Kontrolery Serii PRxx2
Opis Funkcjonalny

Wersja dokumentu: Rev. C

Oprogramowanie firmowe v2.0.3.1544

Oprogramowanie PR Master v4.3.3.500 i wyższe

Dokument ten odnosi się do urządzeń: PR302, PR402 i PR602LCD

roger

Terminy i 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 (skr. IACS – Integrated Access Control System)

System kontroli dostępu złożony z wielu kontrolerów połączonych ze sobą magistralą komunikacyjną która umożliwia monitorowanie systemu online a także realizację pewnych złożonych funkcji sterowania wymagających wymiany informacji pomiędzy urządzeniami podłączonymi do magistrali.

Roger Access Control System (RACS)

System kontroli dostępu składający się z kontrolerów dostępu serii PR (Roger) i zarządzanych przez program PR Master.

Centrala systemu KD

Specjalizowany kontroler pełniący pewne funkcje zarządzające w Zintegrowanym Systemie Kontroli Dostępu (IACS). Funkcja centrali KD zależy od tego z jakimi urządzeniami ono współpracuje. W odniesieniu do kontrolerów serii PRxx1 centrala (CPR32-SE) 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) lub komputer PC wraz z programem zarządzającym.

Interfejs Clock & Data

Interfejs elektryczny który umożliwia wymianę informacji za pośrednictwem sygnałów na liniach CLK i DTA. System RACS wykorzystuje własny protokół transmisji danych na liniach CLK/DTA, który dla odróżnienia od innych standardów Clock & Data jest oznaczany jako RACS Clock & Data lub w skrócie RACS. Standard RACS Clock & Data jest protokołem adresowalnym (adresy=0-15) i umożliwia transmisję danych w odległości do 150m przy wykorzystaniu dowolnych kabli sygnałowych.

Magistrala komunikacyjna

Struktura elektryczna złożona z dwóch przewodów elektrycznych która jest wykorzystywana do komunikacji pomiędzy różnymi urządzeniami do niej podłączonymi. System RACS wykorzystuje magistralę RS485.

Tryb Drzwi

Sposób sterowania elementem wykonawczym odpowiedzialnym za blokowanie/odblokowywanie drzwi. Kontroler PRxx2 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 elektrozaczep 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 Facility 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 (skr. IDENT)

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, w takim przypadku wszystkie te elementy są wymagane w celu pomyślnej identyfikacji, na przykład jeśli na kontrolerze obowiązuje tryb Karta i PIN to Identyfikator = Karta + PIN.

Logowanie

Proces identyfikacji użytkownika na podstawie jego identyfikatora.

Tryb Identyfikacji

Metoda jaką używa kontroler w celu identyfikacji użytkownika. Kontroler PRxx2 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 czas nieograniczony, tzn. do momentu, kiedy jakieś inne zdarzenie przywróci jej stan poprzedni.

Tryb monostabilny (chwilowy)

Tryb monostabilny odnosi się do sytuacji, kiedy jakiś element (np. linia wyjściowa) zmienia swój stan na pewien czas po upływie którego 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 PRxx2 za pośrednictwem linii CLK i 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 żadnym urządzeniem nadrzędnym lub jeśli takie połączenie istnieje lecz jest stosowane wyłącznie do celu programowania urządzenia lub ściągania zarejestrowanej w nim historii zdarzeń.

Flagi systemowe

Stany logiczne w pamięci kontrolera które reprezentują pewne określone zjawiska lub stany urządzenia.

Licznik (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.

Moduły rozszerzeń

Moduły elektroniczne dołączane do urządzenia w celu rozszerzenia jego możliwości i funkcjonalności.

Charakterystyka Ogólna

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. Jednocześnie z kontrolą dostępu kontrolery mogą dokonywać rejestracji zdarzeń dla celów rozliczania czasu pracy (RCP); najbardziej predestynowany do tego celu jest kontroler PR602LCD który jest wyposażony w wyświetlacz LCD oraz klawiaturę z programowalnymi klawiszami funkcyjnymi. Kontroler PRxx2 obsługuje logicznie dwa punkty identyfikacji (czytniki) zwane odpowiednio terminalem ID0 oraz terminalem ID1. Kontrolery PR302 oraz PR602LCD posiadają wbudowany czytnik który jest logicznie traktowany jako terminal ID1 natomiast kontroler PR402 wymaga czytników zewnętrznych. Zasadniczo kontrolery PRxx2 zostały zaprojektowane do współpracy z czytnikami serii PRT (Roger) niemniej mogą one również współpracować z czytnikami pracującymi w standardzie Wiegand oraz Magstripe. W kontrolerze PRxx2 można zarejestrować do 4000 użytkowników, każdy z użytkowników możne posiadać kartę oraz kod PIN. Oprogramowanie firmowe (firmware) kontrolerów może być aktualizowane po instalacji z poziomu komputera (fleszowanie). Kontroler serii PRxx2 może działać całkowicie samodzielnie (Trybie Autonomiczny) 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 ale służą one do sterowania jego pracą a nie do programowania. Przesyłanie ustawień do kontrolerów odbywa się metodą transakcyjną co oznacza że w przypadku nieudanej próby programowania kontroler przywraca poprzednie ustawienia i można wtedy ponownie podjąć próbę jego programowania, cecha ta jest szczególnie istotna gdy kontroler (system) jest rozproszony terytorialnie i zarządzany zdalnie przez sieć komputerową. Komunikacja z kontrolerami (systemem) wymaga zastosowania odpowiedniego interfejsu komunikacyjnego (np. UT-2, UT-2USB lub UT-4).

Tabela nr 1: Zestawienie kontrolerów serii PRxx2 (stan na 12/2007)

Kontroler	**PR402**	**PR302**	**PR602LCD**
Zasilanie	18-22VAC, 24VDC, 12VDC	10-15VDC	10-15VDC
Wejścia NO/NC	4	3	3
Wyjścia przekaźnikowe	2	1	1
Wyjścia tranzystorowe	2	2	2
Wbudowany czytnik	Brak	Tak	Tak
Zewnętrzny czytnik	2	1	1
Klawiatura	Nie	Tak	Tak
Klawisze funkcyjne	Nie	Nie	4 klawisze funkcyjne F1-F4
Inne	Wbudowany zasilacz impulsowy 1.5A z możliwością dołączenia akumulatora	Możliwość przezbrojenia kontrolera do wersji bez klawiatury	Wyświetlacz LCD, praca w warunkach zewnętrznych

Skrócona charakterystyka

- Obustronna kontrola dostępu dla jednego przejścia
- Kontrola dostępu w windach (maks. 32 piętra, wymaga modułów XM-8)
- Współpraca z czytnikami serii PRT (Roger)
- Współpraca z czytnikami Magstripe oraz Wiegand
- Praca autonomiczna lub w zintegrowanym systemie sieciowym
- Identyfikacja za pomocą karty i/lub kodu PIN
- Nieulotny bufor 32.000 zdarzeń
- 4000 użytkowników
- 250 grup dostępu
- 500 stref dostępu
- 99 harmonogramów czasowych ogólnego przeznaczenia
- 128 okresów czasowych w ramach pojedynczego harmonogramu
- 4 harmonogramy specjalne (H1-H4)
- Ustawienia świąteczne (maks. 120 dni)
- Zegar czasu rzeczywistego z podtrzymaniem bateryjnym
- Programowalne linie wejściowe i wyjściowe
- Definiowanie przedziału czasowego ważności użytkownika
- Definiowanie maksymalnej krotności logowania danego użytkownika
- 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 CPR)
- Rejestracja zdarzeń dla celów RCP
- Możliwość definiowania własnych trybów RCP
- Automatyczne i ręczne sterowanie trybem RCP
- Integracja z systemem alarmowym za pośrednictwem linii we/wy
- Współpraca z modułem we/wy XM-2
- Współpraca z modułem dozoru zasilania PSAM-1
- Możliwość aktualizacji oprogramowania (fleszowanie)
- Interfejs komunikacyjny RS485
- Oprogramowanie zarządzające (Windows XP/Vista)
- Transakcyjna metoda przesyłania ustawień
- Zgodność ze standardem EN 50133-4
- Znak CE

Opis Funkcjonalny

Praca w Sieciowym Systemie Kontroli Dostępu

Kiedy system kontroli dostępu posiada magistralę komunikacyjną i jest ona wykorzystywana do wymiany danych pomiędzy urządzeniami (kontrolerami) do niej podłączonymi to taki system nosi nazwę *Sieciowego Systemu Kontroli Dostępu* oznaczanego skrótowo IACS (ang. *IACS - Integrated Access Control System*). W systemie RACS warunkiem koniecznym systemu sieciowego jest obecność w nim centrali CPR32-SE. W przypadku kontrolerów serii PRxx2 uszkodzenie magistrali systemu powoduje częściową utratę funkcjonalności systemu, w szczególności przestają działać funkcje o charakterze globalnym (Strefy Alarmowe i Strefy Anti-passback).

Uwaga: Samo istnienie magistrali komunikacyjnej w systemie KD nie rozstrzyga tego czy jest on systemem sieciowym czy nie. Jeśli uszkodzenie lub brak magistrali komunikacyjnej nie powoduje zaniku żadnych funkcji systemu to taki system nie jest systemem sieciowym. Dla przykładu jeśli w systemie istnieje magistrala komunikacyjna lecz jest ona używana tylko w celu programowania kontrolerów i ściągania zdarzeń to system taki nie jest systemem sieciowym lecz autonomicznym z sztywnym łączem komunikacyjnym do komputera zarządzającego.

Obecność centrali CPR w Zintegrowanym Systemie Kontroli Dostępu

W odniesieniu do kontrolerów serii PRxx2 obecność centrali CPR32-SE udostępnia następujące funkcje:

- ciągłe ściąganie zdarzeń z wewnętrznych buforów pamięci kontrolerów PRxx2 i zapisywanie ich w centralnym buforze zlokalizowanym w centrali CPR
- możliwość definiowania Stref APB (Strefy Anti-passback)
- możliwość definiowania Stref Alarmowych

Uwaga: W systemie RACS 4 zarówno definiowanie Stref APB jak i Stref Alarmowych jest możliwe jedynie w ramach tego samego Podsystemu KD.

Praca w Trybie Autonomicznym

W trybie autonomicznym kontroler działa samodzielnie, nie wymienia informacji z innymi urządzeniami wchodzącymi w skład systemu. W trybie autonomicznym nie są dostępne żadne funkcje o charakterze globalnym (Strefy APB, Strefy Alarmowe) ani ściąganie zdarzeń do centralnego bufora 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 ściągania zdarzeń. W przypadku gdy w systemie są zainstalowane dwa lub więcej kontrolery serii PRxx2 to kontroler o najniższym adresie synchronizuje zegary na wszystkich innych kontrolerach podłączonych do tej samej magistrali komunikacyjnej, dzięki tej funkcji nawet po długim okresie czasu zegary wszystkich kontrolerów wskazują tę samą godzinę a zarejestrowane zdarzenia zachowują chronologię.

Uwaga: Ze względu na to że kontroler PRxx2 nie może być programowany manualnie przed przekazaniem go do użytkowania należy go podłączyć do komputera i odpowiednio skonfigurować. Podłączenie do komputera może być tymczasowe lub stałe i wymaga zastosowania odpowiedniego interfejsu komunikacyjnego (np. UT-2, UT-2USB lub UT-4). Nowy fabrycznie kontroler posiada adres ID=0, o ile zachodzi taka potrzeba to adres ten można zmienić manualnie w czasie procedury Resetu Pamięci lub z poziomu programu zarządzającego.

Komunikacja

Interfejs RS485

Kontroler PRxx2 jest wyposażony w interfejs komunikacyjny pracujący w standardzie RS485. Interfejs ten może być wykorzystywany do dwóch celów: do programowania kontrolera oraz do komunikacji z kontrolerem wtedy gdy jest on elementem zintegrowanego systemu KD. 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 centralę CPR (opcja). Topologia magistrali RS485 w systemie RACS może być kształtowana bardzo elastycznie, dopuszczalne są struktury typu „drzewo", „gwiazda" a także ich kombinacje, nie dopuszcza się jednak stosowania topologii typu „pętla". Magistrala komunikacyjna może być zrealizowana przy użyciu dowolnego typu kabli sygnałowych, niemniej zaleca się używanie skrętki komputerowej bez ekranu. W systemie RACS nie ma konieczności stosowania rezystorów terminujących na końcach magistrali komunikacyjnej.

Maksymalne odległości liczone po kablu w systemie RACS:

- pomiędzy dowolnym kontrolerem a centralą CPR: 1200m
- pomiędzy dowolnym kontrolerem a interfejsem komunikacyjnym: 1200m
- pomiędzy centralą CPR a interfejsem komunikacyjnym: 1200m

Uwaga: Wszystkie urządzenia podłączone do magistrali komunikacyjnej RS485 powinny mieć wspólną masę. Warunek ten jest automatycznie spełniony gdy wszystkie urządzenia są zasilane z tego samego źródła zasilania prądu stałego (z jednego zasilacza). W przypadku gdy zasilanie jest realizowane z wielu źródeł to minusy wszystkich zasilaczy należy połączyć ze sobą używając do tego celu osobnego przewodu a jeśli jest to niemożliwe, minusy poszczególnych zasilaczy należy uziemić przy czym konieczne jest aby różnica potencjałów uziemienia w różnych punktach instalacji nie była większa niż +/-2V.

Struktura złożona z magistrali komunikacyjnej, kontrolerów dostępu (maks. 32) oraz opcjonalnie występującej centrali CPR nosi nazwę *podsystemu kontroli dostępu* lub krótko *podsystemu*. Każdy podsystem w systemie RACS jest podłączony do komputera za pośrednictwem osobnego portu komunikacyjnego. Port komunikacyjny może mieć charakter rzeczywisty (COM) lub wirtualny (Virtual Com Port - VSP). W tym ostatnim przypadku komunikacja z podsystemem KD może odbywać się za pośrednictwem interfejsów które emulują port szeregowy w komputerze np. UT-2USB (USB) lub UT-4 (Ethernet).

Uwaga: Interfejsy komunikacyjne można stosować jedynie na czas programowania kontrolera bądź też mogą być podłączone na stałe i służyć do zarządzania systemem KD.

Każdy kontroler serii PRxx2 może zarządzać pojedynczym przejściem kontrolowanym jedno lub dwustronnie. W chwili obecnej, w ramach jednego systemu RACS 4 można zintegrować do 100 podsystemów, w każdym do 32 kontrolerów. 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.

Interfejs RACS Clock & Data

Oprócz interfejsu RS 485 kontroler PRxx2 jest wyposażony w interfejs RACS Clock & Data. Interfejs ten jest przeznaczony do komunikacji z zewnętrznymi czytnikami oraz modułami rozszerzeń i składa się z dwóch linii: CLK i DTA. Do linii CLK/DTA można dołączyć następujące urządzenia zewnętrzne:

- podstawowy czytnik dostępu (Terminal ID0) po stronie wejścia
- podstawowy czytnik dostępu (Terminal ID1) po stronie wyjścia
- dodatkowy czytniki dostępu po stronie wejścia (dla trybu High Security)
- dodatkowy czytniki dostępu po stronie wyjścia (dla trybu High Security)

- moduł we/wy XM-2 (separacja linii we/wy)
- moduł we/wy XM-8 (kontrolera dostępu w windzie)
- moduł PSAM-1 (dozór zasilaczy serii PS10/PS20)

Uwaga: Pod pojęciem czytnika High Security rozumie się dowolny typ czytnika (np. czytnik zbliżeniowy, PIN, biometryczny etc.) który jest używany jako dodatkowa (druga) metoda identyfikacji użytkownika. W przypadku gdy jest załączony tryb High Security, użytkownik musi najpierw dokonać identyfikacji na czytniku podstawowym a następnie na czytniku dodatkowym, dopiero po pomyślnej identyfikacji na każdym z tych czytników kontroler może przyznać dostęp lub wykonać inną akcję wynikającą z jego logiki działania.

