeń i prezentowane w Trybie Monitorowania programu PR Master.

Opcja: Sygnalizuj Alarm Drzwi na wewnętrznym głośniku – gdy ta opcja jest załączona to poszczególne Alarmy Drzwi (patrz 3.9 Alarm Drzwi) mogą być dodatkowo sygnalizowane akustycznie na wewnętrznym głośniku kontrolera (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302) lub głośniku dołączonego czytnika ale tylko o adresie ID=1 (PR102DR, PR402).

Opcja: Użycie karty/kodu PIN nie kasuje stanu DRZWI OTWARTE – gdy ta opcja jest załączona to stan alarmowy DRZWI OTWARTE (patrz 3.9 Alarm Drzwi) oraz związana z nim Flaga Systemowa o tej samej nazwie (patrz 3.10 Flagi Systemowe (Tajmery)) nie mogą być skasowane poprzez użycie karty zbliżeniowej czy też kodu PIN użytkownika posiadającego prawa dostępu na danym przejściu.

Obszar: Zdarzenia

Opcja: Nie rejestruj zdarzeń z linii [02]: Przycisk wyjścia – gdy ta opcja jest załączona to zdarzenie **[001]: Przyznanie dostępu** nie jest zapisywane w historii zdarzeń i nie jest prezentowane w Trybie Monitorowania programu PR Master w przypadku użycia klawisza funkcyjnego z funkcją **[02]: Zwolnij drzwi**, linii wejściowej z funkcją **[02]: Przycisk wyjścia** oraz linii wejściowej z funkcją **[47]: Przycisk wejścia**. W pozostałych przypadkach udzielenia dostępu (karta zbliżeniowa, kod PIN, zdalnie) zdarzenie **[001]** jest rejestrowane.

Opcja: Nie rejestruj stanu WEJŚCIE SIŁOWE – gdy ta opcja jest załączona to zdarzenie **[005]: Wejście siłowe** związane ze stanem alarmowym WEJŚCIE SIŁOWE (patrz 3.9 Alarm Drzwi) nie jest rejestrowane w historii zdarzeń i nie jest prezentowane w Trybie Monitorowania. Sposoby wywołania tego alarmu są opisane w punkcie 3.10 Flagi Systemowe (Tajmery). Ta opcja nie blokuje

załączenia flagi WEJŚCIE SIŁOWE czy działania linii wyjściowych z funkcjami **[256]:Alarm drzwi** oraz **[28]: Wejście siłowe**.

Opcja: Nie rejestruj stanu Brak AC – gdy ta opcja jest załączona to stan alarmowy związany z awarią zasilania AC nie jest rejestrowany w historii zdarzeń, nie jest on prezentowany w Trybie Monitorowania programu PR Master ale linia wyjściowa z funkcją **[37]: Utrata napięcia sieci AC** jest odpowiednio załączana. Opcja dotyczy zarówno zasilania doprowadzonego bezpośrednio do kontrolera poprzez transformator 230VAC/18VAC (kontroler PR402) jak i współpracy z modułem PSAM-1 (patrz 3.2.6 Współpraca z modułem PSAM-1).

Opcja: Nie rejestruj stanu Niski Stan Akumulatora – gdy ta opcja jest załączona to stan alarmowy związany z niskim stanem podłączonego akumulatora nie jest rejestrowany w historii zdarzeń, nie jest on prezentowany w Trybie Monitorowania programu PR Master ale linia wyjściowa z funkcją **[38]: Niski stan akumulatora** jest odpowiednio załączana. Opcja dotyczy zarówno akumulatora podłączonego bezpośrednio do kontrolera (PR402) jak i współpracy z modułem PSAM-1 (patrz 3.2.6 Współpraca z modułem PSAM-1).

Opcja: Nie rejestruj zmiany stanów na linii [13]: Blokada uzbrojenia – gdy ta opcja jest załączona to zdarzenia **[13]: Blokada uzbrojenia – wyzwolenie** oraz **[13]: Blokada uzbrojenia – powrót** nie są rejestrowane w historii zdarzeń i nie są prezentowane w Trybie Monitorowania. Ta opcja nie ma wpływu na samo działanie linii wejściowej z funkcją **[13]: Blokada uzbrojenia**. Załączenie opcji blokuje jedynie zdarzenia a nie samą linię.

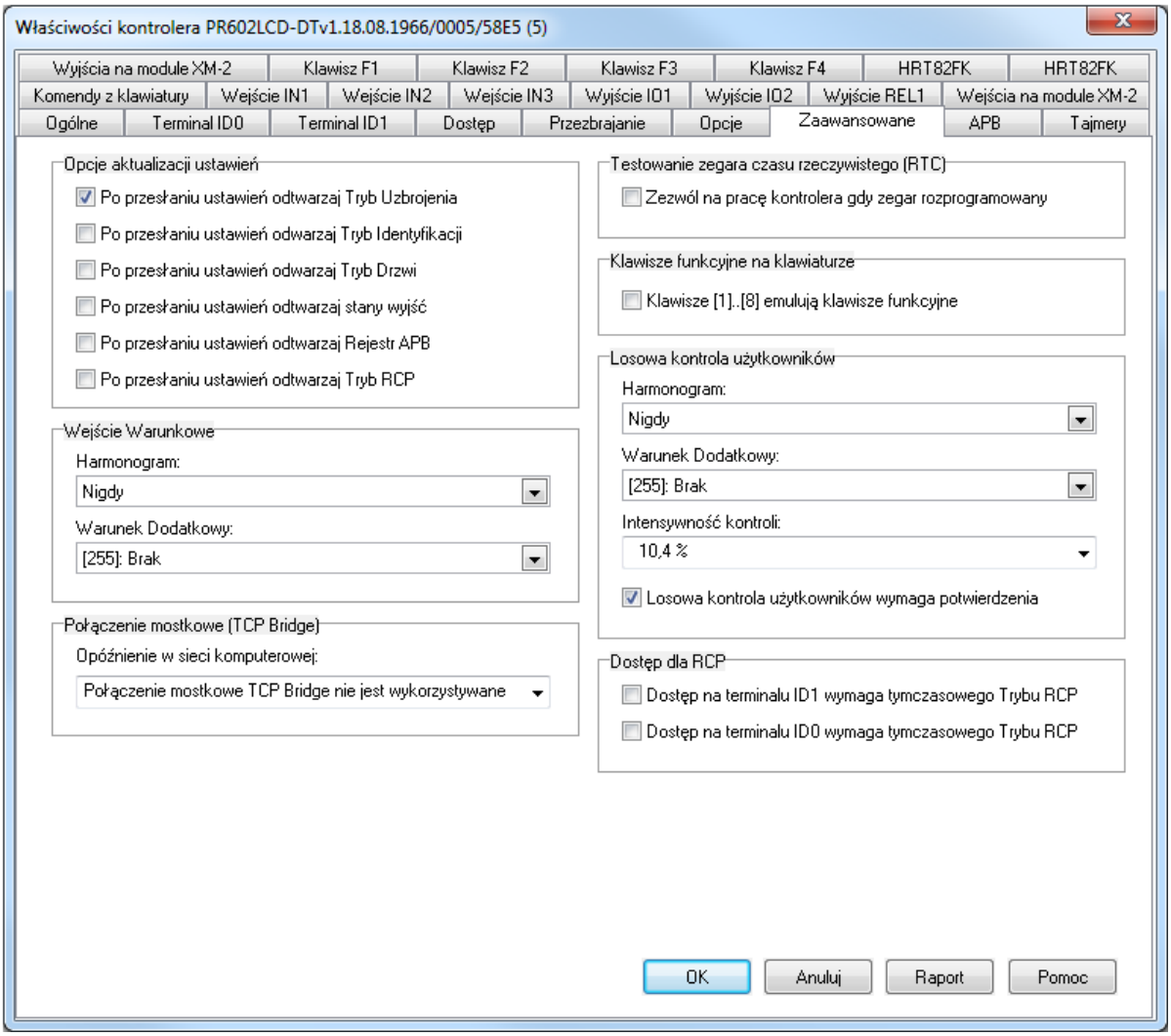
Obszar: Sterowanie Trybem RCP

Opcja: Sterowanie Trybem RCP z harmonogramu – gdy ta opcja jest załączona to możliwa jest zmiana Trybu RCP na czytniku Terminal ID1 (patrz 2.2 Budowa i przeznaczenie) w oparciu o Harmonogram Trybu RCP. W przypadku kontrolerów PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF i PR302 Terminal ID1 to zawsze czytnik wbudowany w kontroler. W przypadku kontrolerów PR402 i PR102DR, Terminal ID1 to jeden z czytników zewnętrznych. Procedura ustawiania harmonogramu RCP jest opisana w punkcie 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master.

Opcja: Term. ID0 przyjmuje ten sam Tryb RCP co Term. ID1 – gdy ta opcja jest załączona to Tryb RCP czytnika Terminal ID0 (patrz 2.2 Budowa i przeznaczenie) zmienia się współbieżnie z Trybem RCP czytnika Terminal ID1. Tryb RCP na Terminalu ID0 jest statyczny, natomiast Tryb RCP na czytniku ID1 może być zmieniany dynamicznie. Dzięki załączeniu tej opcji możliwe jest więc pośrednie dynamiczne zmienianie Trybu RCP na Terminalu ID0. Metody przełączania Trybów RCP na Terminalu ID1 podano w pkt. 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master.

Opcja: Harmonogram – w tym miejscu można wybrać Harmonogram Trybu RCP dla czytnika Terminal ID1. Procedura ustawiania Harmonogramów Trybu RCP, w tym harmonogramów zdefiniowanych przez administratora jest podana w punkcie 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master.

4.7 Zakładka Zaawansowane



Rys. 17 Zakładka Zaawansowane

Obszar: Opcje aktualizacji ustawień

Opcja: Po przesłaniu ustawień odtwarzaj Tryb Uzbrojenia – gdy ta opcja jest załączona to kontroler będzie powracał do stanu uzbrojenia (patrz 3.6 Tryby Uzbrojenia) sprzed momentu przesłania ustawień do kontrolera, chyba że koliduje to z Harmonogramem Przezbrajania, który ma wyższy priorytet (patrz 4.5 Zakładka Przezbrajanie). Gdy opcja nie jest zaznaczona to kontroler domyślnie, po przesłaniu konfiguracji ustawia się w Trybie Uzbrojonym, chyba że koliduje to z Harmonogramem Przezbrajania, który ma wyższy priorytet.

Opcja: Po przesłaniu ustawień odtwarzaj Tryb Identyfikacji - gdy ta opcja jest załączona to kontroler będzie powracał do Trybu Identyfikacji (3.4 Tryby Identyfikacji) ustawionego na kontrolerze przed przesłaniem ustawień. Ta opcja ma wyższy priorytet niż Tryb Identyfikacji ustawiany za pomocą harmonogramu czy też tryb domyślny (patrz 4.2 Zakładka Terminal ID).

Opcja: Po przesłaniu ustawień odtwarzaj Tryb Drzwi – gdy ta opcja jest załączona to kontroler będzie powracał do Trybu Drzwi (patrz 3.5 Tryby Drzwi) ustawionego na kontrolerze przed przesłaniem ustawień. Ta opcja ma wyższy priorytet niż Tryb Drzwi ustawiany za pomocą harmonogramu czy też tryb domyślny (patrz 4.4 Zakładka Dostęp).

Opcja: Po przesłaniu ustawień odtwarzaj stany wyjść – gdy ta opcja jest załączona to kontroler będzie przywracał stan załączenia swoich linii wyjściowych sprzed przesłania ustawień. To odtworzenie dotyczy linii wyjściowych z następującymi funkcjami:

- **[08]: Sterowanie z PC** gdy linia jest załączona zdalnie z poziomu programu PR Master
- **[13]: Harmonogram czasowy + komenda zdalna z PC** gdy linia jest załączona zdalnie z poziomu programu PR Master
- **[64]: ŚWIATŁO**
- **[66]: AUX1**
- **[67]: AUX2**

Opcja: Po przesłaniu ustawień odtwarzaj Rejestr APB – gdy ta opcja jest załączona to kontroler będzie przywracał Rejestr APB (patrz 3.11 Antypowrót (ang. Anti-passback)) sprzed przesłania ustawień.

Opcja: Po przesłaniu ustawień odtwarzaj Tryb RCP – gdy ta opcja jest załączona to kontroler będzie powracał do Trybu RCP (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master) ustawionego na kontrolerze przed przesłaniem ustawień. Ta opcja ma wyższy priorytet niż Tryb RCP ustawiany za pomocą harmonogramu (patrz 4.6 Zakładka Opcje) czy też tryb domyślny (patrz 4.2 Zakładka Terminal ID).

Obszar: Wejście Warunkowe

W tym obszarze można ustawić Wejście Warunkowe (patrz 3.17.2 Wejście Warunkowe) oraz przypisać do niego harmonogram i Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są harmonogramy wbudowane Zawsze i Nigdy. Można również przypisać własny harmonogram definiując Harmonogram Ogólnego Przeznaczenia za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do harmonogramu wskazuje przedział czasowy, w którym Wejście Warunkowe będzie obowiązywać. Aby tryb Wejście Warunkowe funkcjonował konieczne jest zaznaczenie opcji **Załącz APB (Anti-passback)** w zakładce **APB**.

Obszar: Połączenie mostkowe (TCP Bridge)

W tym miejscu można ustawić opóźnienie w przypadku, gdy kontroler jest dołączony do magistrali RS485 za pośrednictwem mostka komunikacyjnego złożonego z dwóch interfejsów UT-4 komunikujących się za pośrednictwem sieci komputerowej. Dostępny zakres ustawień opóźnienia mieści się w przedziale od 20ms do 5s z rozdzielczością 20ms.

Obszar: Testowanie zegara czasu rzeczywistego (RTC)

Opcja: Zezwól na pracę kontrolera gdy zegar rozprogramowany – gdy ta opcja jest załączona to kontroler nie będzie testował poprawności ustawień własnego zegara czasu rzeczywistego co w rezultacie będzie oznaczać, że kontroler będzie mógł funkcjonować również wtedy gdy ten zegar będzie rozprogramowany.

Obszar: Klawisze funkcyjne na klawiaturze

Ten obszar jest widoczny jedynie w przypadku kontrolerów PR602LCD, PR612, PR312EM, PR312MF oraz PR302 czyli kontrolerów wyposażonych w klawiaturę. W tym obszarze dostępna jest opcja, której załączenie umożliwia stosowanie klawiszy numerycznych jako klawiszy funkcyjnych. Klawisze 1…4 odpowiadają wtedy klawiszom funkcyjnym F1…F4 na Terminalu ID1 a klawisze 5…8 odpowiadają klawiszom funkcyjnym F1…F4 na Terminalu ID0 (patrz 2.2 Budowa i przeznaczenie oraz 3.15 Klawisze funkcyjne).

Obszar: Losowa kontrola użytkowników

Funkcja ta służy do wyrywkowego wyznaczania osób celem ich zrewidowania. Gdy funkcja jest załączona kontroler losowo odmawia prawa dostępu użytkownikowi i sygnalizuje strażnikom konieczność wykonania kontroli. Sygnalizacja kontroli losowej jest realizowana akustycznie na wewnętrznym głośniku oraz wyświetlaczu LCD za pomocą komunikatu „STOP Losowa kontrola” (tylko PR602LCD-DT i PR602LCD). Dodatkowo może ona być również sygnalizowana na linii

wyjściowej z funkcją **[39]: Żądanie losowej kontroli** (patrz 3.14 Linie wyjściowe kontrolera). Sygnalizacja kontroli trwa przez 2 s i w czasie tym kontroler wstrzymuje dalsze przyznawanie dostępu. Losowa kontrola dotyczy jedynie użytkowników typu NORMAL (patrz 3.3 Użytkownicy).
Załączenie losowej kontroli użytkowników wymaga wybrania harmonogramu z listy rozwijanej. Można zastosować jeden z harmonogramów wbudowanych tj. Zawsze oraz Nigdy lub zastosować własny Harmonogram Ogólnego Przeznaczenia, który musi być wcześniej zdefiniowany za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. W okresach czasu zdefiniowanych w harmonogramie obowiązuje losowa kontrola użytkowników a w pozostałych okresach jest ona wyłączona. Załączenie losowej kontroli użytkowników (jej harmonogramu) może być skojarzone z Warunkiem Dodatkowym (patrz 3.16 Harmonogramy i Warunki dodatkowe). Losowa kontrola użytkowników jest załączana zgodnie z wybranym harmonogramem po spełnieniu wybranego Warunku Dodatkowego.

Parametr: Intensywność kontroli – w tym miejscu można ustawić jaki statystycznie procent użytkowników będzie podlegać kontroli. Dostępny zakres ustawień intensywności mieści się w przedziale od 0,4% do 99,6% z rozdzielczością 0,4%. Im wyższa wartość zostanie wybrana tym częstsza będzie kontrola użytkowników. Dla przykładu ustawienie intensywności na poziomie 10% powoduje, że statystycznie biorąc co dziesiąta osoba zostanie wyznaczona do kontroli.

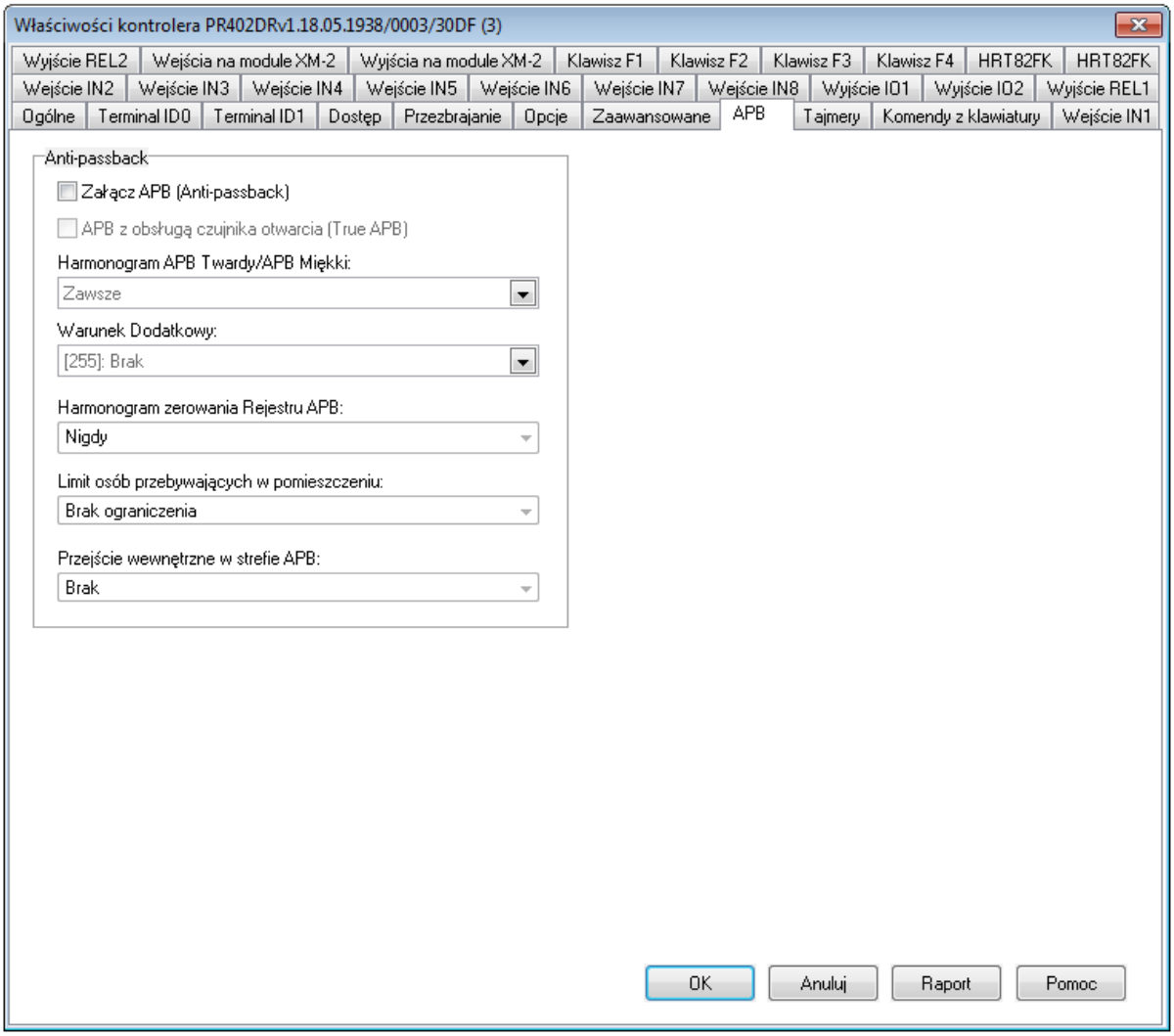
Opcja: Losowa kontrola użytkowników wymaga potwierdzenia – gdy ta opcja jest załączona to w momencie sygnalizacji kontroli losowej, kontroler blokuje przejście do momentu wyzwolenia linii wejściowej z funkcją **[46]: Losowa kontrola – potwierdzenie** (patrz 3.13 Linie wejściowe kontrolera) lub użycia klawisza funkcyjnego z funkcją **[46]: Losowa kontrola – potwierdzenie** (patrz 3.15 Klawisze funkcyjne).