Dane przesyłane z czytnika do kontrolera mogą być interpretowane na wiele różnych sposobów. Niektóre typy czytników (np. czytniki serii PRT) wskazują na typ danych które transmitują (tzn. czy jest to karta czy PIN). Dodatkowo, spotyka się wiele różnych wariantów kodowania transmisji np. z /bez bitów kontrolnych, w postaci szesnastkowej (HEX) lub binarnej (BIN) itp. Na etapie konfiguracji kontrolera instalator powinien zapoznać się z dokumentacją techniczną stosowanych czytników i odpowiednio skonfigurować kontroler tak aby mógł on poprawnie rozpoznawać dane transmitowane z czytników.

Zasadniczo każde urządzenie podłączane do linii CLK/DTA musi posiadać swój niepowtarzalny adres (numer ID) zawierający się w zakresie 0-15. Zasada ta jednak nie dotyczy czytników pracujących w standardzie Wiegand lub Magstripe. Czytniki tego typu nie są adresowalne a ich podłączenie do kontrolera jest uwarunkowane dodatkowymi regułami.

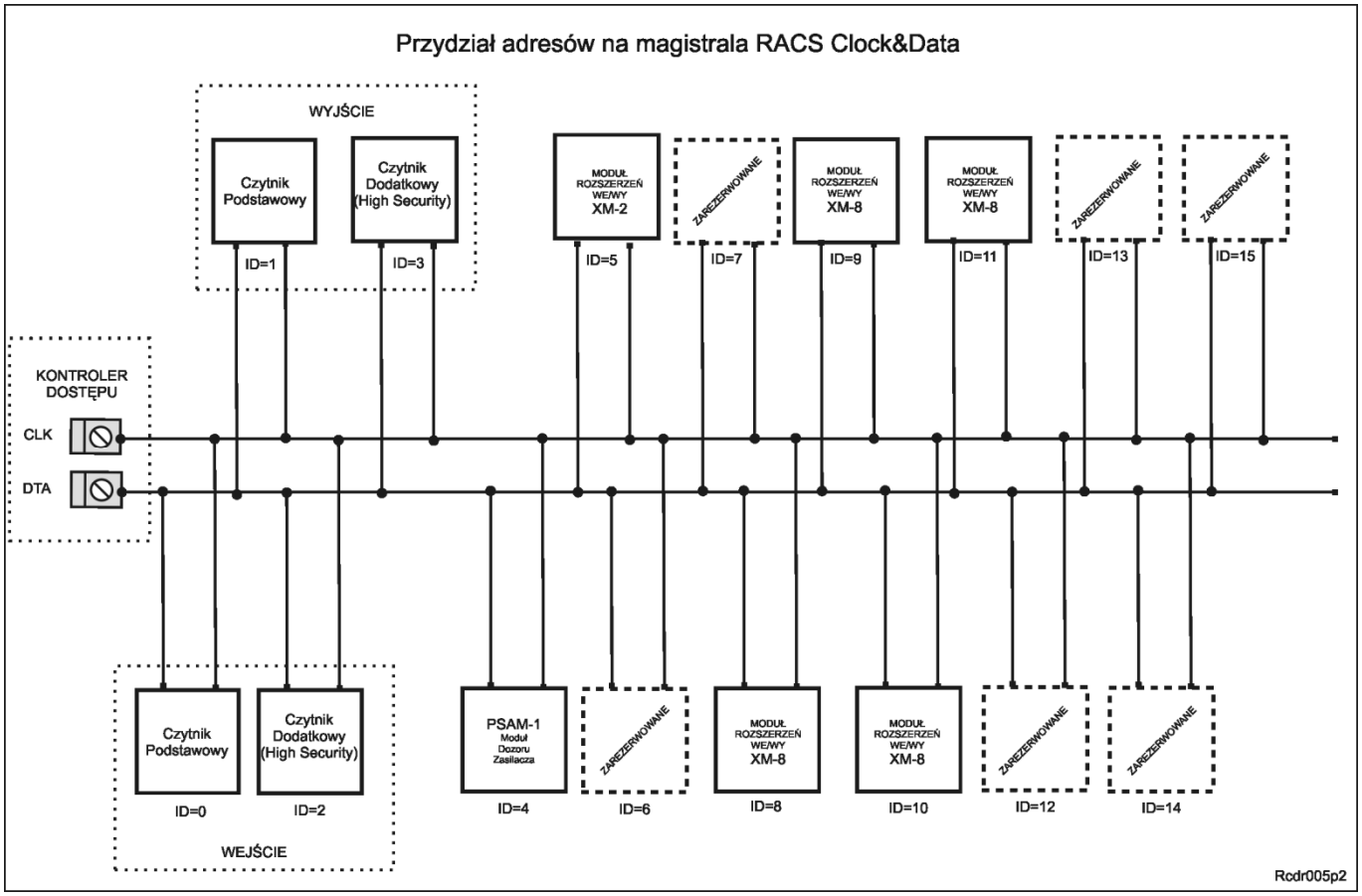
Maksymalna odległość pomiędzy kontrolerem a dowolnym urządzeniem podłączonym do magistrali Clock & Data nie może przekraczać 150m. Struktura oraz rodzaje kabli stosowane dla tej magistrali są całkowicie dowolne, jedynym warunkiem stawianym kablom jest to aby ich całkowita rezystancja mierzona pomiędzy kontrolerem a dołączonym urządzeniem nie była większa niż 50Ω. Wszystkie urządzenia podłączone do linii CLK/DTA powinny mieć wspólny minus zasilania.

Zasady dołączania urządzeń do linii CLK/DTA:

- czytniki podstawowe po stronie wejścia oraz wyjścia muszą pracować w tym samym formacie danych (tzn. RACS Clock & Data, Wiegand lub Magstripe)
- czytniki dodatkowe dla trybu High Security po stronie wejścia oraz wyjścia muszą pracować w tym samym formacie danych (tzn. RACS Clock & Data, Wiegand, Magstripe)
- czytniki dodatkowe dla trybu High Security mogą pracować w innym formacie niż czytniki podstawowe
- w przypadku gdy rolę czytników podstawowych pełnią czytniki z interfejsem Wiegand lub Magstripe to do linii CLK/DTA nie można już dołączyć modułu XM-2 ani PSAM-1, można jednak dołączyć moduły XM-8 i czytniki dodatkowe dla trybu High Security pracujące w tym samym lub innym standardzie komunikacji co czytniki podstawowe
- w przypadku gdy do kontrolera PR402 mają być podłączone dwa czytniki typu Wiegand lub Magstripe to wymagane jest zastosowanie dodatkowej diody półprzewodnikowej lub adaptera PR-GP, który umożliwi rozróżnienie z którego z dwóch czytników pochodzi transmisja (szczegóły podłączeń czytników Wiegand/Magstripe do kontrolerów PRxx2 zostały przedstawione szczegółowo w instrukcji instalacji dla tych kontrolerów)

Jak wynika z przytoczonych zasad w przypadku gdy rolę czytników podstawowych pełnią czytniki pracujące w standardzie Wiegand lub Magstripe to kontroler nie może wtedy obsługiwać modułów rozszerzeń XM-2 i PSAM-1, może jednak nadal współpracować z czytnikami dodatkowymi dla trybu High Security, bez względu na to w jakim standardzie one funkcjonują, może również współpracować z modułami XM-8 (do obsługi wind).

Tabela nr 2: Przydział adresów w interfejsie RACS Clock & Data		
Adres	**Czytnik/moduł**	**Uwagi**
ID=0	Pierwszy czytnik podstawowy	Czytnik podstawowy po stronie wyjścia
ID=1	Drugi czytnik podstawowy	Czytnik podstawowy po stronie wejścia
ID=2	Pierwszy czytnik dodatkowy	Czytnik dodatkowy po stronie wyjścia (dla trybu High Security)
ID=3	Drugi czytnik dodatkowy	Czytnik dodatkowy po stronie wejścia (dla trybu High Security)
ID=4	Moduł dozoru zasilania typu PSAM-1	Moduł dozoru stanu zasilania (moduł może współpracować z zasilaczami PS10/PS20/PS15v24)
ID=5	Moduł rozszerzeń we/wy typu XM-2	Moduł rozszerzeń we/wy z dwoma linami wejściowymi typu NO/NC oraz dwoma wyjściami przekaźnikowymi
ID=6	Zarezerwowane	
ID=7	Zarezerwowane	
ID=8	Pierwszy moduł rozszerzeń we/wy typu XM-8	Moduł rozszerzeń we/wy zawierający 8 wejść NO/NC oraz 8 wyjść przekaźnikowych (REL1-REL8)
ID=9	Drugi moduł rozszerzeń we/wy typu XM-8	Moduł rozszerzeń we/wy zawierający 8 wejść NO/NC oraz 8 wyjść przekaźnikowych (REL1-REL8)
ID=10	Trzeci moduł rozszerzeń we/wy typu XM-8	Moduł rozszerzeń we/wy zawierający 8 wejść NO/NC oraz 8 wyjść przekaźnikowych (REL1-REL8)
ID=11	Czwarty moduł rozszerzeń we/wy typu XM-8	Moduł rozszerzeń we/wy zawierający 8 wejść NO/NC oraz 8 wyjść przekaźnikowych (REL1-REL8)
ID=12	Zarezerwowane	
ID=13	Zarezerwowane	
ID=14	Zarezerwowane	
ID=15	Zarezerwowane	
Uwaga: Opisany w tabeli przydział adresów dotyczy urządzeń (czytników i modułów) które pracują w standardzie RACS Clock & Data i nie stosuje się do czytników standardu Wiegand lub Magstripe.		



Współpraca z modułami XM-8

Moduł XM-8 opracowano jako uniwersalny moduł we/wy niemniej w chwili obecnej możliwość jego wykorzystania jest ograniczona do sytuacji gdy będzie on sterował dostępem w windach lub w innych, podobnych sytuacjach gdzie po identyfikacji użytkownika kontroler ma za zadanie załączyć pewien (uprzednio) zdefiniowany zestaw linii wyjściowych. Wykorzystanie modułów XM-8 do kontroli dostępu w windach polega na tym że każde z wyjść modułu blokuje/odblokowuje klawisz wyboru odpowiadającego mu piętra.

Kontroler PRxx2 może współpracować maksymalnie z czterema modułami rozszerzeń XM-8. Pierwszy moduł XM-8 (o adresie ID=8) kontroluje dostęp do pięter 1-8, drugi (o adresie 9) kontroluje dostęp do pięter 9-16, trzeci (o adresie 10) kontroluje dostęp do pięter 17-24, czwarty (o adresie 11) obsługuje piętra 25-32. Kiedy kontroler przydziela dostęp określonemu użytkownikowi, rozpoznaje najpierw do jakiej Grupy Dostępu on należy a następnie uaktywnia odpowiedni zestaw wyjść na modułach XM-8 które odblokowują tylko te klawisze wyboru pięter do których użytkownicy danej grupy mają prawo dostępu. Po dokonaniu wyboru piętra, wyjścia modułu XM-8 powinny zostać wyzerowane tak aby uniemożliwić osobom postronnym poruszanie się przy użyciu windy w dozorowanym obiekcie. Zerowanie wyjść modułu XM-8 można zrealizować za pośrednictwem dowolnej linii wejściowej kontrolera skonfigurowanej do funkcji **[63]: Kasuj wyjścia na modułach XM-8**. Wyzwolenie tak skonfigurowanego wejścia powoduje natychmiastowe wyłączenie wszystkich wyjść na wszystkich modułach XM-8 podłączonych do kontrolera i tym samym zablokowanie wszystkich klawiszy wyboru piętra. Sygnał zerujący wyjścia modułów XM-8 można pobrać z układu sterowania windą (np. w chwili uruchomienia napędu windy zostanie podany sygnał zerujący wyjścia modułu XM-8) lub zrealizować metodą czasową tzn. wyzerowanie wyjść nastąpi automatycznie po określonym czasie od momentu identyfikacji użytkownika i przyznania mu dostępu. W tym drugim przypadku do kasowania wyjść modułów XM-8 można użyć wyjścia **[99]: Zamek drzwi**. Wyjście to należy podłączyć do linii zerującej wyjścia na modułach XM-8, przy czym należy tak dobrać polaryzację linii wejściowej (NO lub NC) aby zerowanie następowało dopiero w chwili wyłączenia wyjścia **[99]: Zamek drzwi**. Czas wyzwolenia wyjścia **[99]** może być regulowany w zakresie od 1s

do 99 minut lecz z praktycznego punktu widzenia powinien być ustawiany na wartość kilku sekund tak aby użytkownik mógł swobodnie wybrać przycisk piętra na które chce się udać.

W celu uruchomienia obsługi kontroli dostępu w windzie do kontrolera należy dołączyć po jednym module XM-8 na każde osiem pięter podlegających kontroli i w programie zarządzającym wskazać którą z czterech możliwych wind będzie dany kontroler obsługiwał, ustawienia tego dokonuje się w polu **Kontroler obsługuje windę numer:...** (zakładka Właściwości kontrolera/Opcje…)

Współpraca z modułem XM-2
Kontroler PRxx2 może współpracować z jednym modułem we/wy typu XM-2 o adresie ID=5. Zastosowanie tego modułu nie zwiększa ogólnej ilości linii we/wy lecz umożliwia jedynie ich fizyczną separację od kontrolera. Potrzeba separacji linii we/wy od kontrolera zachodzi głównie w odniesieniu do kontrolerów z wbudowanymi czytnikami (np. PR302, PR602LCD) które w przypadku instalacji w miejscach ogólnodostępnych są narażone na ingerencję osób postronnych do ich wnętrza. W wyniku tego zagrożenia osoby te mogą zyskać dostęp do linii kontrolera, a w szczególności do przekaźnika odblokowującego drzwi i/lub sterującego systemem alarmowym, mogą też skutecznie blokować działanie czujnika otwarcia drzwi. Zastosowanie modułu XM-2 uniemożliwia obejście linii IN1/IN2 i REL1/REL2 przez wykonanie prostych połączeń elektrycznych wewnątrz kontrolera gdyż komunikacja pomiędzy kontrolerem a modułem XM-2 odbywa się na drodze cyfrowej.

Moduł XM-2 posiada dwa wyjścia przekaźnikowe (REL1 i REL2) oraz dwa wejścia typu NO/NC (IN1 i IN2). Jak już wcześniej wspomniano wejścia i wyjścia na module XM-2 nie mogą być wykorzystane jako dodatkowe niezależne oprogramowane linie we/wy kontrolera lecz jedynie jako linie dublujące funkcje odpowiadających im wewnętrznych linii kontrolera, obowiązują przy tym następujące zasady:

- Załączenie obsługi modułu XM-2 powoduje że wyjście REL1 na module XM-2 przyjmuje funkcję zaprogramowaną dla wyjścia REL1 na kontrolerze i jest z nim współbieżnie sterowane
- Załączenie obsługi modułu XM-2 powoduje że wyjście REL2 na module XM-2 przyjmuje funkcję zaprogramowaną dla wyjścia REL2 na kontrolerze i jest z nim współbieżnie sterowane (wyjście REL2 jest dostępne tylko na kontrolerze PR402)
- Załączenie obsługi wejścia IN1 na module XM-2 wyłącza obsługę linii IN1 na kontrolerze przy czym wejście IN1 na module przejmuje funkcję zaprogramowaną dla wejścia IN1 na kontrolerze
- Załączenie obsługi wejścia IN2 na module XM-2 wyłącza obsługę linii IN2 na kontrolerze przy czym wejście IN2 na module przejmuje funkcję zaprogramowaną dla wejścia IN2 na kontrolerze

Z modułem rozszerzeń XM-2 są związane następujące opcje:

Opcja: Załącz obsługę modułu XM-2
PRMaster:/Właściwości kontrolera/Opcje/Moduły rozszerzeń/Załącz obsługę modułu XM-2

Zaznaczenie tej opcji powoduje że wyjścia REL1 i REL2 na module XM-2 będą sterowane współbieżnie z wyjściami REL1 i REL2 na kontrolerze.