Obszar: Dostęp dla RCP

Opcja: Dostęp na terminalu ID1 wymaga tymczasowego Trybu RCP – gdy ta opcja jest załączona to użytkownik bez względu na swoje prawa dostępu nie może uzyskać dostępu na terminalu ID1 dopóki nie zostanie wybrany tymczasowy tryb RCP. Taki tryb RCP można aktywować na 8 sek. za pomocą wyjścia lub klawisza funkcyjnego z funkcją **[49]: Wybierz Tryb RCP z klawiatury – zmiana chwilowa**, **[51]: Następny Tryb RCP – zmiana chwilowa** lub **[57]: Ustaw predefiniowany Tryb RCP – zmiana chwilowa**.

Opcja: Dostęp na terminalu ID0 wymaga tymczasowego Trybu RCP – jak wyżej, tyle że dotyczy terminala ID0.

4.8 Zakładka APB



Rys. 18 Zakładka APB

Obszar: Anti-passback

Opcja: Załącz APB – gdy ta opcja jest załączona to mechanizm Anti-passbacku Lokalnego oraz Globalnego jest załączony i możliwe jest wprowadzenie kolejnych związanych z tym ustawień (patrz 3.11 Antypowrót (ang. Anti-passback)).

Opcja: APB z obsługą czujnika otwarcia (True APB) – tą opcję można zaznaczyć po załączeniu opcji: **Załącz APB**. Umożliwia ona obsługę tzw. True APB (patrz 3.11 Antypowrót (ang. Anti-passback)), w ramach którego wymagane jest podłączenie czujnika otwarcia drzwi do linii wejściowej kontrolera z funkcją **[01]: Czujnik otwarcia drzwi**.

Opcja: Harmonogram APB Twardy/Miękki – w tym miejscu można ustawić jeden z harmonogramów wbudowanych tj. Zawsze oraz Nigdy lub Harmonogram Ogólnego Przeznaczenia zdefiniowany za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. W okresach zdefiniowanych w harmonogramie obowiązuje APB Twardy a w pozostałych okresach APB Miękki (patrz 3.11 Antypowrót (ang. Anti-passback)). Wybranie harmonogramu wbudowanego Zawsze oznacza, że przez cały czas obowiązuje APB Twardy a wybranie harmonogramu Nigdy oznacza, że przez cały czas obowiązuje APB Miękki.

Opcja: Warunek Dodatkowy - tym miejscu można przypisać Warunek Dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe) do Harmonogramu APB Twardy/Miękki. Gdy Warunek Dodatkowy nie jest spełniony to obowiązuje APB Miękki a gdy jest spełniony to załączany jest wtedy Harmonogram APB Twardy/Miękki.

Opcja: Harmonogram Zerowania Rejestru APB – w tym miejscu można ustawić harmonogram wbudowany Nigdy lub jeden z Harmonogramów Zerowania APB zdefiniowany przez administratora systemu za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Więcej informacji, patrz 3.11 Antypowrót (ang. Anti-passback).

Parametr: Limit osób w pomieszczeniu – w tym miejscu można ustawić maksymalną ilość osób przebywających w danym pomieszczeniu z pojedynczymi drzwiami. Ta opcja dotyczy Lokalnego APB (realizowanego w ramach jednego kontrolera). W przypadku Globalnego APB limit osób ustala się podczas tworzenia Strefy APB za pomocą opcji **Strefy APB** w oknie głównym programu PR Master. Dostępny zakres ustawień limitu w przedziale od 1 do 3999. Więcej informacji patrz 3.11 Antypowrót (ang. Anti-passback).

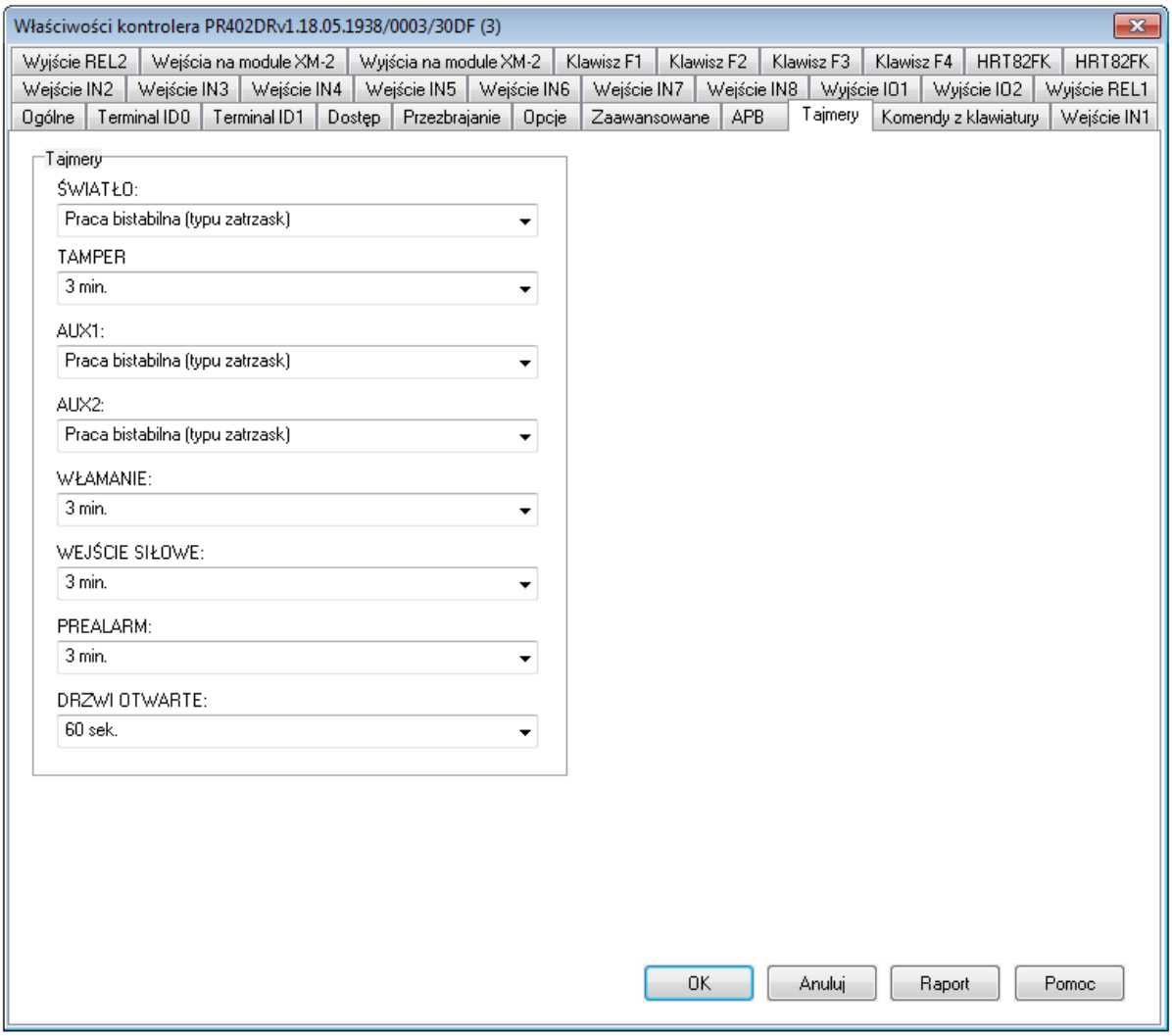
Opcja: Przejście wewnętrzne w strefie APB – w tym miejscu można przypisać kontroler (wraz z jego terminalami) do Strefy APB po to by utworzyć przejście wewnętrzne w tej Strefie APB. Użytkownik może uzyskać dostęp na takim przejściu tylko wtedy gdy dostał się do tej Strefy APB poprzez jeden z jej punktów/terminali wejściowych. Więcej informacji na temat APB podano w 3.11 Antypowrót (ang. Anti-passback).

4.9 Zakładka Tajmery

W tej zakładce dostępne są ustawienia związane z Flagami Systemowymi zwanymi również Tajmerami (patrz 3.10 Flagi Systemowe (Tajmery)). Możliwe jest ustawienie pracy bistabilnej (zatrzask) polegającej na tym, że dany Tajmer jest załączany do momentu zmiany swojego stanu, możliwe jest też całkowite wyłączenie Tajmera oraz przypisanie mu czasu z listy rozwijanej.

Przykład:
*Załączenie Tajmera ŚWIATŁO, który załącza linię wyjściową z funkcją **[64]: ŚWIATŁO** na przykład za pomocą linii wejściowej z funkcją **[68]: Załącz światło** w przypadku ustawienia trybu pracy bistabilnej będzie skutkować tym, że linia wyjściowa **[64]** będzie załączona do momentu wyzwolenia linii wejściowej z funkcją **[69]: Wyłącz światło**.*

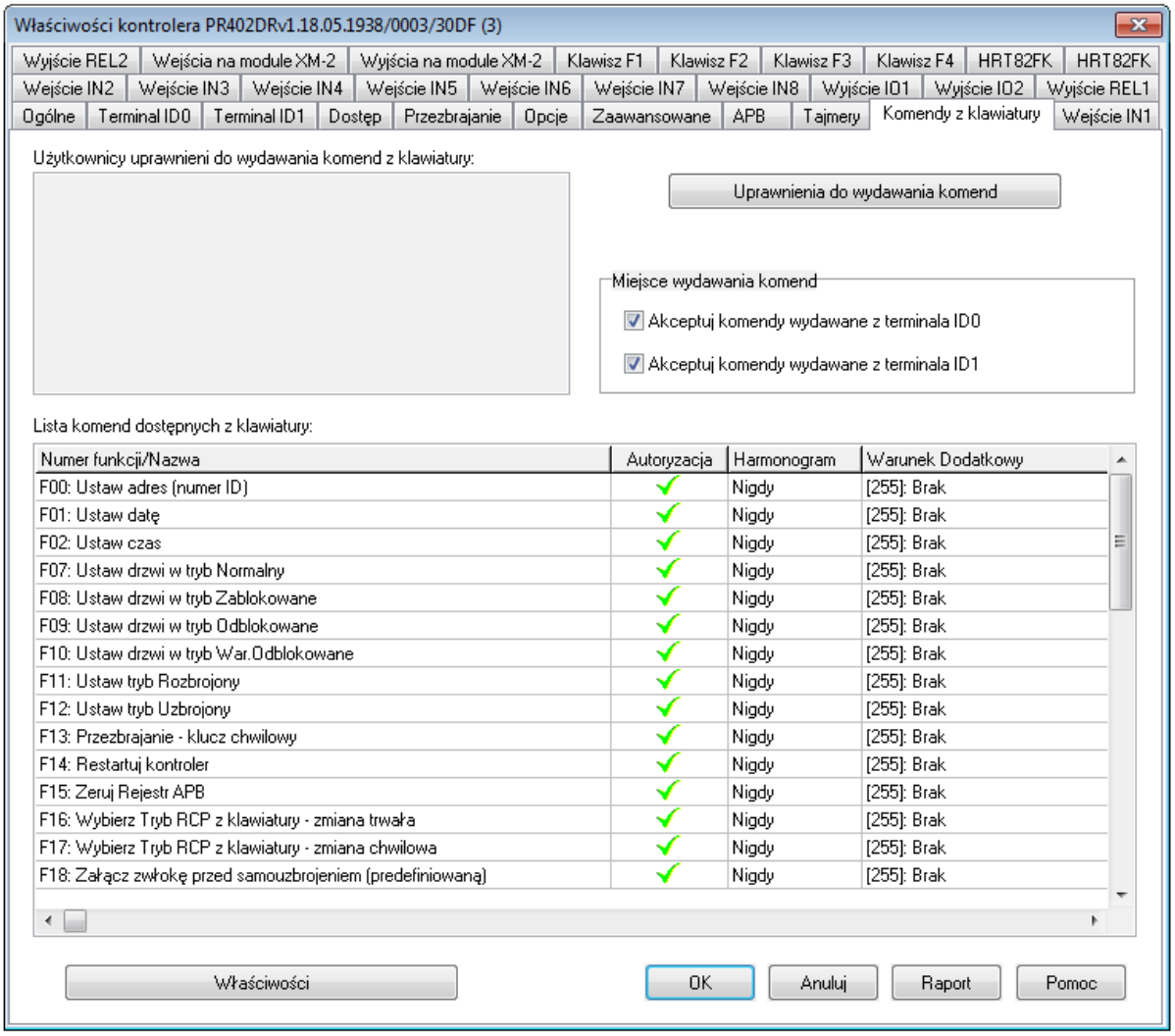
W przypadku ustawienia wartości czasowej dla danej Flagi, może ona być załączana na ten właśnie czas. Dostępny zakres ustawień czasowych Tajmera mieści się w przedziale od 1 sekundy do 120 minut.



Rys. 19 Zakładka Tajmery

4.10 Zakładka Komendy z klawiatury

W tej zakładce możliwe jest ustawienie warunków stosowania Komend z klawiatury kontrolera/czytnika (patrz 3.18 Komendy z klawiatury oraz 2.2 Budowa i przeznaczenie). Możliwe jest również odczytanie jak się daną komendę wprowadza poprzez zaznaczenie danej komendy wskaźnikiem myszki i wybranie przycisku **Właściwości**. W nowo otwartym oknie można również danej komendzie przypisać harmonogram oraz Warunek Dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są dwa harmonogramy wbudowane tj. Zawsze i Nigdy, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym komenda może być używana ale wciąż może ona wymagać autoryzacji. Wybranie harmonogramu Nigdy oznacza, że dana komenda jest całkowicie zablokowana. W tym samym oknie można wybrać czy dana komenda wymaga autoryzacji. Autoryzacja polega na użyciu identyfikatora (karty zbliżeniowej lub kodu PIN) użytkownika, który został dopisany za pomocą opcji **Uprawnienia do wydawania komend.**



Rys. 20 Zakładka Komendy z klawiatury

Opcja: Uprawnienia do wydawania komend – za pomocą tej opcji można ustawić, którzy użytkownicy będą mieli prawo stosować Komendy z klawiatury, gdy komendy mają załączoną Autoryzację.

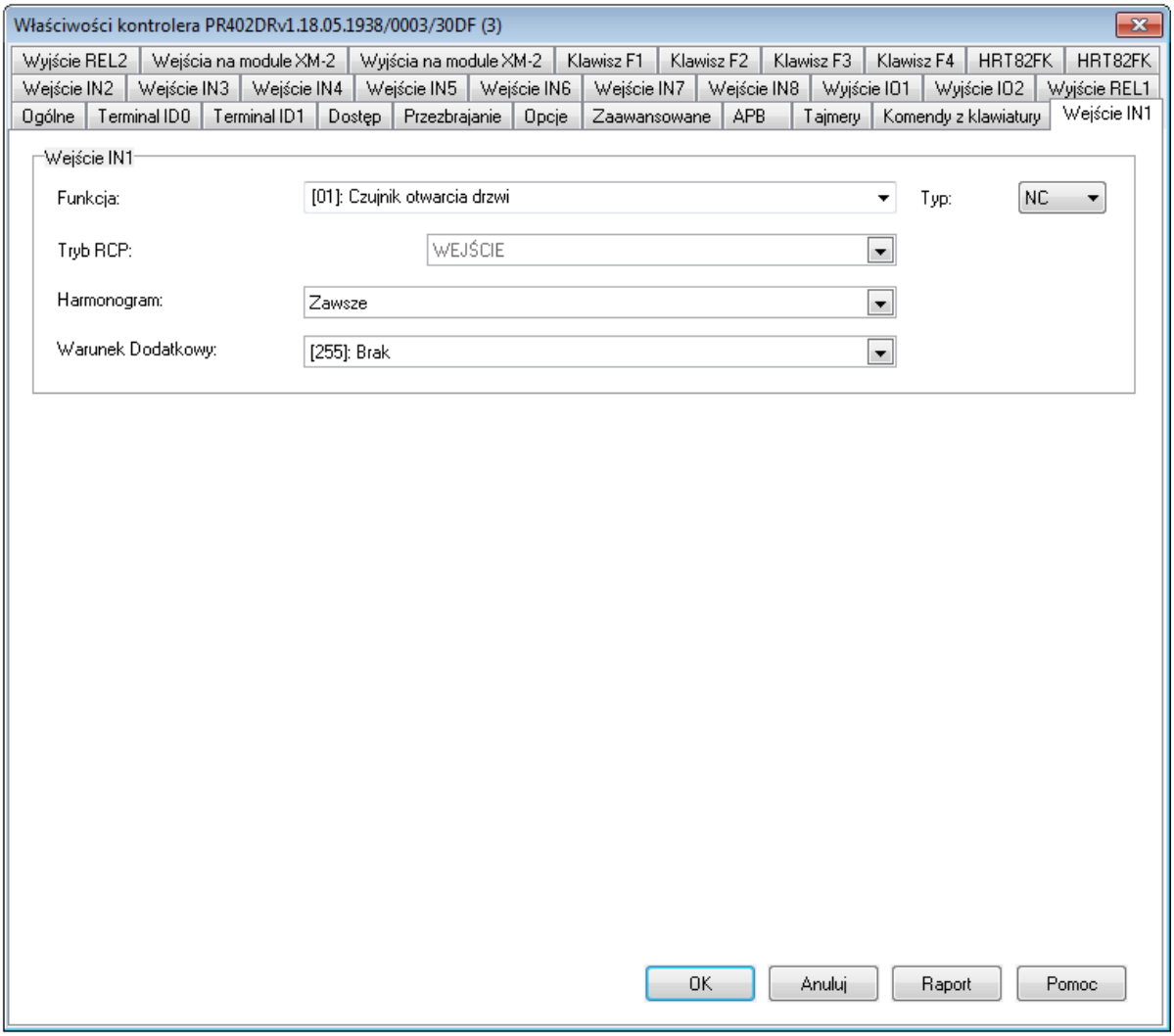
Opcja: Akceptuj komendy wydawane z terminala ID0 – gdy ta opcja jest załączona to można wprowadzać komendy (patrz 3.18 Komendy z klawiatury) za pomocą klawiatury na Terminalu ID0 (patrz 2.2 Budowa i przeznaczenie).