Opcja: Załącz IN1 na XM-2, wyłącz IN1 w kontrolerze
PRMaster:/Właściwości kontrolera/Opcje/Moduły rozszerzeń/Załącz obsługę modułu XM-2/Załącz IN1 na XM-2, wyłącz IN1 w kontrolerze

Zaznaczenie tej opcji powoduje, że kontroler będzie wykorzystywał wejście IN1 znajdujące się na module XM-2 zamiast lokalnego wejścia IN1 znajdującego się na płytce kontrolera. Do zewnętrznego wejścia IN1 będzie przypisana ta sama funkcja jaka została zdefiniowana pierwotnie dla wejścia IN1 znajdującego się na kontrolerze. Po załączeniu tej opcji sygnały elektryczne na wejściu IN1 kontrolera będą ignorowane.

Opcja: Załącz IN2 na XM-2, wyłącz IN2 w kontrolerze
PRMaster:/Właściwości kontrolera/Opcje/Moduły rozszerzeń/Załącz obsługę modułu XM-2/Załącz IN2 na XM-2, wyłącz IN2 w kontrolerze

Zaznaczenie tej opcji powoduje, że kontroler będzie wykorzystywał wejście IN2 znajdujące się na module XM-2 zamiast lokalnego wejścia IN2 znajdującego się na płytce kontrolera. Do zewnętrznego wejścia IN2 będzie przypisana ta sama funkcja jaka została zdefiniowana pierwotnie dla wejścia IN2 znajdującego się na kontrolerze. Po załączeniu tej opcji sygnały elektryczne na wejściu IN2 kontrolera będą ignorowane.

Współpraca z modułem PSAM-1
Kontroler PRxx2 może współpracować z jednym, adresowalnym modułem dozoru zasilania typu PSAM-1 o adresie ID=4 który jest opcjonalnym wyposażeniem zasilaczy PS10, PS20 i PS15v24 (Roger). 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 linii CLK/DTA do urządzenia nadrzędnego (kontroler). Moduł PSAM-1 umożliwia dozorowanie następujących stanów:

- Niski poziomu baterii rezerwowej
- Awaria baterii rezerwowej
- Brak napięcia sieci AC
- Aktualny stan napięcia na wyjściu zasilacza (tylko w trybie sieciowym)

Współpracę z modułem dozoru zasilacza PSAM-1 uaktywnia się za pomocą **opcji: Załącz obsługę modułu dozoru zasilania typu PSAM-1**

PRMaster:/Właściwości kontrolera/Opcje/Moduły rozszerzeń/Załącz obsługę modułu dozoru zasilania typu PSAM-1

Uwaga: Kontroler PR402 nie obsługuje modułu PSAM-1 gdyż posiada dozorowany wewnętrzny zasilacz impulsowy.

Współpraca z czytnikami Wiegand i Magstripe
Zasadniczo kontroler PRxx2 został zaprojektowany do współpracy z czytnikami dostępu serii PRT pracującymi na adresowalnej magistrali RACS Clock & Data, niemniej może on również, pod pewnymi warunkami, współpracować z czytnikami typu Magstripe i Wiegand. Czytniki tego typu mogą być stosowane w miejsce podstawowych czytników dostępu umieszczonych na wejściu i wyjściu z pomieszczenia lub w miejsce czytników dodatkowych wtedy gdy na kontrolerze wykorzystywany jest tryb High Security. Zarówno czytniki Wiegand jak i Magstripe dołącza się do tych samych linii CLK/DTA co czytniki serii PRT istnieją jednak pewne reguły postępowania wymienione poniżej:

- Większość czytników standardu Wiegand/Magstripe może być bezpośrednio (bez żadnych modułów pośredniczących) dołączona dla linii CLK/DTA
- W pewnych przypadkach gdy poziomy elektryczne sygnałów kontrolera i czytnika nie są kompatybilne należy pomiędzy kontroler i czytnik włączyć interfejs PR-GP (Roger)
- Gdy do kontrolera dołącza się dwa czytniki Wiegand/Magstripe trzeba dodatkowo zainstalować diodę półprzewodnikową która umożliwi rozpoznanie z którego czytnika nadchodzi transmisja (szczegóły podłączeń w instrukcji instalacji kontrolerów)

Aby kontroler mógł prawidłowo współpracować z czytnikiem należy w programie zarządzającym poprawnie wskazać 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. Kontroler PRxx2 akceptuje następujące standardy elektryczne:

- Wiegand
- Magstripe (ABA Track II Emulation)
- RACS Clock & Data (Roger)

Wysoki poziom logiczny sygnałów na liniach CLK/DTA może zawierać się w przedziale 4…15V, natomiast poziom niski jest reprezentowany przez napięcie w przedziale 0…2V. Wszystkie urządzenia podłączone do linii CLK/DTA (w tym czytniki dostępu) powinny mieć wspólny minus zasilania. Kontroler obsługuje 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

Współpraca z czytnikami biometrycznymi

Czytniki tego typu identyfikują użytkownika na podstawie jakiejś jego cechy biologicznej, może to być na przykład odcisk palca, źrenica oka, owal twarzy, kształt dłoni i inne. W zasadzie każdy czytnik biometryczny który jest wyposażony w interfejs komunikacyjny Wiegand lub Magstripe może być dołączony do kontrolera jako podstawowy lub dodatkowy czytnik dostępu. Podobnie jak inne czytniki dostępu, czytnik biometryczny w momencie identyfikacji użytkownika wysyła ciąg cyfr. Sposób interpretacji ich leży całkowicie po stronie kontrolera. Z reguły każdy czytnik biometryczny posiada jakąś metodę programowania, ręczną lub z poziomu komputera, która umożliwia przypisanie każdemu użytkownikowi zarejestrowanemu w czytniku określonego ciągu liczbowego. Ciąg ten może być taki sam jak kod karty lub kod PIN przypisany danemu użytkownikowi w systemie KD lub może wskazywać bezpośrednio na jego numer ID. Za każdym razem gdy kontroler odbierze dane z czytnika biometrycznego dokonuje ich interpretacji tzn. ustala od jakiego użytkownika one pochodzą i na tej podstawie podejmuje dalsze działania (tzn. może przyznać dostęp lub podjąć inną akcję wynikająca z logiki działania).

Z reguły integracja czytników biometrycznych w systemie RACS wymaga stosowania dwóch rodzajów oprogramowania; jednego do obsługi systemu KD oraz drugiego do obsługi czytnika biometrycznego. Istnienie takiej dwoistości jest pewnym utrudnieniem dla administratora systemu KD gdyż wymaga od niego zarządzania dwoma listami użytkowników oraz ich wzajemnej synchronizacji. Problem administracji obydwoma listami użytkowników jest znacznie ograniczony w

przypadku użycia czytników linii papilarnych typu F7 i F10 (dystrybucja Roger) których obsługa została zarówno sprzętowo jak i programowo wbudowana w system RACS.

Współpraca z czytnikami linii papilarnych typu F7 i F10
Integracja czytnika F7 i F10 w systemie RACS została zrealizowana przy następujących założeniach:

- W momencie identyfikacji czytnik wysyła ciąg bitów który wskazuje na numer ID użytkownika który właśnie dokonał identyfikacji
- Czytnik wysyła dane w formacie Wiegand
- Czytnik jest podłączony do kontrolera za pośrednictwem linii CLK/DTA
- Czytnik jest na stałe podłączony do magistrali komunikacyjnej systemu RACS (RS485) lub do sieci komputerowej Ethernet

W rezultacie zastosowania tej metody integracji, konfigurowanie kontrolerów dostępu oraz czytnika(ów) biometrycznych jest realizowane z poziomu tego samego oprogramowania zarządzającego systemem KD (PR Master) oraz przy użyciu wspólnej magistrali komunikacyjnej (RS485) lub alternatywnie za pośrednictwem sieci komputerowej. Każda zmiana na liście użytkowników systemu jest współbieżnie uaktualniana zarówno na kontrolerach dostępu jak i na czytnikach biometrycznych. Dodatkowo, program PR Master ułatwia rejestrowanie odcisków palców oraz organizuje ich przechowywanie w bazie danych systemu RACS.

Użytkownicy

W kontrolerze 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 formatu RACS Clock & Data wprowadzanie kodu PIN zawsze należy zakończyć klawiszem [#] który oznacza koniec kodu PIN. 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 kontrolera 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. Każda klasa użytkowników charakteryzuje się innymi uprawnieniami w zakresie funkcji programowania oraz przezbrajania kontrolera.

Tabela nr 3: Typy użytkowników

Nazwa	Numer ID	Opis
MASTER	000	Uprawnienie do otwierania drzwi oraz przezbrajania, użytkownik ten może być zdefiniowany w trakcie Resetu Pamięci lub z poziomu programu PR Master. Zdefiniowanie użytkownika MASTER umożliwia wstępne przetestowanie kontrolera. Przy pomocy identyfikatora MASTER instalator może natychmiast sprawdzić poprawność sterowania elementem wykonawczym i ewentualnie przezbroić kontroler przy czym w celu przezbrojenia kontrolera należy dwukrotnie użyć karty Master lub jego PIN-kodu. Użytkownik MASTER jest użytkownikiem „bez grupy", oznacza to że zawsze bez względu na aktualnie obowiązujące harmonogramy dostępu kontroler może przyznać mu prawo dostępu (o ile inne opcje nie będą tego blokowały).
SWITCHER Full	ID=001-049	Uprawniony do otwierania drzwi oraz do przezbrajania kontrolera. Przezbrojenie kontrolera wymaga dwukrotnego użycia identyfikatora SWITCHER natomiast przyznanie dostępu następuje z chwilą pierwszego użycia tego identyfikatora.

SWITCHER Limited	ID=050-999	Uprawnienie tylko do przezbrajania kontrolera, przezbrojenie następuje w następstwie jednokrotnego użycia identyfikatora
NORMAL	ID=1000-3999	Uprawnienie tylko do otwierania drzwi. Użytkownicy typu NORMAL o numerze ID większym niż 1000 mogą posiadać dodatkowo atrybut Local SWITCHER który uprawnia ich również do przezbrajania kontrolera. Tak jak w przypadku użytkowników SWITCHER Full przezbrojenie kontrolera przez użytkowników NORMAL posiadających atrybut Local SWITCHER wymaga dwukrotnego użycia identyfikatora. W odróżnieniu od pozostałych klas użytkowników atrybut Local SWICTHER przydziela się indywidualnie każdemu użytkownikowi na każdym kontrolerze osobno.

W kontrolerach PRxx2 identyfikacja użytkowników jest realizowana za pośrednictwem przypisanych im identyfikatorów. Rolę identyfikatora użytkownika może spełniać kod PIN, karta lub jego numer ID.

Uwaga: Zapis IDENT jest rozumiany jako operacja wprowadzenia ważnego identyfikatora. Forma identyfikatora zależy od aktualnie obowiązującego na czytniku trybu identyfikacji. W kontrolerach PRxx2 tryb identyfikacji definiuje się indywidualnie dla każdej strony przejścia.

Przykłady:

IDENT=[PIN][#]+[Karta] lub

IDENT=[Karta]+[PIN][#] lub

IDENT=[PIN] [#] lub

IDENT=[Karta] lub

IDENT=[numer ID]

Grupy Dostępu

Użytkownicy kontrolera mogą posiadać status **Bez Grupy** lub przynależeć do jednej ze zdefiniowanych w systemie Grup Dostępu. W kontrolerach PRxx2 można zdefiniować maksymalnie 250 Grup Dostępu. Przynależność do danej Grupy Dostępu determinuje prawa dostępu użytkownika w ramach danego systemu KD. Wszyscy użytkownicy należący do tej samej Grupy Dostępu mają te same uprawnienia dostępu, w szczególnym przypadku grupa może się składać tylko z jednego użytkownika. Członkowie grupy uzyskują dostęp do określonych obszarów zwanych Strefami Dostępu zgodnie z indywidualnie zdefiniowanymi harmonogramami czasowymi. Użytkownicy posiadający status Bez Grupy posiadają dostęp do wszystkich Stref Dostępu bez żadnych ograniczeń czasowych – w rezultacie mają dostęp do wszystkich pomieszczeń przez całą dobę. Domyślnie, każdy nowododany użytkownik systemu RACS 4 ma status Bez Grupy.

Uwaga: W systemie RACS 4 każdy z użytkowników może należeć wyłącznie do jednej Grupy Dostępu, nie ma możliwości przypisywania użytkownika do wielu grup.

Tryby Identyfikacji

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

Tabela nr 4: Tryby Identyfikacji	
Nazwa trybu	**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 wymaga tylko karty nie akceptuje kodów PIN
Tylko PIN	Kontroler wymaga tylko kodu PIN nie akceptuje karty

Tryby Identyfikacji definiuje się indywidualnie dla każdej strony przejścia. O ile tryb identyfikacji nie zostanie zmieniony to kontroler stosuje tzw. Domyślny Tryb Identyfikacji. Tryb Identyfikacji dotyczy wszystkich użytkowników. Sterowanie trybami identyfikacji może odbywać się na cztery sposoby:

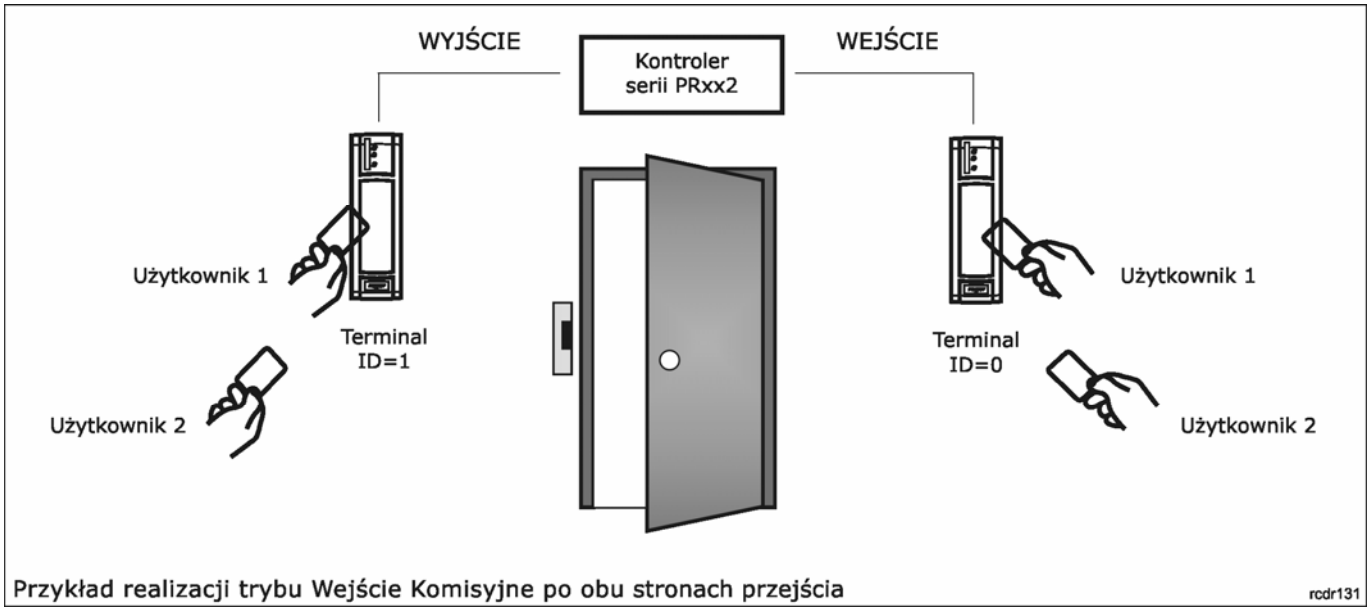
- Za pomocą harmonogramu czasowego
- Za pomocą linii wejściowych
- Za pomocą klawiszy funkcyjnych
- Za pomocą poleceń (komend) z klawiatury

Opcje Specjalne

Wejścia Komisyjne

PRMaster:/Właściwości kontrolera/Dostęp/Wejście komisyjne

Jeśli ten tryb jest włączony to dostęp do pomieszczenia może być przyznany dopiero wtedy gdy dwóch użytkowników, jeden po drugim, dokona poprawnej identyfikacji. Każdy z użytkowników musi dokonać identyfikacji wg tego Trybu 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 po tej samej stronie przejścia co użytkownik pierwszy lub po drugiej stronie. Załączenie trybu Wejścia Komisyjnego odnosi się do obydwu stron przejścia, nie można załączyć tego trybu indywidualnie dla każdej ze stron. Działanie trybu Wejście Komisyjne może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu.