Opcja: Akceptuj komendy wydawane z terminala ID1 – gdy ta opcja jest załączona to można wprowadzać komendy (patrz 3.18 Komendy z klawiatury) za pomocą klawiatury na Terminalu ID1 (patrz 2.2 Budowa i przeznaczenie).

4.11 Zakładki Wejście IN1…IN8

W zależności od tego ile fizycznie linii wejściowych posiada kontroler (patrz Tabela 1), dostępne jest od 2 do 8 zakładek wyjść. W zakładce **Wejście IN1** oraz pozostałych zakładkach wejść, można przypisać określoną funkcję (patrz 3.13 Linie wejściowe kontrolera) do danej linii wejściowej. Można również określić jaki jest typ danej linii - NC (normally close) lub NO (normally open). W przypadku funkcji związanych z Trybami RCP (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master) można wybrać Tryb RCP ustawiany przez daną linię wejściową. Z daną linią wejściową można skojarzyć Harmonogram oraz Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można

przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym linia wejściowa będzie mogła być załączana. W przypadku wybrania harmonogramu Zawsze, linia wejściowa będzie mogła być używana w każdym momencie. Przypisany harmonogram nie załącza danej linii wejściowej a jedynie odblokowuje lub blokuje możliwość jej załączania w określonych przedziałach czasu.

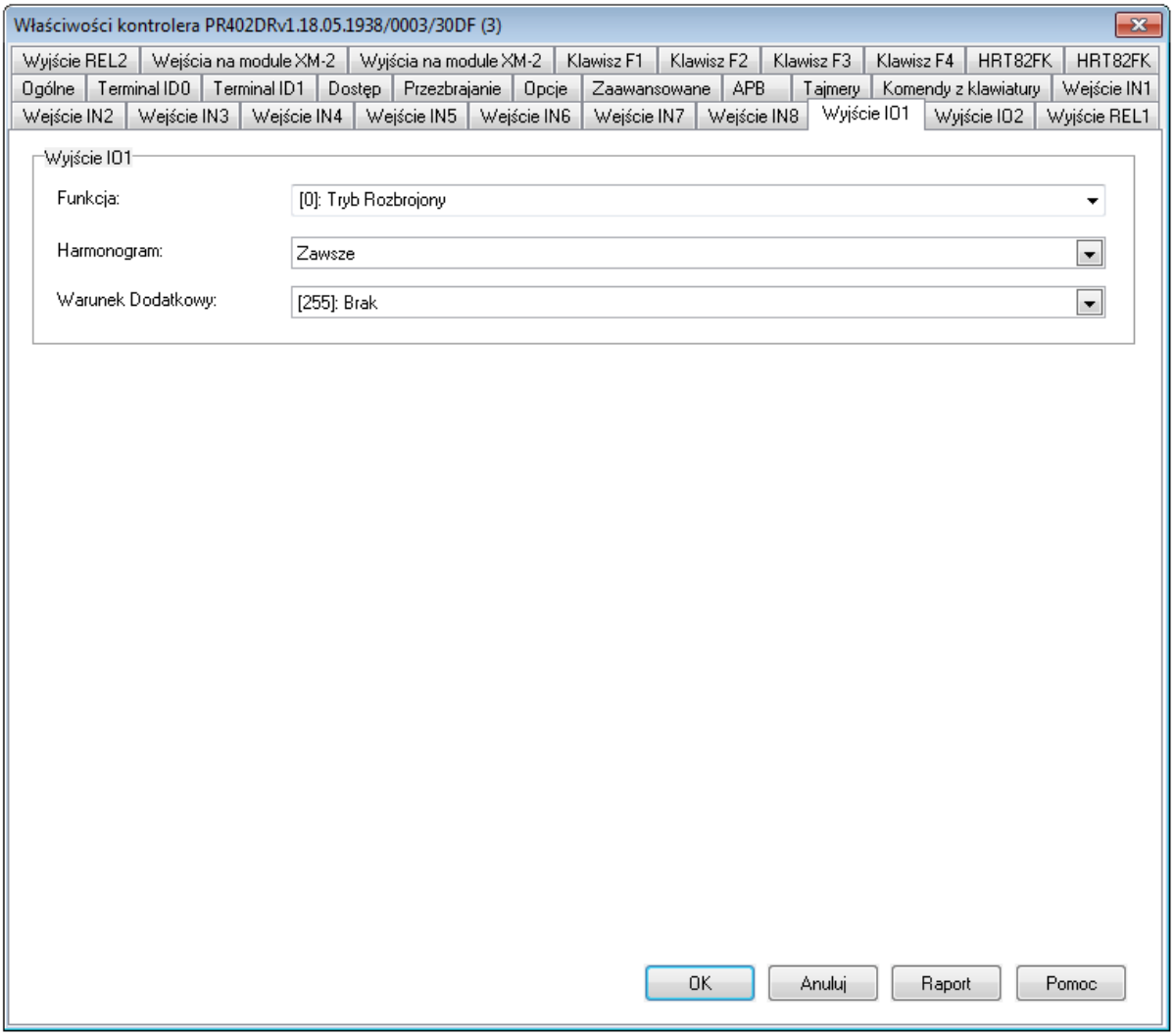


Rys. 21 Zakładka Wejście IN1

4.12 Zakładki Wyjście IO1…IO2

W zależności od tego ile fizycznie wyjść tranzystorowych posiada kontroler (patrz Tabela 1) dostępne są 1 lub 2 zakładki wyjść. W zakładce **Wyjście IO1** lub **Wyjście IO2**, można przypisać do nich określoną funkcję (patrz 3.14 Linie wyjściowe kontrolera). Z daną linią wyjściową można skojarzyć Harmonogram oraz Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym linia wyjściowa będzie mogła być załączana. W przypadku wybrania harmonogramu Zawsze, linia wyjściowa będzie mogła być używana w każdym momencie. Przypisany harmonogram nie załącza danej linii wyjściowej a jedynie odblokowuje lub blokuje możliwość jej załączania w danym przedziale czasu. Wyjątek stanowią funkcje **[12]:**

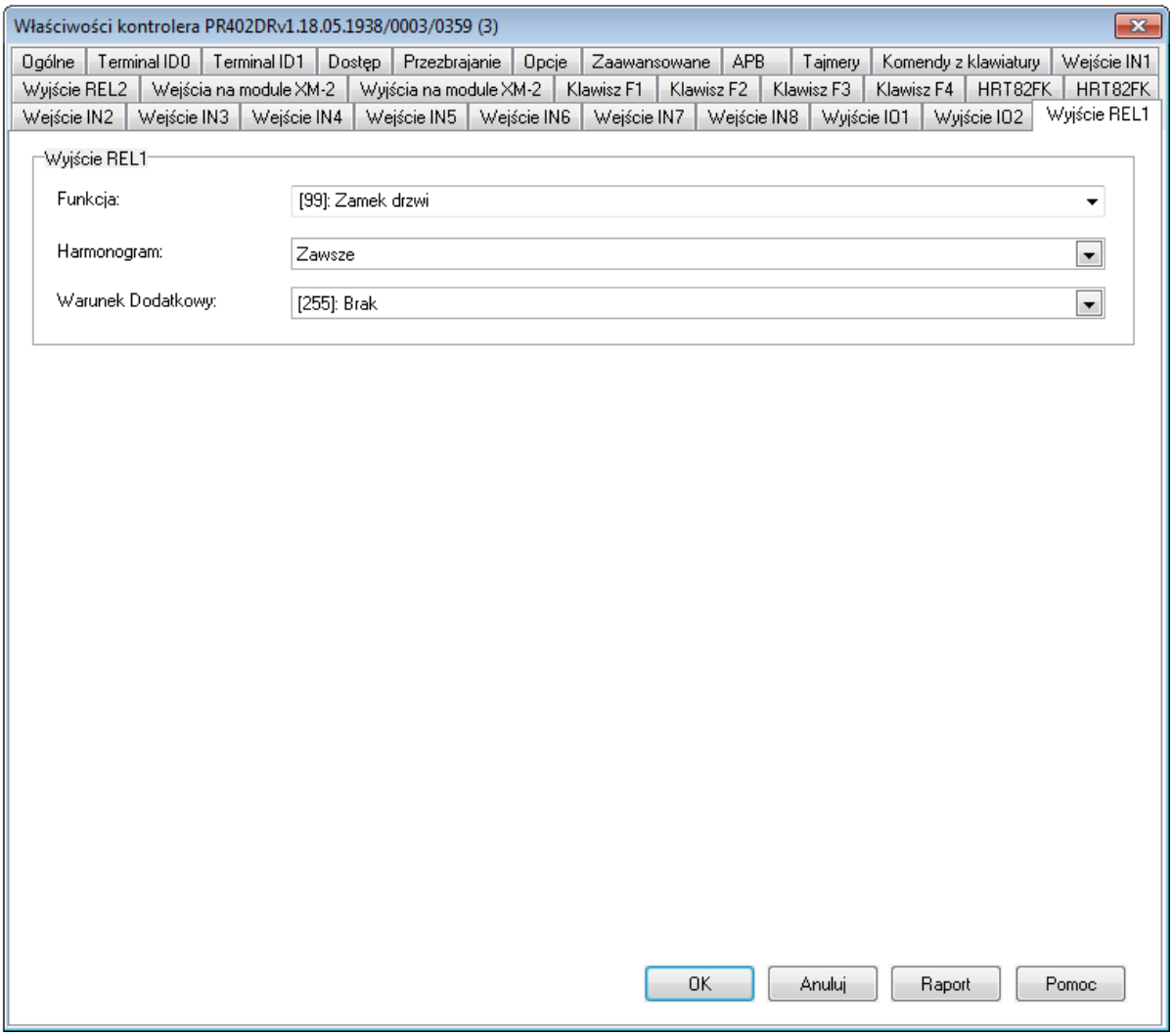
Harmonogram czasowy oraz **[13]: Harmonogram czasowy + komenda zdalna z PC**, które są załączane właśnie w oparciu o przypisany do nich harmonogram.