Przykład realizacji trybu Wejście Komisyjne po obu stronach przejścia

Wejście Warunkowe

PRMaster:/Właściwości kontrolera/Zaawansowane/Wejście Warunkowe

Gdy na kontrolerze obowiązuje tryb Wejście Warunkowe to prawo wejścia do pomieszczenia posiadają nie tylko osoby uprawnione ale również wszystkie inne pod warunkiem, że jest już ktoś w środku. 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

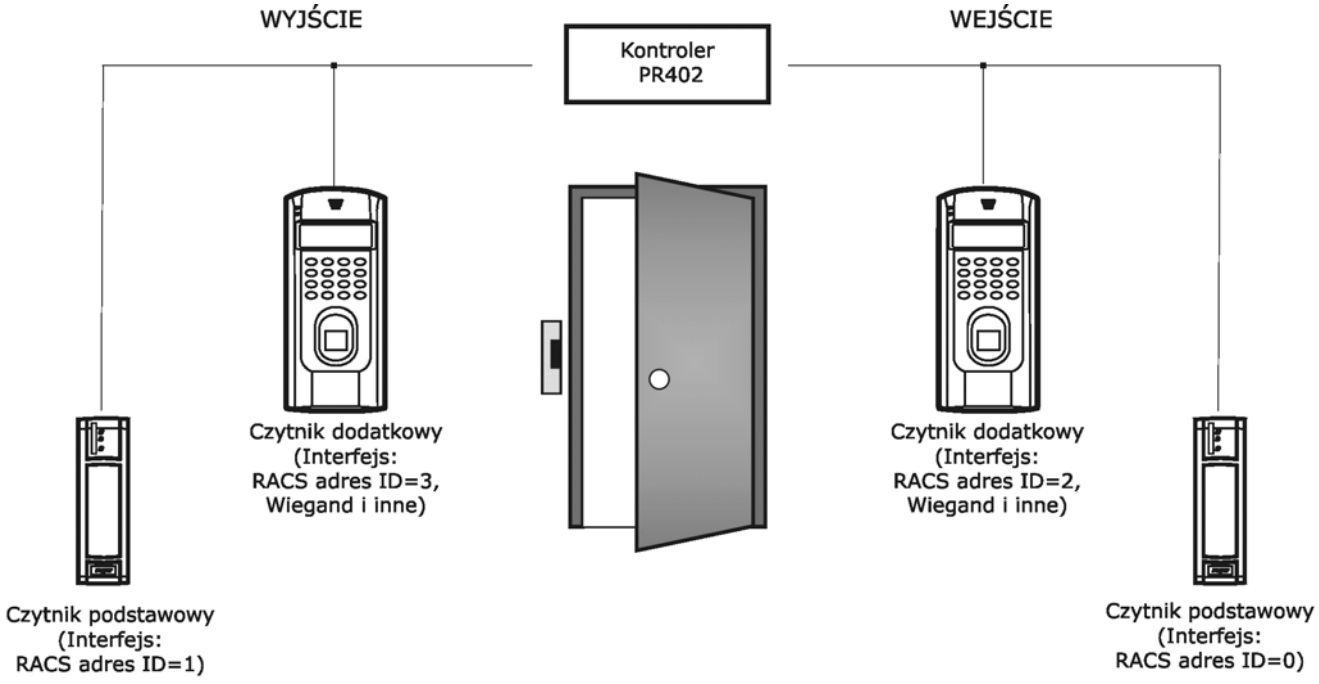
wyjście z pomieszczenia jest możliwe dla wszystkich użytkowników bez względu na ich uprawnienia i na ilość osób znajdujących się w wewnątrz.

Domyślnie, czytnik ID0 funkcjonuje jako czytnik wejściowy do pomieszczenia natomiast czytnik ID1 jako czytnik wyjściowy, niemniej przyporządkowanie to może zostać zmienione z poziomu programu zarządzającego (*zakładka: Terminal ID0 i Terminal ID1, parametr: Lokalizacja czytnika, ustawienie: Wejście do pomieszczenia lub Wyjście z pomieszczenia*) wtedy logowanie na czytniku ID1 jest uznawane za wejście do pomieszczenia a logowanie na czytniku ID0 jako wyjście. Sterowanie trybem Wejścia Warunkowego odbywa się za pośrednictwem harmonogramu czasowego i może podlegać Warunkowi Dodatkowemu. Tryb Wejście Warunkowe wymaga załączenia funkcji anti-passback'u lokalnego.

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.

Tryb High Security
PRMaster:/Właściwości kontrolera/Terminal ID1(ID0)/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* 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. Zwykle, role czytnika dodatkowego pełni czytnik biometryczny (np. czytnik linii papilarnych) niemniej w ogólnym przypadku może być to dowolny typ czytnika.



Przykład realizacji trybu High Security po obu stronach przejścia (przykład z PR402) rcdr132

Losowa kontrola użytkowników
PRMaster:/Właściwości kontrolera/Zaawansowane/Losowa kontrola użytkowników

Funkcja ta służy do wyrywkowego wyznaczania osób celem ich zrewidowania. Gdy funkcja jest załączona kontroler losowo odmawia prawa dostępu przypadkowemu użytkownikowi i sygnalizuje

strażnikom konieczność wykonania kontroli. Sygnalizacja kontroli losowej jest realizowana akustycznie na wewnętrznym głośniku oraz wyświetlaczu LCD (PR602LCD). Opcjonalnie, może ona być również realizowana na linii wyjściowej **[39]: Żądanie losowej kontroli**. Sygnalizacja kontroli trwa przez 2 s i w czasie tym kontroler wstrzymuje dalsze przyznawanie dostępu. Intensywność kontroli można definiować wskazując jaki procent wszystkich osób ma być skierowanych do kontroli. Dla przykładu ustawienie intensywności na poziomie 10% powoduje, że statystycznie biorąc co dziesiąta osoba zostanie wyznaczona do kontroli. Działanie funkcji może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu.

Opcja: Losowa kontrola użytkowników wymaga potwierdzenia

Załączenie opcji powoduje, że w momencie skierowania osoby do rewizji kontroler załącza sygnalizację żądania kontroli (głośnik, linia wyjściowa [39]) oraz wstrzymuje przyznawanie dostępu aż do momentu potwierdzenia kontroli za pośrednictwem klawisza funkcyjnego lub linii wejściowej zaprogramowanych do funkcji: **[46]: Losowa kontrola – potwierdzenie**.

Tryby Drzwi

Tryb Drzwi określa zasady na jakich kontroler blokuje/odblokowuje dozorowane drzwi. Rozróżnia się cztery Tryby Drzwi:

Tabela nr 5: Tryby Drzwi

Nazwa trybu	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
Warunkowo Odblokowane	Początkowo drzwi są w stanie Normalnym, z chwilą przyznania dostępu pierwszej osobie drzwi przechodzą do trybu Odblokowane
Zamknięte	Drzwi są permanentnie zablokowane niezależnie od tego czy użytkownik który próbuje wejść jest uprawniony do wejścia czy nie

Domyślnym trybem drzwi jest tryb Normalny, zmiana trybu drzwi może nastąpić w wyniku działania następujących mechanizmów:

- Harmonogram czasowy (Harmonogramy Trybu Drzwi)
- Linia wejściowa
- Klawisz funkcyjny
- Komenda z klawiatury
- Komenda zdalna z komputera zarządzającego

Przezbrajanie

Tryby Uzbrojenia

Kontroler PRxx2 ma dwa stany uzbrojenia: Uzbrojony i Rozbrojony; aktualny stan uzbrojenia jest sygnalizowany na dwukolorowym wskaźniku LED STAN przy czym stanowi uzbrojenia odpowiada kolor czerwony natomiast stanowi rozbrojenia odpowiada kolor zielony. W kontrolerze PR402 stan uzbrojenia jest dodatkowo sygnalizowany na wskaźnikach LED znajdujących się na płycie głównej, w tym przypadku każdemu stanowi odpowiada osobny wskaźnik LED.

Uwaga: Jeżeli czytniki serii PRT dołączone do kontrolera pracują w innych trybach niż tryb RACS Clock & Data to sterowanie ich wskaźnikami LED jest realizowane na odmiennych zasadach i nie musi odzwierciedlać aktualnego stanu uzbrojenia kontrolera.

Sterowanie trybem uzbrojenia kontrolera może być realizowane na kilka sposobów wymienionych poniżej:

- Manualnie przy pomocy identyfikatorów
- Automatycznie z poziomu harmonogramu czasowego
- Z linii wejściowej
- Z klawisza funkcyjnego
- Poleceniem (komendą) z klawiatury
- Zdalnie z poziomu centrali CPR
- Zdalnie z komputera zarządzającego

Wszystkie wymienione sposoby przezbrajania mogą być stosowane współbieżnie. Wyjątkiem od tej zasady jest sytuacja gdy stan uzbrojenia jest sterowany z poziomu linii wejściowej **[03]: Przezbrajanie – klucz stały**, wybranie tego sposobu przezbrajania blokuje wszystkie inne metody sterowania stanem uzbrojenia kontrolera.

W przypadku współbieżnego stosowania wielu metod przezbrajania kontroler przyjmuje taki stan jaki wynika z ostatnio zastosowanego mechanizmu przezbrajającego.

Przezbrajanie przy pomocy identyfikatorów
Kontroler może być przezbrajany przy pomocy identyfikatorów: MASTER, SWITCHER Full, SWITCHER Limited lub NORMAL z atrybutem Local SWITCHER.

Sposób przezbrajania:

- Wprowadź identyfikator (karta, kod PIN lub obydwa te elementy w zależności od aktualnie obowiązującego trybu identyfikacji)
- Jeśli użytkownik do którego należy użyty identyfikator posiada aktualnie prawo dostępu kontroler przyzna dostęp i zwolni drzwi
- Poczekaj, aż wskaźnik LED SYSTEM zacznie pulsować
- Gdy wskaźnik SYSTEM pulsuje dokonaj powtórnie identyfikacji (bez względu na tryb identyfikacji tym razem wystarczy tylko jedna z dostępnych form identyfikacji tzn. karta lub PIN)

Przezbrajanie przy pomocy identyfikatora SWICHTER LTD wymaga tylko jednokrotnego użycia identyfikatora i nigdy nie powoduje przyznania dostępu.

Opcja: Gdy brak dostępu SWITCHER nie może przezbrajać
PRMaster:/Właściwości kontrolera/Opcje/Gdy brak dostępu SWITCHER nie może przezbrajać

Opcja ta dotyczy użytkowników klasy SWITCHER i powoduje że o ile w danym momencie dany użytkownik nie posiada prawa dostępu do pomieszczenia to nie może również używać swojego identyfikatora do przezbrojenia kontrolera.

Przezbrajanie kontrolera przez harmonogram czasowy
Kontroler może zmieniać stan uzbrojenia samoczynnie wg zdefiniowanego harmonogramu czasowego zwanego Harmonogramem Przezbrajania. Jeśli kontroler należy do pewnej Strefy Alarmowej to posiada taki sam Harmonogram Przezbrajania jaki obowiązuje dla danej Strefy Alarmowej. Jeśli jednak kontroler nie należy do żadnej Strefy Alarmowej to można mu przypisać dowolny harmonogram czasowy. Wskazanie harmonogramu *Nigdy* powoduje że kontroler na stałe będzie przebywał w trybie uzbrojenia, natomiast wskazanie harmonogramu *Zawsze* spowoduje że kontroler przez cały czas pracy będzie w trybie rozbrojenia.

Harmonogram Przezbrajania jest w istocie zwykłym harmonogramem czasowym (tzw. Harmonogram Ogólnego Przeznaczenia) który został użyty do sterowania trybem uzbrojenia kontrolera. Harmonogram Przezbrajania składa się z przedziałów czasowych *Od..Do…*, przedziały te wskazują

kiedy kontroler ma przechodzić samoczynnie do stanu rozbrojenia, poza tymi przedziałami kontroler ma samoczynnie powracać do stanu uzbrojenia. Algorytm przezbrajania przez harmonogram czasowy działa w następujący sposób; w momentach czasu wskazywanych przez parametr *Od:* kontroler bezwarunkowo przechodzi do stanu rozbrojenia natomiast o godzinie wskazywanej przez parametr *Do:* kontroler powraca do stanu uzbrojenia, aczkolwiek przejście do stanu uzbrojenia może być niemożliwe jeśli linia wejściowa **[13]: Blokada uzbrojenia** jest wyzwolona albo drzwi są otwarte. W przypadku gdy uzbrojenie zostało zablokowane przez dowolny z wymienionych warunków kontroler samoczynnie uruchamia zwłokę czasową **Domyślna zwłoka czasowa przed samouzbrojeniem** a po jej upływie ponownie próbuje się uzbroić. Proces jest powtarzany aż do skutku lub do momentu gdy upłynie okres uzbrojenia wynikający z harmonogramu czasowego.

Moment samoczynnego uzbrojenia może być również odwlekany przez użytkownika, przy czym ma on do dyspozycji następujące metody:

- Użycie klawisza funkcyjnego
- Wyzwolenie linii wejściowej
- Polecenie z klawiatury (komenda)
- Automatycznie z chwilą przyznania dostępu

Czas o jaki zostaje przesunięty moment uzbrojenia przez użytkownika jest określony przez parametr **Dodatkowa zwłoka czasowa przed samouzbrojeniem**. Odliczanie tej zwłoki czasowej można skasować w dowolnym momencie poprzez:

- Użycie klawisza funkcyjnego
- Wyzwolenie linii wejściowej
- Polecenie z klawiatury (komendę)

Po skasowaniu tej zwłoki czasowej kontroler natychmiast podejmuje próbę uzbrojenia.

Opcja: Sterowanie przezbrajaniem z harmonogramu
PRMaster:/Właściwości kontrolera/Przezbrajanie/Sterowanie przezbrajaniem z harmonogramu

Gdy opcja ta jest załączona stan uzbrojenia kontrolera zmienia się automatycznie wg odpowiedniego harmonogramu czasowego przy czym może być to harmonogram przezbrajania zdefiniowany dla danej Strefy Alarmowej do której należy kontroler lub może to być dowolny inny harmonogram czasowy gdy kontroler nie należy do żadnej Strefy Alarmowej. Gdy opcja jest wyłączona sterowanie uzbrojeniem przez harmonogramy czasowe jest wyłączone.

Sygnalizacja zbliżającego się uzbrojenia
PRMaster:/Właściwości kontrolera/Przezbrajanie/Samouzbrajanie/Alert przed samouzbrajaniem

Kontroler może akustycznie sygnalizować fakt zbliżającego się uzbrojenia na wewnętrznym głośniku czytnika oraz na linii wyjściowej **[33]: Alert przed samouzbrojeniem – wyjście niemodulowane** i/lub **[34]: Alert przed samouzbrojeniem – wyjście modulowane**. Sygnalizacja zbliżającego się uzbrojenia jest załączana w czasie określonym przez parametr **Alert przed samouzbrojeniem**. Celem tej sygnalizacji jest ostrzeżenie osób pozostających w pomieszczeniach że wkrótce nastąpi planowane uzbrojenie kontrolera.

Opcja: Przyznanie dostępu opóźnia samouzbrojenie
PRMaster:/Właściwości kontrolera/Przezbrajanie/Samouzbrajanie/Przyznanie dostępu opóźnia samouzbrojenie

Działanie opcji polega na tym że automatycznie w momencie przyznania dostępu kontroler opóźnia moment planowanego uzbrojenia o czas wskazywany przez licznik **Dodatkowa zwłoka czasowa przed samouzbrojeniem**. Dzięki opcji tej użytkownicy poruszający się przez przejście nie są zobligowani do dodatkowych czynności w celu opóźnienia momentu samouzbrojenia.

Opcja: Harmonogram przezbrajania steruje tylko uzbrajaniem
PRMaster:/Właściwości kontrolera/Przezbrajanie/Opcje przezbrajania/Harmonogram przezbrajania steruje tylko uzbrajaniem

Normalnie, harmonogram przezbrajania określa przedziały czasu *Od..Do…*gdy kontroler samoczynnie przechodzi do stanu rozbrojenia i poza nim przywraca stan uzbrojenia. Po załączeniu opcji **Harmonogram przezbrajania steruje tylko uzbrajaniem** działanie harmonogramu przezbrajania ogranicza się jedynie do procesu samoczynnego uzbrajania natomiast samoczynne rozbrajanie jest pomijane. Opcję tę stosuje się wtedy gdy istnieje potrzeba wymuszenia uzbrojenia o pewnych godzinach rozbrajanie natomiast ma się odbywać w skutek interwencji użytkownika. Dla przykładu, jeśli harmonogram przezbrajania zawiera przedział czasowy 12:00-13:00 to normalnie w tych godzinach kontroler samoczynnie przejdzie do stanu rozbrojenia, gdy opcja **Harmonogram przezbrajania steruje tylko uzbrajaniem** będzie załączona to kontroler nie rozbroi się samoczynnie o godz. 12:00 ale wykona samoczynne uzbrojenie o godzinie 13:00.

Opcja: Uzbrojenie kasuje tryb Odblokowane
PRMaster:/Właściwości kontrolera/Przezbrajanie/Opcje przezbrajania/Uzbrojenie kasuje tryb Odblokowane

Załączenie tej opcji powoduje że w momencie uzbrojenia kontroler będzie kasował tryb drzwi Odblokowane i przywracał tryb Normalny. Opcja ta ma na celu uniemożliwienie pozostawienia przejścia otwartego w sytuacji gdy kontroler przejdzie do trybu uzbrojenia.

Opcja: Szybkie Rozbrajanie
PRMaster:/Właściwości kontrolera/Przezbrajanie/Opcje przezbrajania/Szybkie Rozbrajanie

Opcja ta dotyczy identyfikatorów klasy MASTER, SWITCHER Full oraz użytkowników NORMAL z załączonym atrybutem Local SWICTHER. Załączenie tej opcji powoduje że zmiana stanu uzbrojenia kontrolera następuje już z chwilą pierwszego użycia identyfikatora a nie jak to ma miejsce normalnie po dwóch, następujących bezpośrednio po sobie, użyciach identyfikatora tego typu.

Uwaga: Opcja ta nie ma wpływu na sposób przezbrajania kontrolera przy użyciu identyfikatora typu SWITCHER Ltd., wystarczy jedno użycie tego identyfikatora aby kontroler zmienił stan uzbrojenia.

Opcja: Przezbrajanie wymaga 5-krotnego odczytu identyfikatora
PRMaster:/Właściwości kontrolera/Przezbrajanie/Opcje przezbrajania/Przezbrajanie wymaga 5-krotnego odczytu identyfikatora

Załączenie opcji tej powoduje że w celu przezbrojenia kontrolera przy pomocy karty zbliżeniowej należy zbliżyć ją do czytnika i nie oddalając jej odczekać aż czytnik pięciokrotnie ją odczyta a następnie zmieni stan uzbrojenia. Opcję te wykorzystuje się głównie w celu zabezpieczenia kontrolera przed przypadkowym przezbrojeniem wskutek dwukrotnego odczytu identyfikatora zbliżeniowego.

Uwaga: Jeśli na czytniku obowiązuje aktualnie tryb Karta i PIN to przy załączonej ww. opcji należy wprowadzić jednokrotnie kod PIN a następnie zbliżyć kartę do czytnika i odczekać aż nastąpi pięć odczytów.

Opcja: Samoczynnie przywróć tryb uzbrojenia po czasie
PRMaster:/Właściwości kontrolera/Przezbrajanie/Samouzbrajanie/Samoczynnie przywróć tryb uzbrojenia po czasie

Załączenie tej opcji powoduje że jeśli w trakcie okresu uzbrojenia który wynika z działania harmonogramu czasowego ktoś rozbroi manualnie kontroler to przy załączonej tej opcji kontroler samoczynnie po upływie czasu zdeklarowanego dla tej opcji powróci do trybu uzbrojenia.

Opcja: Blokuj uzbrojenie gdy drzwi otwarte
PRMaster:/Właściwości kontrolera/Przezbrajanie/Opcje przezbrajania/Harmonogram przezbrajania steruje tylko uzbrajaniem

Załączenie opcji powoduje że w przypadku gdy drzwi są otwarte kontroler nie będzie mógł wejść w stan uzbrojenia. Celem tej opcji jest zablokowanie możliwości uzbrojenia kontrolera gdy drzwi nie są zamknięte.

Definiowanie Praw Dostępu

Definiowanie praw dostępu w systemie RACS polega na wskazaniu kto, gdzie i kiedy ma mieć prawo dostępu. Proces ustalania zasad dostępu można podzielić na następujące etapy:

- Podział użytkowników na Grupy Użytkowników
- Podział kontrolerów na Strefy Dostępu
- Definiowanie Harmonogramów Czasowych (kalendarzy)
- Powiązanie Grup Użytkowników ze Strefami Dostępu oraz Harmonogramami Czasowymi. Etap ten polega na wskazaniu harmonogramu czasowego który określi przedziały dni/godzin kiedy użytkownicy danej grupy będą mieli prawo dostępu do wybranej Strefy Dostępu
- 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 czytnik
- Sprawdzenie dodatkowych mechanizmów sterujących dostępem (APB, opcje specjalne, tryb drzwi itd.)
- Decyzja o dostępie
- Odblokowanie drzwi

Uwaga: W kontrolerach serii PRxx2 prawa dostępu definiuje się indywidualnie dla każdej ze stron przejścia czyli osobno dla wejścia i wyjścia.

Kontroler nie przyznaje dostępu gdy:

- Odczytany identyfikator nie jest znany
- Odczytany identyfikator nie jest pełny np. wprowadzono tylko PIN choć na czytniku obowiązuje tryb Karta i PIN
- Kiedy wprowadzony identyfikator należy do użytkownika typu SWITCHER Limited
- Gdy z harmonogramu czasowego wynika że dana Grupa 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**
- 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.

Sygnalizacja dostępu
Zawsze, kiedy kontroler przyznaje dostęp zapala wskaźnik LED OTWARTE który pozostaje zapalony tak długo jak drzwi są w stanie odblokowania.

Sterowanie elementem wykonawczym
W praktyce spotyka się cztery podstawowe sposoby sterowania elementem wykonawczym:

- Przez podanie zasilania (np. elektrozaczep)
- Przez odjęcie zasilania (np. zwora magnetyczna)
- Przez podanie impulsu (np. sterowanie szlabanem)
- Przez sterowanie silnikiem wykonawczym

Kontroler może sterować zamkiem za pośrednictwem trzech wyjść: **[97]: Zamek drzwi - wejście**, **[98]: Zamek drzwi – wyjście**, **[99]: Zamek drzwi**. Kontroler aktywuje wyjście [99] bez względu na to czy dostęp został przyznany z czytnika wejściowego czy wyjściowego, wyjścia [97] i [98] są aktywowane w zależności na którym czytniku (wejściowym lub wyjściowym) nastąpiło przyznanie dostępu. Wyjścia [97] i [99] służą generalnie do kontroli przejść z bramką obrotową gdzie zachodzi potrzeba wskazania kierunku obrotu bramki.

W momencie przyznania dostępu drzwi zostają odblokowane na czas określony przez parametr **Czas na wejście** który może być zdefiniowany w zakresie od 1 sekundy do 99 minut. Opcjonalnie sterowanie zamkiem drzwiowym może być realizowane w trybie *zatrzask*, wtedy drzwi zostają odblokowane na czas nieograniczony aż do momentu wystąpienia kolejnego przyznania dostępu (*praca bistabilna*).

Opcja: Zamek drzwiowy sterowany bistabilnie (sterowanie typu zatrzask)
PRMaster:/Właściwości kontrolera/Dostęp/Opcje sterowania dostępem/Zamek drzwiowy sterowany bistabilnie

Gdy opcja jest załączona to każde przyznanie dostępu przełącza wyjście sterujące elementem wykonawczym do stanu przeciwnego. Wyjście pozostaje w tym stanie aż do momentu gdy kontroler ponownie przyzna komuś dostęp. 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.

Opcja: Samoczynne blokowanie drzwi (ang. Auto-relock)
PRMaster:/Właściwości kontrolera/Dostęp/Opcje sterowania dostępem/Samoczynne blokowanie drzwi

Stosowanie tej opcji ma sens jedynie wtedy kontroler współpracuje z czujnikiem otwarcia drzwi. Załączenie tej opcji powoduje że kontroler może skrócić **Czas na wejście**. Opcja ta ma dwa warianty:

- Blokuj element wykonawczy po otwarciu drzwi
- Blokuj element wykonawczy po domknięciu drzwi

W pierwszym przypadku kontroler kasuje wyjście sterujące zamkiem w momencie gdy rozpozna że drzwi zostały już otwarte, wariant ten stosuje się w odniesieniu do urządzeń które odblokowują drzwi w momencie podania zasilania (np. elektro-zaczep). W drugim przypadku kontroler wyłącza wyjście sterujące zamkiem w momencie gdy rozpozna że drzwi zostały ponownie domknięte, wariant ten stosuje się w odniesieniu do urządzeń które odblokowują drzwi poprzez zdjęcie zasilania (np. zwora elektromagnetyczna).

Opcja: Blokuj dostęp gdy kontroler uzbrojony
PRMaster:/Właściwości kontrolera/Dostęp/Opcje sterowania dostępem/Blokuj dostęp gdy kontroler jest w stanie uzbrojenia

Gdy opcja jest załączona kontroler może przyznać dostęp do pomieszczenia tylko wtedy gdy znajduje się on w trybie rozbrojenia. Jeśli jest w trybie uzbrojenia dostęp jest permanentnie

zablokowany dla wszystkich użytkowników, również tych którzy posiadają w danej chwili prawo dostępu do pomieszczenia. Dzięki opcji tej użytkownicy uprawnieni do przezbrajania kontrolera mogą czasowo blokować i odblokowywać dostęp dla pozostałych użytkowników systemu bez względu na ustawienia harmonogramów dostępu.

Kod Obiektu (ang. Facility Code)
PRMaster:/Właściwości kontrolera/Dostęp/Kod Obiektu

Kod Obiektu to 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 kodu karty które po przetworzeniu na postać dziesiętną dają liczbę z zakresu od 000-255.

Załączenie opcji Kod Obiektu powoduje że kontroler przyznaje dostęp wszystkim kartom które mają ten sam Kod Obiektu.

Działanie funkcji Kod Obiektu może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu.

PREALARM
Stan PREALARM informuje że ktoś w czasie pięciu minut dokonał pięciu kolejnych prób użycia niedozwolonego identyfikatora (karty, PIN-u). Stan PREALARM-u może być sygnalizowany indywidualnie na wyjściu **[29]: Prealarm** lub na wyjściu **[256]: Alarm Drzwi**.

Opcja: Blokuj odczyt kart i PIN-ów w stanie Prealarm-u
PRMaster:/Właściwości kontrolera/Opcje/Blokuj odczyt kart i PIN-ów w stanie Prealarm-u

Po załączeniu tej opcji kontroler blokuje na czas pięciu kolejnych minut odczyt kart oraz kodów PIN po wystąpieniu stanu Prealarm-u.

WŁAMANIE
Stan WŁAMANIE następuje w wyniku aktywacji linii wejściowej skonfigurowanej do funkcji **[09] WŁAMANIE.**

Opcja: Ignoruj linie [09] WŁAMANIE gdy kontroler rozbrojony
PRMaster:/Właściwości kontrolera/Opcje/Ignoruj linie [09] WŁAMANIE gdy kontroler rozbrojony

Załączenie tej opcji uniemożliwia załączenie alarmu gdy kontroler znajduje się w stanie rozbrojenia.

Opcja: Kod PIN pod przymusem
Celem tej funkcji jest sygnalizacja sytuacji gdy kod PIN został wprowadzony pod przymusem. Gdy załączona jest ta opcja to wprowadzenie kodu PIN różniącego się o jedność na ostatniej pozycji jest interpretowane jako wprowadzenie kodu pod przymusem co następnie wywołuje sygnalizację stanu WEJŚCIE SIŁOWE.

Przykład:

Prawidłowy kod to [4569][#]. Wprowadzenie kodu [4568][#] bądź [4560][#] jest interpretowane jako wprowadzenie kodu pod przymusem.

Uwaga: Aby kontroler właściwie rozpoznawał kody PIN wprowadzone pod przymusem należy zadbać o to aby kody użytkowników różniły się więcej niż o jedność na ostatniej pozycji. Program PR Master samoczynnie sprawdza czy ten warunek jest spełniony. Jeśli jednak rozpoznawanie kodów PIN pod przymusem nie jest celowe można w ustawieniach programu PR Master wyłączyć tą funkcję i wtedy program będzie dopuszczał definiowanie kodów PIN różniących się między sobą o dowolną wartość.

Opcja: Nie sygnalizuje użycia kodu PIN pod przymusem
PRMaster:/Właściwości kontrolera/Opcje/Nie sygnalizuje użycia kodu PIN pod przymusem

Załączenie tej opcji powoduje że wprowadzenie kodu PIN różniącego się o +/-1 na ostatniej pozycji od kodu właściwego nie będzie wywoływało sygnalizacji stanu WEJŚCIE SIŁOWE.

Opcja: Klawisz [#] zamiennie sygnalizuje dzwonek lub zwalnia drzwi
PRMaster:/Właściwości kontrolera/Termina ID1(ID0)/Opcje klawisza#/Klawisz [#] zamiennie sygnalizuje dzwonek lub zwalnia drzwi

Działanie tej opcji dotyczy tylko sytuacji gdy klawisz [#] jest użyty samodzielnie. W przypadku załączenia tej opcji użycie samodzielne klawisza [#] jest interpretowane przez kontroler jako użycie przycisku *Dzwonek* lub *Przycisku Wyjścia* przy czym o tym w jaki sposób zostanie to zinterpretowane decyduje harmonogram czasowy przypisany do tej funkcji. Domyślnie, dla omawianej funkcji jest przypisany harmonogram *Nigdy* co powoduje że przycisk [#] przez cały czas działa jako przycisk dzwonka, użycie harmonogramu *Zawsze* spowoduje że klawisz [#] będzie przez cały czas działał jak przycisk wyjścia. Użycie innego harmonogramu powoduje że w przedziałach czasowych zdefiniowanych przez ten harmonogram przycisk [#] będzie działał jako *Przycisk Wyjścia* natomiast poza nimi jako przycisk *Dzwonek*. W opcji tej działanie klawisza [#] jest tożsame z użyciem przycisku podłączonego do wejścia **[7]: Dzwonek** lub **[02]: Przycisk wyjścia** i odnosi się zarówno do klawiszy [#] dostępnych na czytnikach zewnętrznych jak i zintegrowanych z kontrolerem (np. PR302, PR602LCD).

Flagi Systemowe

Flagi Systemowe lub w skrócie *Flagi* to stany logiczne w pamięci kontrolera które odzwierciedlają pewne określone 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 innych, dowolnie wybranych celów (np. AUX1, AUX2).

Pierwotnie, każda flaga znajduje się w stanie wyłączenia, przejście jej do stanu załączenia może nastąpić jedynie w następstwie wystąpienia pewnych, specyficznych dla danej flagi mechanizmów. Powrót flagi do stanu normalnego następuje samoczynnie po upływie czasu określonego przez jej licznik lub pod wpływem innego, właściwego dla niej zdarzenia.