Rys. 22 Zakładka Wyjście IO1

4.13 Zakładki Wyjście REL1…REL2

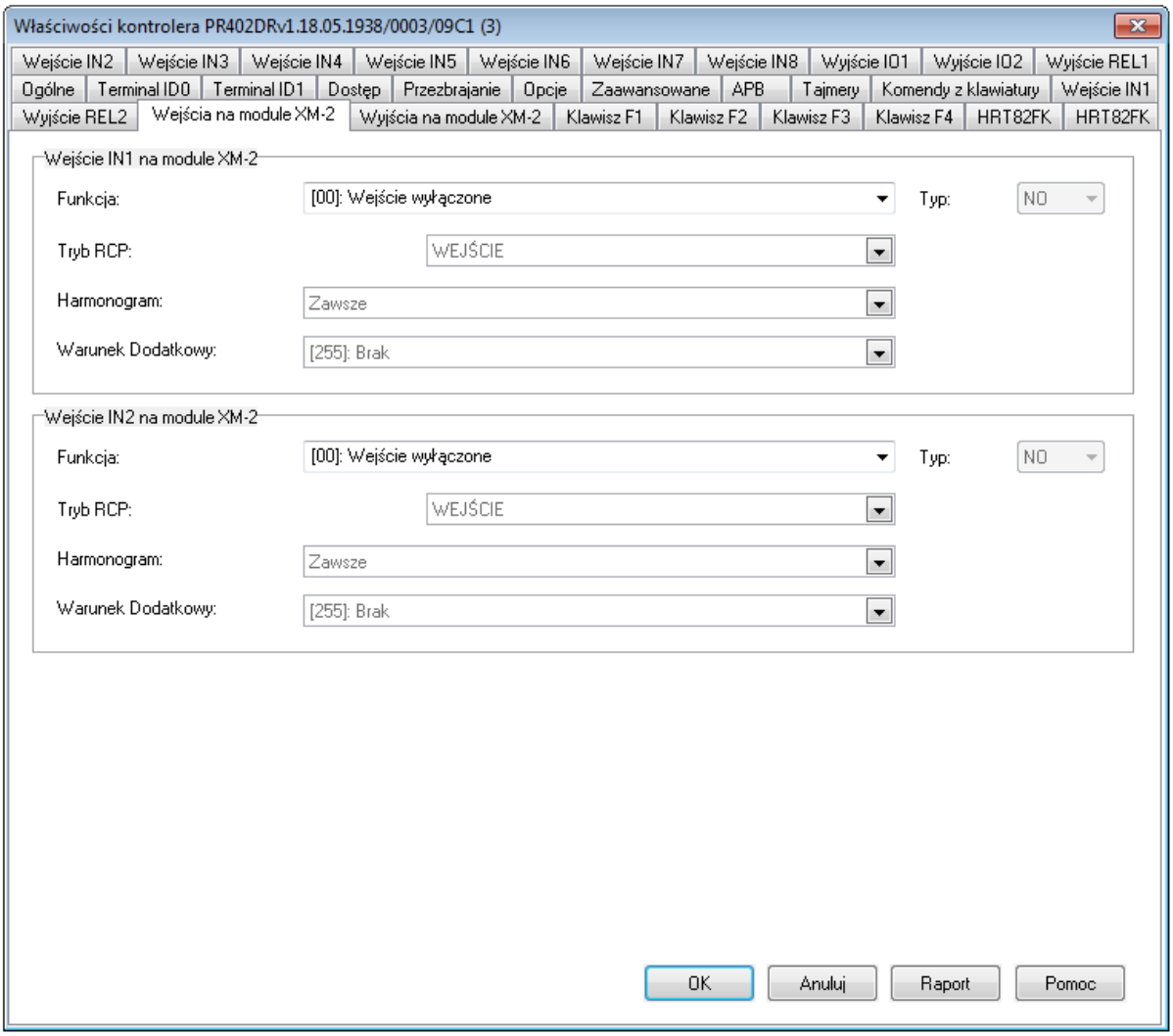
W zależności od tego ile fizycznie wyjść przekaźnikowych posiada kontroler (patrz Tabela 1) dostępne są 1 lub 2 zakładki wyjść. W zakładce **Wyjście REL1** lub **Wyjście REL2**, można przypisać do nich określoną funkcję (patrz 3.14 Linie wyjściowe kontrolera). Z daną linią wyjściową można skojarzyć Harmonogram oraz Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym linia wyjściowa będzie mogła być załączana. W przypadku wybrania harmonogramu Zawsze, linia wyjściowa będzie mogła być używana w każdym momencie. Przypisany harmonogram nie załącza danej przekaźnikowej linii wyjściowej a jedynie odblokowuje lub blokuje możliwość jej załączania w danym przedziale czasu. Domyślnym ustawieniem wyjścia REL1 jest funkcja **[99]: Zamek drzwi**, która jest stosowana do zwalniania zamka drzwi.



Rys. 23 Zakładka Wyjście REL1

4.14 Zakładka Wejścia na module XM-2

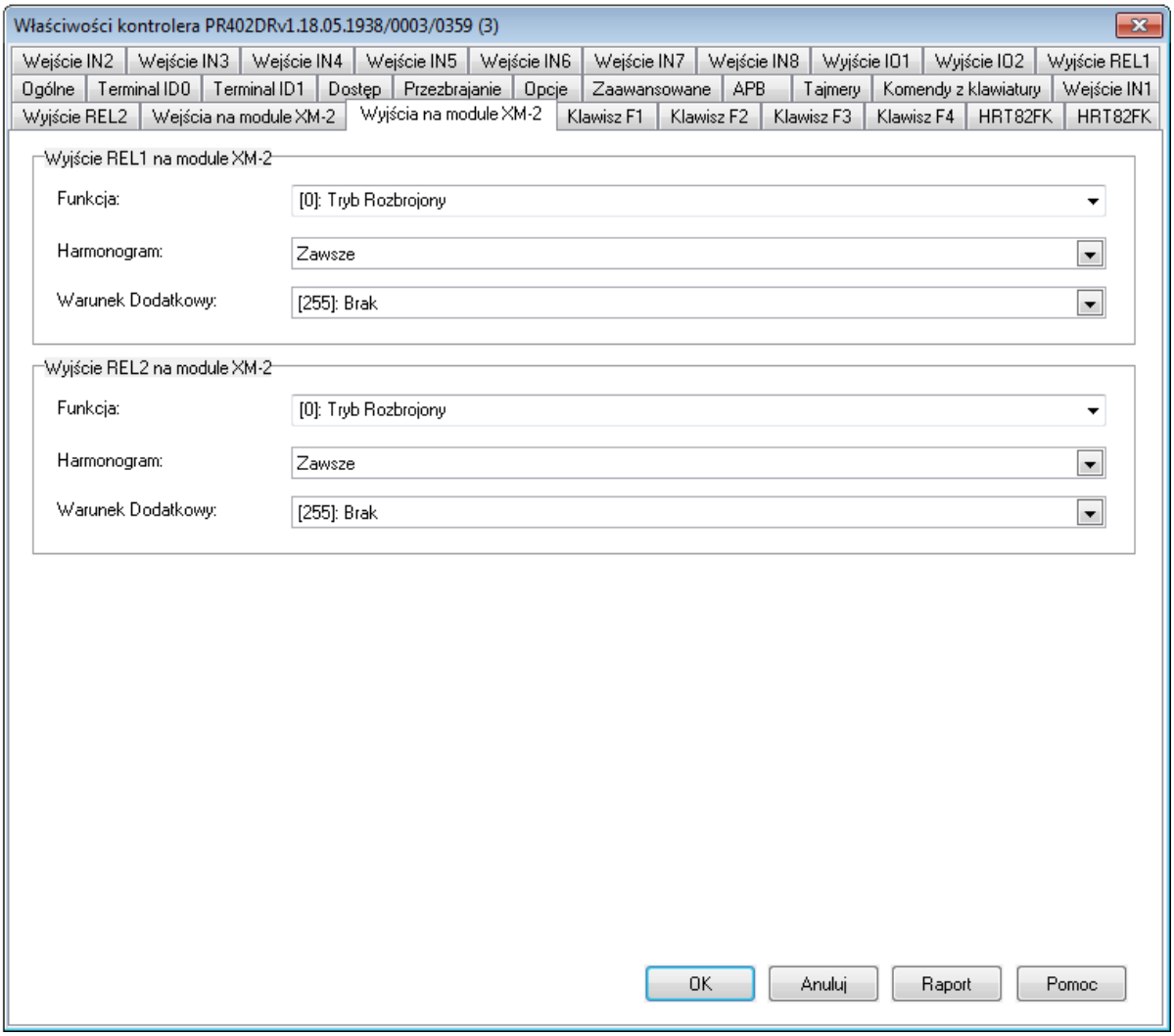
Do kontrolera firmy ROGER można podłączyć ekspander XM-2 (patrz 3.2.4 Współpraca z ekspanderem WE/WY XM-2), który zwiększa całkowitą ilość linii wejściowych obsługiwanych przez kontroler o dwie linie dostępne na tym właśnie module. Aby ekspander XM-2 mógł być obsługiwany to oprócz jego podłączenia do kontrolera za pomocą magistrali RACS CLK/DTA (patrz 3.2.3 Interfejs RACS CLK/DTA) trzeba go również załączyć za pomocą opcji **Załącz obsługę ekspandera XM-2** dostępnej w zakładce **Opcje** we właściwościach kontrolera. Linie wejściowe ekspandera XM-2 konfiguruje się identycznie jak linie wejściowe dostępne w zakładkach **Wejście IN1…IN8** (patrz 4.11 Zakładki Wejście IN1…IN8)



Rys. 24 Zakładka Wejścia na module XM-2

4.15 Zakładka Wyjścia na module XM-2

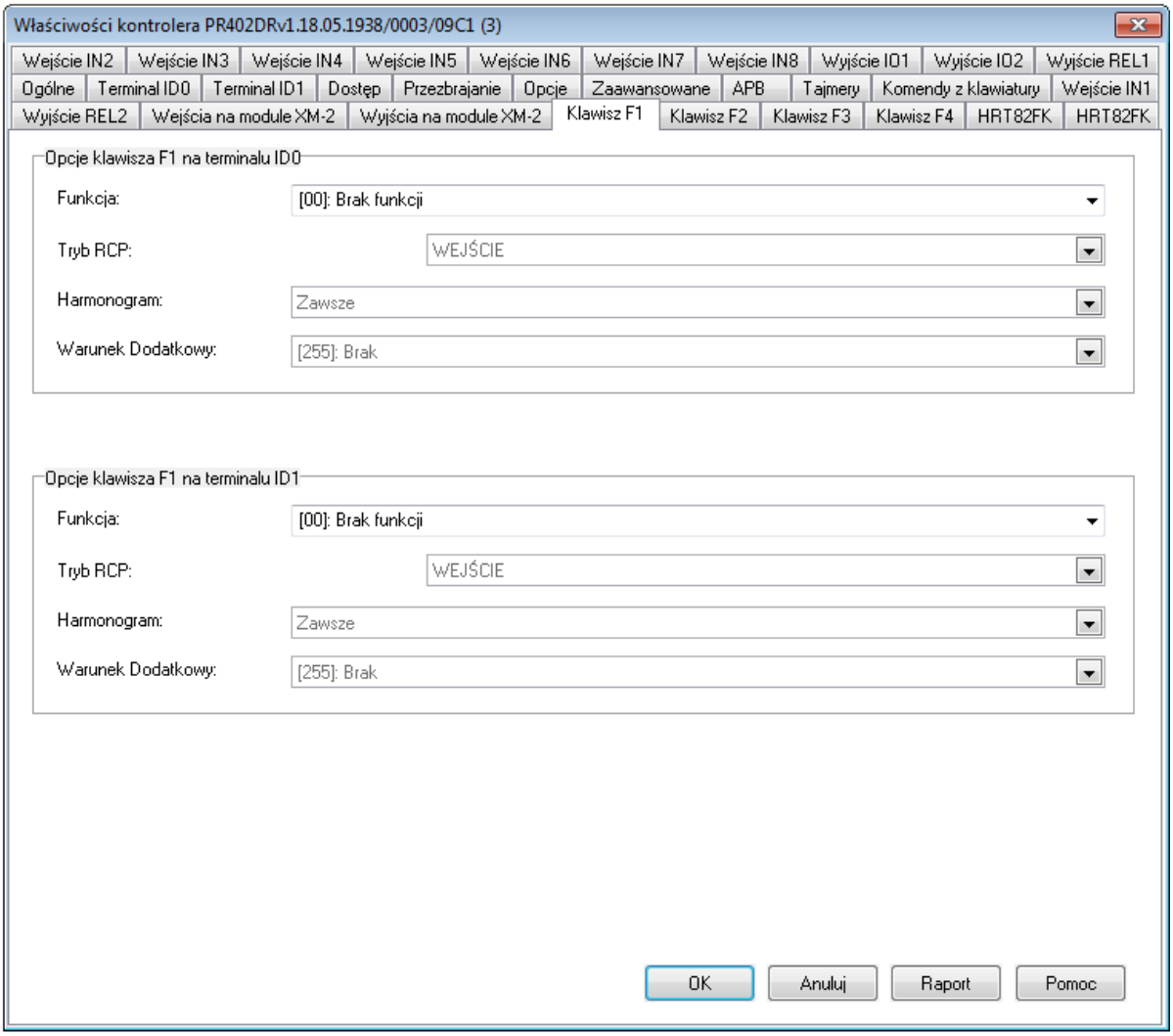
Do kontrolera firmy ROGER można podłączyć ekspander XM-2 (patrz 3.2.4 Współpraca z ekspanderem WE/WY XM-2), który zwiększa całkowitą ilość przekaźnikowych linii wyjściowych obsługiwanych przez kontroler o dwie linie dostępne na tym właśnie module. Aby ekspander XM-2 mógł być obsługiwany to oprócz jego podłączenia do kontrolera za pomocą magistrali RACS CLK/DTA (patrz 3.2.3 Interfejs RACS CLK/DTA) trzeba go również załączyć za pomocą opcji **Załącz obsługę ekspandera XM-2** dostępnej w zakładce **Opcje** we właściwościach kontrolera. Przekaźnikowe linie wyjściowe ekspandera XM-2 konfiguruje się identycznie jak przekaźnikowe linie wyjściowe dostępne w zakładkach **Wyjście REL1...REL2** (patrz 4.13 Zakładki Wyjście REL1…REL2).



Rys. 25 Zakładka Wyjścia na module XM-2

4.16 Zakładki Klawisz F1…F4

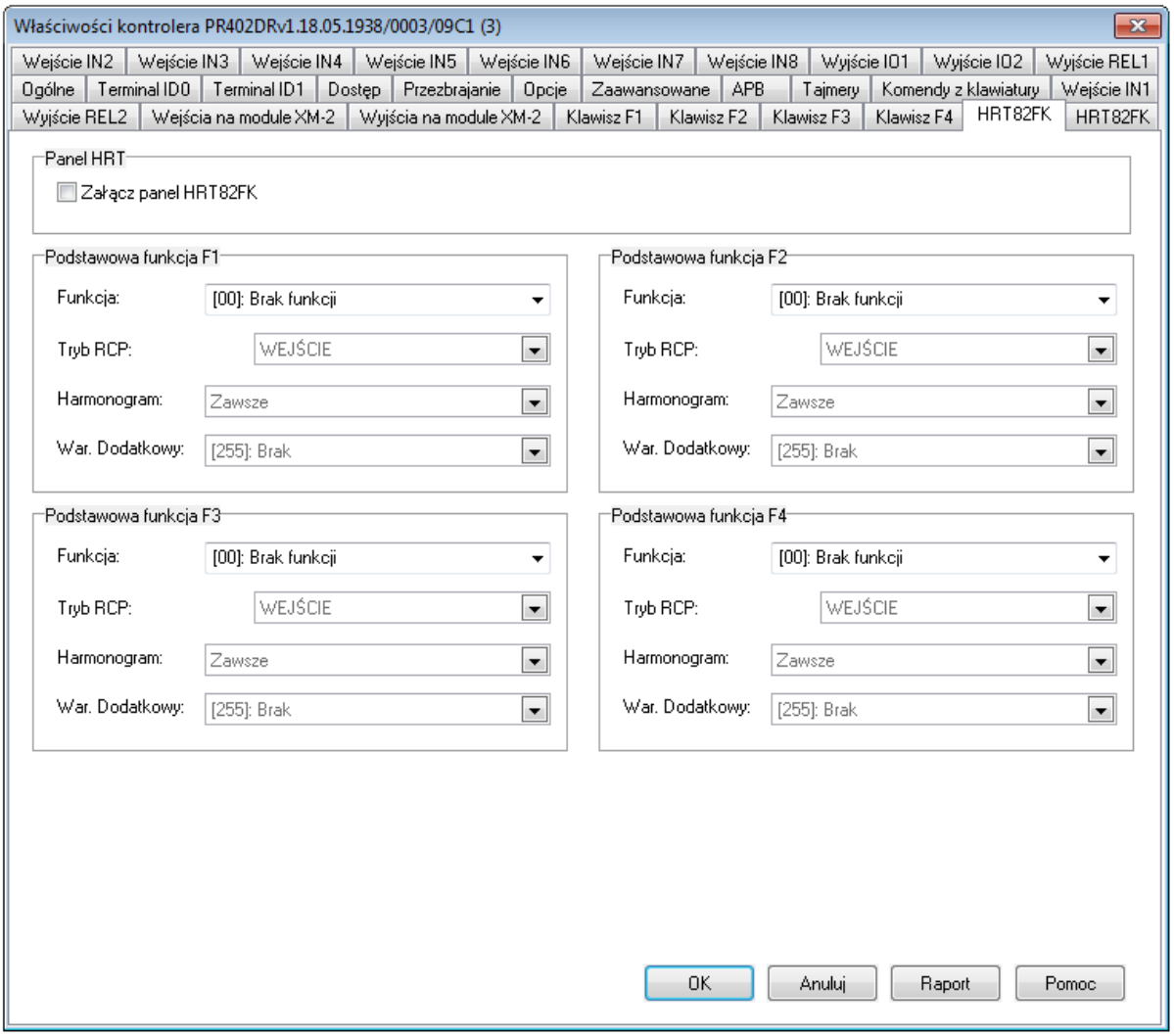
W programie PR Master, we właściwościach kontrolera dostępne są 4 zakładki związane z klawiszami funkcyjnymi. Fizycznie, klawiaturę z czterema klawiszami funkcyjnymi posiadają jedynie kontrolery PR602LCD-DT i PR602LCD. Natomiast do wszystkich kontrolerów firmy ROGER można podłączyć czytnik zewnętrzny z klawiaturą i dwoma klawiszami funkcyjnymi (model PRT12LT). W zakładkach **Klawisz F1…F4** można wprowadzać ustawienia dla klawiszy funkcyjnych na Terminalu ID1 oraz Terminalu ID0 (patrz 2.2 Budowa i przeznaczenie). W ramach dostępnych opcji do danego klawisza można przypisać funkcję (patrz 3.15 Klawisze funkcyjne) jak również skojarzyć ją z Harmonogramem i Warunkiem dodatkowym (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są dwa harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym klawisz będzie mógł być używany. W przypadku wybrania harmonogramu Zawsze, klawisz będzie mógł być stosowany przez cały czas. Przypisany harmonogram nie załącza danego klawisza a jedynie odblokowuje możliwość jego załączania w danych przedziałach czasu. W przypadku funkcji związanych z Trybami RCP (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master) można wybrać Tryb RCP ustawiany przez dany klawisz funkcyjny.