Czas na jaki dana flaga zostaje załączona określa jej licznik. Po upływie czasu określonego przez licznik flaga samoczynnie powraca do stanu normalnego czyli stanu wyłączenia. Liczniki dla pewnych 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 prezentowany na linii wyjściowej.

Tabela nr 6: Flagi Systemowe	
Nazwa	**Opis**
TAMPER	Flaga zostaje załączona w momencie rozpoznania stanu aktywnego na wejściu **[08:] TAMPER**, flaga jest zerowana w momencie rozbrojenia kontrolera lub automatycznie gdy upłynie czas określony przez jej licznik.
WŁAMANIE	Flaga zostaje załączona w momencie rozpoznania stanu aktywnego na linii **[09]: WŁAMANIE** lub może być aktywowana z klawiatury poprzez komendę **[F30]: Załącz stan WŁAMANIE**. Flaga jest zerowana w momencie rozbrojenia kontrolera lub po czasie określonym przez jej licznik.
ŚWIATŁO	Sterowanie tą flagą, zarówno załączenie jak i jej wyłączenie, może być realizowane na kilka, wymienionych poniżej sposobów: • z linii wejściowych • polecenia (komendy) z klawiatury • z klawisza funkcyjnego Dodatkowo, flaga ta ulega automatycznemu wyłączeniu z chwilą upłynięcia czasu określonego przez jej licznik.
AUX 1	Sterowanie na identycznych zasadach co flagą ŚWIATŁO.
AUX 2	Sterowanie na identycznych zasadach co flagą ŚWIATŁO.

WEJŚCIE SIŁOWE	Flaga ta zostaje załączona w momencie wystąpienia stanu WEJŚCIE SIŁOWE. Natomiast zerowanie flagi następuje: • automatycznie po czasie zdefiniowanym przez jej licznik • w momencie rozbrojenia kontrolera • po użyciu uprawnionego identyfikatora
PREALARM	Flaga ta zostaje załączona w momencie wystąpienia stanu PREALARM. Flaga jest zerowana w identycznych przypadkach jak flaga WEJŚCIE SIŁOWE.
DRZWI OTWARTE	Flaga ta zostaje załączona w momencie wystąpienia stanu DRZWI OTWARTE. Natomiast zerowanie flagi następuje: • automatycznie po czasie zdefiniowanym przez jej licznik • w momencie rozbrojenia kontrolera • po użyciu uprawnionego identyfikatora • oraz z chwilą domknięcia drzwi.

Uwaga: Istnieje możliwość załączenia Opcji: Użycie karty/kodu PIN nie kasuje stanu DRZWI OTWARTE, która uniemożliwia zerowanie flagi poprzez użycie uprawnionego identyfikatora.

Alarm Drzwi
Przez pojęcie stanu 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 osobnej linii wyjściowej lub zbiorczo na linii **[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.

Tabela nr 7: Alarmy Drzwi

Stan	**Opis**	**Priorytet**	**Metoda sygnalizacji**
PREALARM	Stan ten występuje w następstwie wystąpienia pięciu kolejnych prób wprowadzenia nieznanego identyfikatora w czasie nie dłuższym niż pięć minut.	Niski	Pojedynczy impuls powtarzany co 2 sekundy.
DRZWI OTWARTE	Stan powstaje w momencie gdy drzwi nie zostaną domknięte po upływie czasu określonego przez: **Czas na zamknięcie**.	Średni	Dwa impulsy powtarzane co 2 sekundy.
WEJŚCIE SIŁOWE	Stan występuje w przypadku wykrycia otwarcia drzwi bez udziału kontrolera lub na skutek wprowadzenia kodu PIN pod przymusem.	Najwyższy	Pojedynczy impuls trwający 1 sekundę, powtarzany co 1 sekundę.

Opcje: Nie sygnalizuj stanu PREALARM, Nie sygnalizuj stanu DRZWI OTWARTE, Nie sygnalizuj stanu WEJŚCIE SIŁOWE
PRMaster:/Właściwości kontrolera/Opcje/Alarm Drzwiowy/Nie sygnalizuj stanu..

Domyślnie Alarm Drzwi sygnalizuje wystąpienie dowolnego z trzech alarmów szczegółowych: PREALARM, DRZWI OTWARTE i WEJŚCIE SIŁOWE. Zaznaczenie opcji **Nie sygnalizuj...** powoduje wyłączenie sygnalizacji konkretnego (wskazanego w opcji) stanu alarmowego.

Dla przykładu, zaznaczenie opcji **Nie sygnalizuj stanu PREALARM** spowoduje, że w momencie wystąpienia tego stanu linia wyjściowa Alarm Drzwi pozostanie nieaktywna. Stan ten nie będzie również sygnalizowany na wewnętrznym głośniku czytnika (jeśli uprzednio zostanie załączona opcja sygnalizacji alarmu na wewnętrznym przetworniku akustycznym). Linia ta załączy się natomiast w chwili wystąpienia stanu DRZWI OTWARTE i/lub WEJŚCIE SIŁOWE.

Ponadto istnieje możliwość wyłączenia sygnalizacji **Alarmu Drzwi** gdy kontroler znajduje się w stanie rozbrojenia za pomocą **Opcji: Nie sygnalizuj Alarmu Drzwi gdy kontroler rozbrojony.** Opcja ta ma na celu uniemożliwienie załączenia alarmu w sytuacji gdy kontroler przejdzie do trybu rozbrojenia.

Anti-passback (APB)

W przypadku załączenia funkcji Anti-passback użytkownik jest zobligowany do logowania się naprzemiennie raz na wejściu raz na wyjściu z pomieszczenia lub 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

Ze względu na sposób reakcji kontrolera na naruszanie zasad APB rozróżnia się:

- APB Twardy
- APB Miękki

APB Lokalny
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.

APB Globalny
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. Gdy w systemie obowiązuje APB Globalny to aby wyjść z danej Strefy APB użytkownik musi najpierw do niej wejść. APB Globalny może być stosowany w systemach posiadających minimum dwa kontrolery, dodatkowo w systemie musi być zainstalowana centrala typu CPR32-SE.

Uwaga: Wykorzystanie funkcji globalnego APB wymaga centrali CPR32-SE z oprogramowaniem firmowym w wersji 30.17 lub wyższej.

Opcja: APB z obsługą czujnika wejścia (ang. True APB)
PRMaster:/Właściwości kontrolera/Zaawansowane/APB z obsługą czujnika wejścia

Normalnie, po przyznaniu dostępu, kontroler uznaje że dany użytkownik wszedł (wyszedł) z pomieszczenia i stosownie do tego uaktualnia Rejestr APB. Załączenie tej opcji powoduje że aktualizacja Rejestru APB jest dokonywana dopiero wtedy gdy kontroler rozpozna że po przyznaniu dostępu drzwi zostały otwarte, gdy to nie nastąpi kontroler nie zmienia stanu Rejestru APB i uznaje że użytkownik nie wszedł pomimo tego że kontroler przyznał mu dostęp. Działanie tej opcji wymaga aby kontroler współpracował z czujnikiem otwarcia drzwi.

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 (Public). 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 4.2 Strefa APB może obejmować tylko kontrolery należące do tego samego Podsystemu. Nie można zdefiniować Strefy APB zawierającej kontrolery zlokalizowane w różnych Podsystemach.

Rejestr APB
Rejestr APB to obszar pamięci kontrolera w której przechowywane są informacje wskazujące po której stronie przejścia (na którym czytniku, wejściowym czy wyjściowym) każdy z użytkowników ostatnio się logował. Każdy z użytkowników zarejestrowanych w kontrolerze posiada swój Status APB który przybierać może cztery wartości wymienione poniżej:

Tabela nr 8: Status APB

Typ	Opis
Zalogowany na czytniku ID0	Użytkownik ostatnio zalogował się na terminalu ID0
Zalogowany na czytniku ID1	Użytkownik ostatnio zalogował się na terminalu ID1
Niezalogowany	Brak danych dotyczących ostatniego logowania – w takiej sytuacji najbliższe logowanie może odbywać się zarówno na czytniku wejściowym jak i wyjściowym z pomieszczenia lub strefy.
Zablokowany	Dostęp dla danego użytkownika jest całkowicie zablokowany, tzn. że bez względu na lokalizację czytnika każda próba zalogowania się zostanie odrzucona. Stan ten będzie utrzymywany dopóki status ten nie zostanie zmieniony.

Zerowanie Rejestru APB (Reset APB)
Operacja zerowania Rejestru APB powoduje że wszyscy użytkownicy zarejestrowani w kontrolerze otrzymują status: Niezalogowany. Po tej operacji 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.

Zerowanie Rejestru APB jest wykonywane automatycznie po włączeniu zasilania, może być również wykonane następującymi metodami:

- Z poziomu linii wejściowej
- Z klawisza funkcyjnego
- Poleceniem (komendą) z klawiatury
- Zdalnie (komendą) z komputera zarządzającego
- Automatycznie za pomocą harmonogramu czasowego (Harmonogram Zerowania APB)

Hierarchia Stref APB
Hierarchia Stref APB odzwierciedla relacje terytorialne pomiędzy różnymi Strefami APB zdefiniowanymi w ramach jednego podsystemu KD. W systemie KD z załączoną funkcją globalnego APB użytkownicy mogą przemieszczać się tylko między 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.

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.

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.

APB Twardy (APB Hard)
Gdy na kontrolerze obowiązuje Anti-passback Twardy to próba naruszenia zasad APB wywołuje odmowę dostępu (dwa długie sygnały dźwiękowe) oraz rejestrację zdarzenia Naruszenie APB.

APB Miękki (APB Soft)
Gdy na kontrolerze obowiązuje Anti-passback Miękki to każda próba naruszenia zasad APB wywołuje jedynie zarejestrowanie zdarzenia Naruszenie APB które informuje o fakcie naruszenia zasad APB lecz nie blokuje dostępu.

Harmonogram przełączania APB Twardy/Miękki
PRMaster:/Właściwości kontrolera/Zaawansowane/Anti-passback/Harmonogram przełączania APB Twardy/Miękki

Przełączanie kontrolera pomiędzy funkcją APB Twardy/Miękki jest realizowane za pomocą harmonogramu czasowego definiowanego dla tej funkcji. Harmonogram ten przełącza kontroler pomiędzy pracą w trybie APB Twardy-Miękki. Gdy harmonogram ten jest zdefiniowany jako *Zawsze* kontroler przez cały czas działa w trybie APB Twardy, jeśli harmonogram ten jest zdefiniowany jako *Nigdy* kontroler przez cały czas funkcjonuje w trybie APB Miękki. W przypadku zdefiniowania innego harmonogramu czasowego kontroler samoczynnie przechodzi do trybu APB Miękki w okresach czasu wskazywanych przez dany harmonogram i powraca do trybu APB Twardy poza tymi przedziałami czasowymi.

Strefy Alarmowe

Strefa Alarmowa to grupa kontrolerów które współbieżnie zmieniają swój aktualny stan uzbrojenia. Gdy dowolny kontroler należący do danej Strefy Alarmowej zmieni swój stan uzbrojenia (nie jest istotne co było przyczyną zmiany stanu uzbrojenia) reszta kontrolerów wchodzących w skład tej Strefy Alarmowej zostaje przezbrojona w ten sam sposób. Funkcja współbieżnego przezbrajania jest realizowana przez centralę CPR. Centrala ta w sposób ciągły monitoruje stany uzbrojenia wszystkich kontrolerów w systemie i gdy jeden z nich zmieni 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.

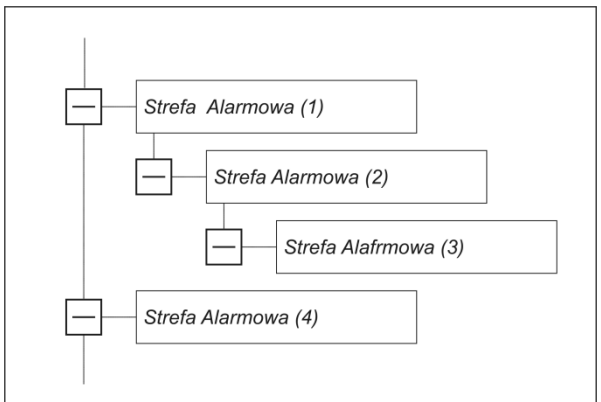
Gdy sterowanie stanem uzbrojenia kontrolera jest realizowane za pośrednictwem linii wejściowej **[03]: Przezbrajanie – klucz stały**, to stan uzbrojenia tego kontrolera nie może być zdalnie zmieniany przez urządzenie nadrzędne (centrala CPR) ani przez żaden inny mechanizm. Kontroler taki może należeć do Strefy Alarmowej lecz należy mieć na uwadze że stan jego uzbrojenia będzie zależał jedynie od stanu tej linii wejściowej i nie będzie podlegał sterowaniu z poziomu centrali CPR.

Hierarchia Stref Alarmowych

W systemie KD można zdefiniować jedną lub więcej Stref Alarmowych. Strefy Alarmowe mogą być niezależne od siebie lub tworzyć pewną zhierarchizowaną strukturę. Gdy Strefy Alarmowe są niezależne, to zmiana stanu uzbrojenia każdej 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.



Przykład hierarchii stref alarmowych rcdr001p3

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 stref (2). Uzbrojenie strefy (1) powoduje uzbrojenie stref (2) i (3) natomiast uzbrojenie strefy (2) powoduje uzbrojenie strefy (3).

Linie Wejściowe

Kontroler PR402 posiada cztery dwustanowe linie wejściowe (IN1…4), pozostałe kontrolery serii PRxx2 posiadają trzy wejścia (IN1..3). Każdą linię wejściową można indywidualnie skonfigurować co do funkcji oraz sposobu wyzwalania (NO/NC), dodatkowo linie dzielą się na linie typu *klucz stały* i *klucz chwilowy*. 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. Rodzaj klucza linii określa czy kontroler reaguje jedynie w chwili jej wyzwolenia (klucz chwilowy) lub na każdą zmianę jej stanu (klucz stały). Dla przykładu linia **[01]: Czujnik otwarcia** jest linią typu klucz stały i kontroler reaguje zarówno na jej wyzwolenie jak i powrót do stanu normalnego, linia **[02]: Przycisk wyjścia** jest linią typu klucz chwilowy – kontroler reaguje tylko na jej wyzwolenie.