Rys. 26 Zakładka Klawisz F1

4.17 Zakładki HRT82FK

Do kontrolera firmy ROGER można podłączyć panel klawiszy funkcyjnych HRT82FK (patrz 3.2.7 Współpraca z panelem HRT82FK), który zwiększa całkowitą ilość klawiszy funkcyjnych obsługiwanych przez kontroler o cztery klawisze dostępne na tym właśnie panelu. Każdemu klawiszowi można przypisać dwie różne funkcje (podstawową i dodatkową) aktywowane odpowiednio poprzez krótkie i długie przyciśnięcie. Aby panel HRT82FK mógł być obsługiwany to należy podłączyć go do kontrolera za pomocą magistrali RACS CLK/DTA (patrz 3.2.3 Interfejs RACS CLK/DTA).



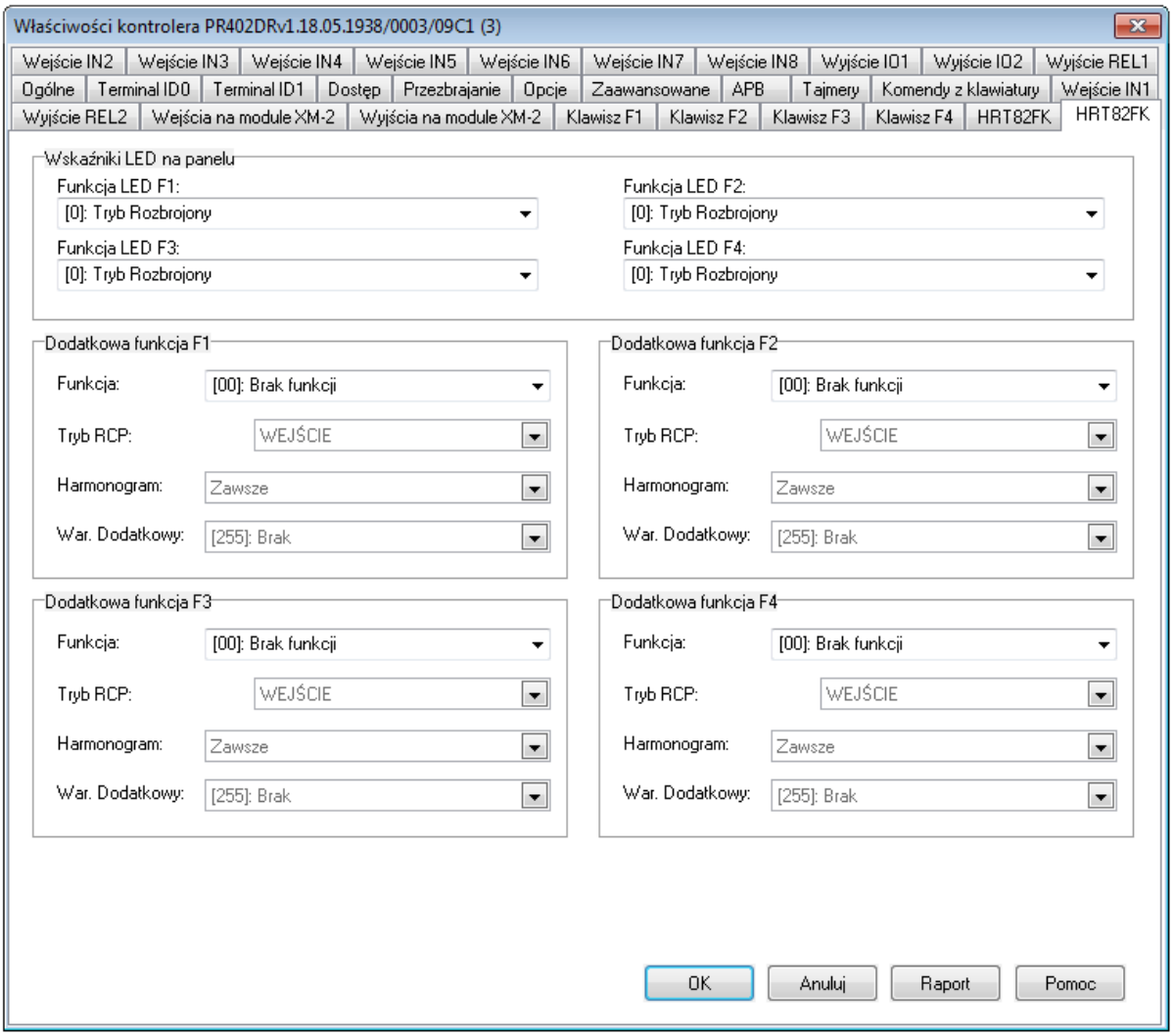
Rys. 27 Zakładka HRT82FK

Obszar: Panel HRT

Opcja: Załącz panel HRT82FK - gdy ta opcja jest załączona to możliwa jest obsługa panelu klawiszy funkcyjnych HRT82FK, w tym możliwość przypisywania funkcji podstawowych i dodatkowych. Więcej informacji na temat panelu HRT82FK podano w punkcie 3.2.7 Współpraca z panelem HRT82FK oraz w instrukcji panelu HRT82FK dostępnej na stronie www.roger.pl

Obszar: Podstawowa funkcja F1

Dostępne są cztery obszary konfiguracji odpowiadające poszczególnym klawiszom funkcyjnym panelu. Każdemu klawiszowi można przypisać funkcję podstawową (patrz 3.15 Klawisze funkcyjne), która jest aktywowana poprzez krótkie naciśnięcie klawisza jak też Harmonogram i Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są dwa harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym klawisz będzie mógł być używany. W przypadku wybrania harmonogramu Zawsze, klawisz będzie mógł być stosowany przez cały czas. Przypisany harmonogram nie załącza danego klawisza a jedynie odblokowuje możliwość jego załączania w danych przedziałach czasu. W przypadku funkcji związanych z Trybami RCP (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master) można wybrać Tryb RCP ustawiany przez dany klawisz funkcyjny.



Rys. 28 Zakładka HRT82FK

Obszar: Wskaźniki LED na panelu

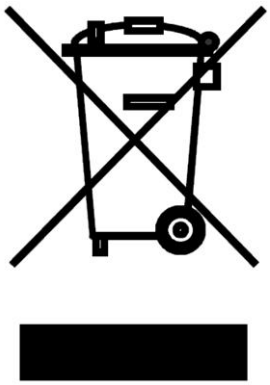
Każdemu skojarzonemu z klawiszem wskaźnikowi LED można przypisać funkcję z listy funkcji wyjściowych (patrz 3.14 Linie wyjściowe kontrolera). W praktyce wskaźnikom przypisuje się funkcje związane z funkcjami klawiszy po to by sygnalizować załączenie/wyłączenie klawisza.

Przykład:
Jeśli do klawisza F1 przypisana zostanie funkcja podstawowa [70]: Przełącz ŚWIATŁO a do wskaźnika LED klawisza F1 funkcja [64]: ŚWIATŁO to każde załączenie Flagi systemowej ŚWIATŁO za pomocą klawisza F1 będzie potwierdzane zapalaniem wskaźnika F1.

Obszar: Dodatkowa funkcja F1

Dostępne są cztery obszary konfiguracji odpowiadające poszczególnym klawiszom funkcyjnym panelu. Każdemu klawiszowi można przypisać funkcję dodatkową (patrz 3.15 Klawisze funkcyjne), która jest aktywowana poprzez dłuższe (domyślnie 3 sek.) naciśnięcie klawisza jak też Harmonogram i Warunek dodatkowy (patrz 3.16 Harmonogramy i Warunki dodatkowe). Dostępne są dwa harmonogramy wbudowane tj. Nigdy i Zawsze, jak również można przypisać własny Harmonogram Ogólnego Przeznaczenia, który definiuje się za pomocą opcji **Harmonogramy** w oknie głównym programu PR Master. Okres Od..Do tego harmonogramu wskazuje przedział czasowy, w którym klawisz będzie mógł być używany. W przypadku wybrania harmonogramu Zawsze, klawisz będzie mógł być stosowany przez cały czas. Przypisany harmonogram nie załącza danego klawisza a jedynie odblokowuje możliwość jego załączania w danych przedziałach czasu. W

przypadku funkcji związanych z Trybami RCP (patrz 3.19.2 Rejestracja czasu pracy w oparciu o program RCP Master) można wybrać Tryb RCP ustawiany przez dany klawisz funkcyjny.

	Symbol ten umieszczony na produkcie lub opakowaniu oznacza, że tego produktu nie należy wyrzucać razem z innymi odpadami gdyż może to spowodować negatywne skutki dla środowiska i zdrowia ludzi. Użytkownik jest odpowiedzialny za dostarczenie zużytego sprzętu do wyznaczonego punktu gromadzenia zużytych urządzeń elektrycznych i elektronicznych. Szczegółowe informacje na temat recyklingu można uzyskać u odpowiednich władz lokalnych, w przedsiębiorstwie zajmującym się usuwaniem odpadów lub w miejscu zakupu produktu. Gromadzenie osobno i recykling tego typu odpadów przyczynia się do ochrony zasobów naturalnych i jest bezpieczny dla zdrowia i środowiska naturalnego. Masa sprzętu podana jest w instrukcji.

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