Tabela nr 9: Linie Wejściowe

Kod	Funkcja	Klucz	Opis
00	Wejście wyłączone	Brak	Linia nie jest obsługiwana
01	Czujnik otwarcia	Stały	Linia jest dedykowana do podłączenia czujnika otwarcia drzwi. Gdy linia jest wyzwolona kontroler uznaje że drzwi są otwarte, gdy linia jest w stanie normalnym uznaje że drzwi są zamknięte
02	Przycisk wyjścia	Chwilowy	Wyzwolenie linii powoduje zwolnienie drzwi na zasadach identycznych jak po przyznaniu dostępu. Wejście takie jest przeznaczone do podłączenia tzw. przycisku wyjścia od środka lub innego typu kontaktu którego użycie ma zwalniać drzwi
03	Przezbrajanie - klucz stały	Stały	Linia ta służy do sterowania aktualnym stanem uzbrojenia. Gdy linia jest w stanie normalnym kontroler jest w stanie uzbrojenia, gdy linia jest wyzwolona kontroler przechodzi do stanu rozbrojenia. Uwaga: W kontrolerze może być zdefiniowana tylko jedna linia tego typu. W przypadku zdefiniowania takiej linii przestają działać wszystkie inne metody przezbrajania kontrolera
05	Dozór napięcia sieci AC	Stały	Gdy linia jest w stanie normalnym kontroler interpretuje to że zasilanie sieciowe w dozorowanym zasilaczu jest obecne, gdy linia jest wyzwolona oznacza to że zasilania sieciowego nie ma. Wejście tego typu może być wykorzystane do podłączenia źródła sygnału który sygnalizuje zanik zasilania sieciowego AC Uwaga: Niezależnie od tego wejścia kontroler PR402 dozoruje obecność napięcia zmiennego dołączonego do jego zacisków AC
06	Dozór stanu akumulatora	Stały	Gdy linia jest w stanie normalnym kontroler interpretuje to że stan akumulatora rezerwowego w dozorowanym zasilaczu jest właściwy, gdy linia jest wyzwolona oznacza to że stan tego akumulatora jest niezadowalający. Wejście tego typu może być wykorzystane do podłączenia sygnału elektrycznego lub styku który sygnalizuje niski stan lub awarię akumulatora rezerwowego

			Uwaga: Niezależnie od tej linii kontroler PR402 dozoruje stan akumulatora rezerwowego dołączonego do zacisków AC
07	Dzwonek	Stały	Wyzwolenie linii załącza sygnalizację dzwonka na wewnętrznym głośniku i opcjonalnie na linii wyjściowej **[15]: Dzwonek**
08	TAMPER	Chwilowy	Wyzwolenie linii jest interpretowane jako naruszenie obwodu antysabotażowego i powoduje załączenie flagi systemowej TAMPER
09	WŁAMANIE	Chwilowy	Wyzwolenie linii jest interpretowane jako zadziałanie 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 czytnik nie może być uzbrojony.
14	Zwolnij drzwi - klucz stały	Stały	Przez cały czas jak linia jest wyzwolona kontroler bezwarunkowo odblokowuje drzwi tzn. aktywuje wyjście sterujące elementem wykonawczym
46	Losowa kontrola - potwierdzenie	Stały	Wyzwolenie linii powoduje skasowanie sygnalizacji żądania losowej kontroli użytkownika. Linia jest wykorzystywana tylko przez załączonej opcji: Losowa kontrola użytkownika wymaga potwierdzenia
48	Wybierz tryb RCP z klawiatury - zmiana trwała	Chwilowy	Wyzwolenie linii powoduje trwałe przełączenie kontrolera do trybu RCP wskazanego przez trzy cyfry wprowadzone z klawiatury kontrolera. Nowy tryb RCP trwa do momentu wystąpienia kolejnego zdarzenia które zmieni tryb RCP. Zmiana trybu RCP dotyczy zdarzeń rejestrowanych na terminalu ID1
49	Wybierz tryb RCP z klawiatury - zmiana chwilowa	Chwilowy	Wyzwolenie linii powoduje chwilowe przełączenie kontrolera do trybu RCP wskazanego przez trzy cyfry wprowadzone z klawiatury kontrolera. Nowy tryb RCP trwa do momentu najbliższego logowania lecz nie dłużej niż 8 sekund. Zmiana trybu RCP dotyczy zdarzeń rejestrowanych na terminalu ID1
50	Następny tryb RCP - zmiana trwała	Chwilowy	Wyzwolenie linii powoduje trwałe przełączenie kontrolera do następnego z dostępnych trybów RCP używanych w systemie. Nowy tryb RCP trwa do momentu wystąpienia kolejnego zdarzenia które zmieni tryb RCP na kontrolerze. Zmiana trybu RCP dotyczy zdarzeń rejestrowanych na terminalu ID1. Ten typ wejścia występuje tylko na kontrolerze PR602LCD
51	Następny tryb RCP - zmiana chwilowa	Chwilowy	Wyzwolenie linii powoduje chwilowe przełączenie kontrolera do następnego z dostępnych trybów RCP używanych w systemie. Nowy tryb RCP trwa do momentu najbliższego logowania użytkownika lecz nie dłużej niż 8 sekund. Zmiana dotyczy zdarzeń rejestrowanych na terminalu ID1. Ten typ wejścia

			występuje tylko na kontrolerze PR602LCD
56	Ustaw predefiniowany tryb RCP – zmiana trwała	Chwilowy	Wyzwolenie tego wejścia przełącza kontroler w nowy tryb RCP wcześniej zadeklarowany dla tej linii wejściowej. Nowy tryb RCP obowiązuje przez nieograniczony czas tzn. aż do momentu wystąpienia kolejnego zdarzenia które go zmieni. Każda linia wejściowa może ustawiać inny tryb RCP. Zmiana trybu RCP dotyczy zdarzeń rejestrowanych na terminalu ID1
57	Ustaw predefiniowany tryb RCP – zmiana chwilowa	Chwilowy	Wyzwolenie tego wejścia przełącza kontroler w nowy tryb RCP wcześniej zadeklarowany dla tej linii wejściowej. Nowy tryb RCP obowiązuje do momentu najbliższego logowania użytkownika lecz nie dłużej niż 8 sekund. Każda linia wejściowa może ustawiać inny tryb RCP wcześniej dla niej zdefiniowany. Zmiana trybu RCP dotyczy zdarzeń rejestrowanych na terminalu ID1
58	Załącz zwłokę czasową przed samouzbrojeniem	Chwilowy	Wyzwolenie linii załącza **Dodatkową zwłokę czasową przed uzbrojeniem**. Wyzwalając tą linię można opóźniać moment planowanego uzbrojenia które wynika z działania harmonogramu czasowego (Harmonogram Przezbrajania)
59	Kasuj zwłokę czasową przed samouzbrojeniem	Chwilowy	Wyzwolenie linii kasuje zwłokę czasową przed samouzbrojeniem – kontroler natychmiast podejmuje próbę samouzbrojenia
60	Zeruj Rejestr APB	Chwilowy	Wyzwolenie linii zeruje Rejestr APB, wszystkim użytkownikom systemu zostaje nadany Status APB: Niezalogowany
61	Przezbrajanie - klucz chwilowy	Chwilowy	Wyzwolenie linii powoduje zmianę aktualnego stanu uzbrojenia kontrolera
62	Ustaw wyjścia na modułach XM-8	Chwilowy	Wyzwolenie linii załącza wszystkie wyjścia na modułach XM-8 dołączonych do kontrolera
63	Kasuj wyjścia na modułach XM-8	Chwilowy	Wyzwolenie linii wyłącza wszystkie wyjścia na modułach 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: Otwarte
66	Ustaw drzwi w tryb War. Odblokowane	Chwilowy	Wyzwolenie linii ustawia tryb drzwi: Warunkowo Otwarte
67	Ustaw tryb drzwi Zablokowane	Chwilowy	Wyzwolenie linii ustawia tryb drzwi: Zamknięte
68	Ustaw flagę ŚWIATŁO	Chwilowy	Wyzwolenie linii załącza flagę ŚWIATŁO
69	Kasuj flagę ŚWIATŁO	Chwilowy	Wyzwolenie linii wyłącza flagę ŚWIATŁO
70	Przełącz flagę ŚWIATŁO	Chwilowy	Wyzwolenie linii przełącza flagę ŚWIATŁO do stanu przeciwnego

71	Ustaw flagę AUX1	Chwilowy	Wyzwolenie linii załącza flagę AUX1
72	Kasuj flagę AUX1	Chwilowy	Wyzwolenie linii wyłącza flagę AUX1
73	Przełącz flagę AUX1	Chwilowy	Wyzwolenie linii przełącza flagę AUX1 do stanu przeciwnego
74	Ustaw flagę AUX2	Chwilowy	Wyzwolenie linii załącza flagę AUX2
75	Kasuj flagę AUX2	Chwilowy	Wyzwolenie linii wyłącza flagę AUX2
76	Przełącz flagę AUX2	Chwilowy	Wyzwolenie linii przełącza flagę AUX2 do stanu przeciwnego
78	Ustaw tryb Rozbrojony - klucz chwilowy	Chwilowy	Wyzwolenie linii przełącza kontroler do trybu rozbrojenia
79	Ustaw tryb Uzbrojony - klucz chwilowy	Chwilowy	Wyzwolenie linii przełącza 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

Linie Wyjściowe

Kontroler PR402 posiada dwa wyjścia tranzystorowe (IO1 i IO2) oraz dwa wyjścia przekaźnikowe (REL1 i REL2) pozostałe kontrolery serii PRxx2 posiadają tylko jedno wyjście przekaźnikowe REL1 i dwa tranzystorowe (IO1 i IO2). Wszystkie wyjścia są liniami o programowalnej funkcji. Wyjścia przekaźnikowe REL1 i REL2 udostępniają po jednym izolowanym styku NO/NC/COM i obciążalności 1.5A/24V (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 15V DC. Linie tranzystorowe posiadają wewnętrzne zabezpieczenia które automatycznie wyłączają linie po przekroczeniu dopuszczalnego prądu.

Tabela nr 10: Linie Wyjściowe

Kod	Funkcja	Opis
00	Tryb Rozbrojony	Gdy kontroler jest uzbrojony linia ta jest wyłączona, gdy kontroler jest rozbrojony linia ta jest załączona

08	Wyjście sterowane z PC	Linia jest sterowana wyłącznie z poziomu komend wydawanych z programu PR Master
09	Czas na wejście	Wyjście jest załączone przez cały czas jak kontroler jest w trakcie odliczania **Czasu na wejście**
10	Status drzwi	Wyjście to przechodzi do stanu załączenia w momencie otwarcia drzwi i pozostaje w tym stanie tak długo jak drzwi pozostają otwarte co w praktyce oznacza że powtarza stan czujnika otwarcia
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 zdefiniowany dla tego wejścia harmonogram czasowy przy czym przedziały *Od…Do…* wskazują kiedy linia ma być załączona
13	Harmonogram czasowy + komenda zdalna z PC	Działa jaki linia [12] dodatkowo może być sterowana komendami z poziomu programu PR Master. Obie metody sterowania są równoprawne i mogą być stosowane współbieżnie
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 (triod) lub sterowania przejściem dwukierunkowym wtedy wskazuje ono kierunek przejścia
15	Dzwonek	Wyjście jest załączane na czas 2 sekund w momencie wystąpienia sygnalizacji stanu Dzwonek. Sygnalizację dzwonka można wyzwolić przy pomocy klawisza funkcyjnego bądź z linii wejściowej
16	Pomieszczenie nie jest puste	Wyjście załącza się w momencie wejścia pierwszej osoby do nadzorowanego pomieszczenia 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 osiągnie limit. Wyjście zostaje wyłączone gdy liczba osób wewnątrz pomieszczenia spadnie poniżej zdefiniowanego maksimum
18	Drzwi - Tryb Normalny	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Normalny
19	Drzwi - Tryb Odblokowane	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Odblokowane
20	Drzwi - Tryb War. Odblokowane	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: War. Odblokowane
21	Drzwi - Tryb 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
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 dowolnym z podłączonych do niego czytników. 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 Clock & Data
25	Impuls na rozbrojenie	Wyjście jest wyzwalane na czas ok. 2s za każdym razem kiedy kontroler przejdzie do stanu rozbrojenia
26	Impuls na uzbrojenie	Wyjście jest wyzwalane na czas ok. 2s za każdym razem kiedy kontroler przejdzie do stanu uzbrojenia
27	Żądanie uzbrojenia	Wyjście załącza się na czas ok.2 s każdorazowo gdy kontroler podejmie próbę przejścia do stanu uzbrojenia. Aby wyjście się załączyło wystarczy sama próba uzbrojenia kontrolera, a nie fakt uzbrojenia
28	WEJŚCIE SIŁOWE	Wyjście powtarza stan flagi WEJSCIE SIŁOWE. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
29	PREALARM	Wyjście powtarza stan flagi PREALARM. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
30	DRZWI OTWARTE	Wyjście powtarza stan flagi DRZWI OTWARTE. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
31	Gong	Wyjście załącza się na czas ok. 2s każdorazowo gdy kontroler rozpozna że drzwi zostały otwarte
32	Naruszenie APB	Wyjście załącza się na czas około 2s w momencie naruszenia zasad APB
33	Alert przed samouzbrojeniem - wyjście niemodulowane	Wyjście przechodzi do stanu załączenia gdy do momentu samouzbrojenia pozostało tyle czasu ile wskazuje tajmer **Alert przed samouzbrojeniem**, wyjście zostaje wyłączne z chwilą gdy czas wskazywany przez tajmer się skończy i kontroler przejdzie do stanu uzbrojenia
34	Alert przed samouzbrojeniem - wyjście modulowane	Jak wyżej z tą różnicą że wyjście jest załączane impulsowo wg schematu: dwa impulsy powtarzane co ok. 8 s.
35	Tryb Uzbrojony	Gdy kontroler jest rozbrojony linia ta jest wyłączona, gdy kontroler jest uzbrojony linia ta jest załączona
39	Żądanie losowej kontroli	Wyjście to przechodzi na 2s do stanu załączenia w momencie wytypowania osoby do kontroli. Jeśli jednak załączona jest

		opcja **Losowa kontrola użytkownika wymaga potwierdzenia** to wyjście pozostaje załączone do momentu skasowania sygnalizacji żądania kontroli za pomocą linii wyjściowej lub klawisza funkcyjnego ([46]: Losowa kontrola – potwierdzenie)
64	ŚWIATŁO	Wyjście powtarza stan flagi ŚWIATŁO. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
65	TAMPER	Wyjście powtarza stan flagi TAMPER. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
66	AUX1	Wyjście powtarza stan flagi AUX1. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
67	AUX2	Wyjście powtarza stan flagi AUX2. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
68	WŁAMANIE	Wyjście powtarza stan flagi WŁAMANIE. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone
84	Tryb Karta lub PIN dla terminala ID0	Wyjście jest załączone przez cały czas jak na terminalu ID0 obowiązuje tryb Karta lub PIN
85	Tryb Tylko Karta dla terminala ID0	Wyjście jest załączone przez cały czas jak na terminalu ID0 obowiązuje tryb Tylko Karta
86	Tryb Tylko PIN dla terminala ID0	Wyjście jest załączone przez cały czas jak na terminalu ID0 obowiązuje tryb Tylko PIN
87	Tryb Karta i PIN dla terminala ID0	Wyjście jest załączone przez cały czas jak na terminalu ID0 obowiązuje tryb Karta i PIN
88	Tryb Karta lub PIN dla terminala ID1	Wyjście jest załączone przez cały czas jak na terminalu ID1 obowiązuje tryb Karta lub PIN
89	Tryb Tylko Karta dla terminala ID1	Wyjście jest załączone przez cały czas jak na terminalu ID1 obowiązuje tryb Tylko Karta
90	Tryb Tylko PIN dla terminala ID1	Wyjście jest załączone przez cały czas jak na terminalu ID1 obowiązuje tryb Tylko PIN
91	Tryb Karta i PIN dla terminala ID1	Wyjście jest załączone przez cały czas jak na terminalu ID1 obowiązuje tryb Karta i PIN
97	Zamek drzwi - wejście	Wyjście jest wyzwalane na czas określony przez parametr **Czas na wejście** 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 - wyjście	Wyjście jest wyzwalane na czas określony przez parametr **Czas na wejście** 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** bez względu na to z którego terminala został przyznany dostęp. Wyjście przeznaczone jest do sterowania elementem wykonawczym odblokowującym drzwi
256	Alarm drzwi	Wyjście sygnalizuje wystąpienie stanu: Alarmu Drzwi Uwaga: Alarm Drzwi jest funkcją zespoloną składającą się z trzech typów alarmów szczegółowych: DRZWI OWTARTE, 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

Harmonogramy Czasowe

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...** zdefiniowanych z dokładnością do 1 minuty. W systemie RACS rozróżnia się następujące typy harmonogramów czasowych:

- Harmonogram Ogólnego Przeznaczenia
- Harmonogram Trybu RCP
- Harmonogramy Trybu Drzwi
- Harmonogramy Zerowania APB

Harmonogramy Ogólnego Przeznaczenia - Harmonogramy Ogólnego Przeznaczenia mogą być stosowane do wielu różnych funkcji i opcji dostępnych w kontrolerze, niemniej najczęściej znajdują zastosowanie w odniesieniu do definiowania praw dostępu.

Harmonogramy Trybu RCP - służą do automatycznej zmiany trybu RCP na terminalu ID1.

Harmonogramy Trybu Drzwi - służą do automatycznej zmiany trybu drzwi.

Harmonogramy Zerowania APB - wskazują momenty czasu kiedy kontroler samoczynnie wyzeruje Rejestr APB.

Ustawienia Świąteczne

Ustawienia Świąteczne 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 można zdefiniować cztery typy harmonogramów zastępczych: H1, H2, H3 i H4. Definiowanie święta polega na wskazaniu daty święta oraz konkretnego harmonogramu zastępczego (H1-H4) który będzie w danym dniu obowiązywał. Kontrolery PRxx2 umożliwiają zdefiniowanie 120 dni świątecznych.

Warunki Dodatkowe

Warunek Dodatkowy wskazuje na dodatkową okoliczność lub stan który musi wystąpić aby dana funkcja/opcja dla której dany warunek jest przypisany mogła wystąpić. Dla przykładu jeśli do klawisza F1 zostanie zdefiniowany warunek dodatkowy **Zezwól gdy kontroler uzbrojony** to klawisz ten będzie działał tylko wtedy gdy kontroler będzie w stanie uzbrojenia. Warunek dodatkowy można zdefiniować dla wielu funkcji i opcji kontrolera jak również dla linii wejściowych i wyjściowych. Gdy warunek dodatkowy zdefiniowany dla linii wejściowej nie jest spełniony to linia taka nie jest obsługiwana; podobnie, gdy warunek dodatkowy dla linii wyjściowej nie jest spełniony to linia taka pozostaje w stanie wyłączenia.

Tabela nr 11: Warunki Dodatkowe	
Kod	**Opis**
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

Rejestracja Czasu Pracy (RCP)

System RACS nie jest systemem przeznaczonym samodzielnie do rozliczania czasu pracy niemniej może rejestrować zdarzenia które później zostaną wyeksportowane do innego, dedykowanego do tego celu programu, który dokona szczegółowych rozliczeń czasu pracy zgodnie z obowiązującymi w danym kraju zasadami lub wymogami użytkownika.

W systemie RACS każdy punkt identyfikacji (czytnik) może być jednocześnie punktem rejestracji zdarzeń dla systemu RCP. Kontroler PRxx2 udostępnia dwa punkty identyfikacji (terminal ID0 i ID1), każdy z tych punktów może rejestrować zdarzenia o odmiennym trybie RCP. Tryb RCP dla czytnika ID0 jest ustawiony na stałe i nie może być zmieniany w trakcie pracy, tryb RCP czytnika ID1 może być dynamicznie zmieniany na szereg sposobów.

Uwaga: W przypadku załączenia opcji **Term.ID0 przyjmuje ten sam tryb RCP co term.ID1** możliwe jest również dynamiczne sterowanie trybem RCP dla terminala ID0.

System RACS 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 każdy tryb RCP może posiadać dodatkowo dwa parametry które doprecyzowują jego znaczenie. Znaczenie tych parametrów jest dowolne i może być definiowane przez administratora systemu.

Tryby RCP o kodach 0-50 są zarezerwowane i należą w systemie RACS do grupy predefiniowanych trybów RCP, tryby o kodach 50-255 mogą być swobodnie definiowane przez administratora systemu. W systemie RACS istnieją cztery predefiniowane tryby RCP:

- WEJŚCIE (Kod 000)
- WYJŚCIE (Kod 016)
- WYJŚCIE SŁUŻBOWE (Kod 017)
- BRAK (Kod 032) - zdarzenia oznaczone tym trybem 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 (polecenie Eksport do RCP w oknie Historia zdarzeń) a następnie zaimportować je do właściwego programu.

Sterowanie trybem RCP

Jak wspomniano wcześniej, tryb RCP dla terminala ID0 jest przypisany na stałe natomiast tryb RCP terminala ID1 może być dynamiczne zmieniany w trakcie pracy systemu. 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 sposoby sterowania trybem RCP:

- Z linii wejściowej
- Z klawisza funkcyjnego
- Z harmonogramu czasowego (Harmonogram Trybu RCP)
- Z klawiatury czytnika

Możliwe jest współbieżne stosowanie różnych mechanizmów sterowania trybem RCP.

Tabela nr 12: Metody zmiany trybu RCP		
Metoda	**Opcja**	**Działanie**
Sterowanie z linii wejściowych	[48]: Wybierz tryb RCP z klawiatury – zmiana trwała	W następstwie wyzwolenia tej linii kontroler 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 kontroler 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 i odnosi się do zdarzeń pochodzących z terminala ID1, (NNN=000-255)
	[50]: Następny tryb RCP – zmiana trwała	W następstwie wyzwolenia tej linii kontroler przechodzi do kolejnego trybu RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter trwały. Metoda ta jest dostępna jedynie na kontrolerze PR602LCD
	[51]: Następny tryb RCP – zmiana chwilowa	W następstwie wyzwolenia tej linii kontroler przechodzi do kolejnego z trybów RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1. Metoda ta jest dostępna jedynie na kontrolerze PR602LCD
	[56]: Ustaw predefiniowany tryb RCP – zmiana trwała	W następstwie wyzwolenia tej linii kontroler przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej 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 kontroler przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej, zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1
Sterowanie za pomocą klawiszy funkcyjnych	[50]: Następny tryb RCP – zmiana trwała	W następstwie użycia przycisku funkcyjnego kontroler przechodzi do kolejnego z trybów RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1. Funkcja ta jest dostępna tylko na kontrolerze PR602LCD
	[51]: Następny tryb RCP – zmiana chwilowa	W następstwie użycia przycisku funkcyjnego kontroler przechodzi do kolejnego z trybów RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter chwilowy i odnosi się do

		zdarzeń pochodzących z terminala ID1. Funkcja ta jest dostępna tylko na kontrolerze PR602LCD
	[56]: Predefiniowany tryb RCP – zmiana trwała	W następstwie użycia przycisku funkcyjnego kontroler przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej, zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1
	[57]: Predefiniowany tryb RCP – zmiana chwilowa	W następstwie użycia przycisku funkcyjnego kontroler przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej, zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1
Sterowanie za pomocą funkcji użytkownika (komend z klawiatury)	F16: Ustaw tryb RCP o kodzie [NNN] – zmiana trwała	W następstwie użycia tej funkcji kontroler przechodzi do trybu RCP wskazanego przez cyfry [NNN], zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1, (NNN=000-255)
	F17: Ustaw tryb RCP o kodzie [NNN] – zmiana chwilowa	W następstwie użycia tej funkcji kontroler przechodzi do trybu RCP wskazanego przez cyfry [NNN], zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1, (NNN=000-255)
Inne metody	Z klawiatury za pomocą sekwencji klawiszy [*][#] Uwaga: Mechanizm ten jest dostępny tylko na kontrolerze PR602LCD	Każdorazowo po naciśnięciu sekwencji klawiszy [*][#] kontroler przechodzi do kolejnego trybu RCP spośród trybów zdefiniowanych w danym systemie. Sekwencje [*][#] można powtarzać aż do mementu gdy na wyświetlaczu pojawi się oczekiwany tryb RCP. Zmiana trybu RCP metodą [*][#] może mieć charakter trwały lub chwilowy a decyduje o tym opcja: **Zmiana trybu RCP przez klawisze [*][#]**, nowy tryb RCP odnosi się do zdarzeń pochodzących z terminala ID1. Domyślnie przejście do następnego trybu RCP następuje automatycznie z chwilą naciśnięcia sekwencji [*][#] jednak jeśli zostanie zdefiniowane hasło: **Hasło gdy zmiana trybu RCP metodą [*][#]** to przed przełączeniem do nowego trybu kontroler będzie wymagał podania wcześniej zdefiniowanego hasła. Zastosowanie hasła do zmiany trybu RCP metodą [*][#] umożliwia ograniczenie ilości osób którzy mogą zmieniać tryb RCP metodą [*][#]
	Harmonogram Trybu RCP	Harmonogram ten definiuje przedziały czasowe w których kontroler samoczynnie będzie zmieniał tryb RCP. Harmonogram ten definiuje się dla każdego dnia tygodnia osobno oraz dla dni świątecznych. Zmiana trybu RCP odnosi się do zdarzeń pochodzących z terminala ID1
Uwaga: Wszystkie metody zmiany trybu RCP opisane powyżej odnoszą się wyłącznie do zdarzeń pochodzących z terminala ID1. W kontrolerach PR302, PR302LCD oraz PR602LCD terminal ID1 jest fizycznie zintegrowany z kontrolerem (wbudowany w kontroler) i stanowi z nim jedno urządzenie, w przypadku kontrolera PR402 zarówno terminal ID1 jak i ID0 są czytnikami zewnętrznymi.		

Opcja: Term.ID0 przyjmuje ten sam tryb RCP co term.ID1
PRMaster:/Właściwości kontrolera/Opcje/Sterowanie trybem rejestracji RCP/Term.ID0 przyjmuje ten sam tryb RCP co term.ID1

Załączenie tej opcji powoduje że zdarzenia które wystąpią na terminalu ID0 będą zarejestrowane z tym samym trybem RCP jaki obowiązywał w danej chwili dla terminala ID1. Dzięki tej opcji wszystkie metody sterowania trybem RCP mogą jednocześnie oddziaływać na obydwa punkty identyfikacji tzn. i na terminal ID0 i ID1.

Klawisze Funkcyjne

Klawisze funkcyjne dostępne są na niektórych czytnikach serii PRT jak też na kontrolerze PR602LCD. Kontrolery serii PRxx2 dopuszczają zdefiniowanie do czterech klawiszy funkcyjnych dla każdej strony przejścia. Działanie każdego klawisza funkcyjnego może być indywidualnie oprogramowane do jednej z dostępnych funkcji. Program PR Master dopuszcza oprogramowanie wszystkich czterech klawiszy funkcyjnych dla każdego z terminali (ID0 i ID1) bez względu czy fizycznie istnieją one w danym czytniku czy nie.

Tabela nr 13: Opcje klawiszy funkcyjnych

Opcja	Kod	Opis
Brak funkcji	00	Klawisz funkcyjny, do którego nie przypisano żadnych działań
Zwolnij drzwi	02	Użycie klawisza zwalnia kontrolowane drzwi na identycznych zasadach jak po przyznaniu dostępu
Rejestracja	04	Każde użycie przycisku zostaje rejestrowane w pamięci zdarzeń lecz kontroler nie podejmuje żadnych dodatkowych działań
Losowa kontrola - potwierdzenie	46	Każde użycie klawisza funkcyjnego powoduje zarejestrowanie zdarzenia potwierdzającego wykonanie kontroli wylosowanego użytkownika i skasowanie sygnalizacji jej żądania
WŁAMANIE	09	Użycie klawisza włącza flagę WŁAMANIE
Następny tryb RCP - zmiana trwała	50	W następstwie użycia klawisza funkcyjnego kontroler 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
Następny tryb RCP - zmiana chwilowa	51	W następstwie użycia klawisza funkcyjnego kontroler przechodzi do kolejnego z trybów RCP spośród trybów zdefiniowanych w systemie, zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1. Metoda ta jest dostępna jedynie na kontrolerze PR602LCD
Predefiniowany tryb RCP – zmiana trwała	56	W następstwie użycia klawisza funkcyjnego kontroler przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej, zmiana trybu ma charakter trwały i odnosi się do zdarzeń pochodzących z terminala ID1
Predefiniowany tryb RCP –	57	W następstwie użycia klawisza funkcyjnego kontroler

zmiana chwilowa		przechodzi do trybu RCP który został zdefiniowany indywidualnie dla tej linii wejściowej, zmiana trybu ma charakter chwilowy i odnosi się do zdarzeń pochodzących z terminala ID1
Załącz zwłokę przed samouzbrojeniem	58	Użycie klawisza opóźnia moment samouzbrojenia o dodatkowy czas określony przez parametr: **Dodatkowa zwłoka czasowa przed samouzbrojeniem**
Wyłącz zwłokę przed samouzbrojeniem	59	Użycie klawisza anuluje odliczanie zwłoki czasowej przed samouzbrojeniem
Zeruj Rejestr APB	60	Użycie klawisza zeruje (resetuje) rejestr APB
Zmień stan uzbrojenia - klucz chwilowy	61	Użycie klawisza przezbraja kontroler, użycie klawisza nie implikuje jednak że kontroler zmieni stan a jedynie że dokona próby zmiany swojego stanu uzbrojenia
Zeruj wyjścia na module XM-8	62	Użycie klawisza zeruje wszystkie wyjścia na modułach XM-8 dołączonych do kontrolera
Załącz wyjścia module XM-8	63	Użycie klawisza załącza wszystkie wyjścia na modułach XM-8 dołączonych do kontrolera
Ustaw drzwi w tryb Normalny	64	Użycie klawisza ustawia tryb drzwi: Normalny
Ustaw drzwi w tryb Odblokowane	65	Użycie klawisza ustawia tryb drzwi: Odblokowane
Ustaw drzwi w tryb War. Odblokowane	66	Użycie klawisza ustawia tryb drzwi: Warunkowo Odblokowane
Ustaw drzwi w tryb Zablokowane	67	Użycie klawisza ustawia tryb drzwi: Zablokowane
Załącz flagę ŚWIATŁO	68	Użycie klawisza załącza flagę ŚWIATŁO
Wyłącz flagę ŚWIATŁO	69	Użycie klawisza wyłącza flagę ŚWIATŁO
Przełącz flagę ŚWIATŁO	70	Użycie klawisza przełącza flagę ŚWIATŁO do stanu przeciwnego
Załącz flagę AUX1	71	Użycie klawisza załącza flagę AUX1
Wyłącz flagę AUX1	72	Użycie klawisza wyłącza flagę AUX1
Przełącz flagę AUX1	73	Użycie klawisza przełącza flagę AUX1 do stanu przeciwnego
Załącz flagę AUX2	74	Użycie klawisza załącza flagę AUX2
Wyłącz flagę AUX2	75	Użycie klawisza wyłącza flagę AUX2
Przełącz flagę AUX2	76	Użycie klawisza przełącza flagę AUX2 do stanu przeciwnego
Wyłącz flagi WŁAMANIE+TAMPER	77	Użycie klawisza wyłącza flagi WŁAMANIE oraz TAMPER
Ustaw tryb Rozbrojony	78	Użycie klawisza przełącza kontroler do trybu rozbrojenia
Ustaw tryb Uzbrojony	79	Użycie klawisza przełącza kontroler do trybu uzbrojenia
Ustaw tryb Karta lub PIN dla term.ID0	84	Użycie klawisza ustawia tryb Karta lub PIN dla terminala ID0
Ustaw tryb Tylko Karta dla term.ID0	85	Użycie klawisza ustawia tryb Tylko Karta dla terminala ID0

Ustaw tryb Tylko PIN dla term. ID0	86	Użycie klawisza ustawia tryb Tylko PIN dla terminala ID0
Ustaw tryb Karta i PIN dla term.ID0	87	Użycie klawisza ustawia tryb Karta i PIN dla terminala ID0
Ustaw tryb Karta lub PIN dla term.ID1	88	Użycie klawisza ustawia tryb Karta lub PIN dla terminala ID1
Ustaw tryb Tylko Karta dla term.ID1	89	Użycie klawisza ustawia tryb Tylko Karta dla terminala ID1
Ustaw tryb Tylko PIN dla term.ID1	90	Użycie klawisza ustawia tryb Tylko PIN dla terminala ID1
Ustaw tryb Karta i PIN dla term.ID1	91	Użycie klawisza ustawia tryb Karta i PIN dla terminala ID1
Dzwonek	255	Użycie klawisza powoduje załączenie sygnalizacji dzwonka

Działanie każdego klawisza funkcyjnego może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu. Klawisz funkcyjny działa wtedy gdy zezwala na to harmonogram czasowy przypisany temu klawiszowi oraz gdy spełniony jest warunek dodatkowy dla tego klawisza.

Komendy Klawiaturowe

Kontroler udostępnia możliwość wprowadzania szeregu komend (poleceń) z klawiatury. Prawo do wprowadzania komend może być nadane wszystkim użytkownikom systemu lub tylko wybranym. Stosowanie komendy może wymagać od użytkownika potwierdzenia swojej tożsamości przez zalogowanie się aczkolwiek obowiązek ten może zostać programowo wyłączony (Autoryzacja). Domyślnie kontroler akceptuje komendy wprowadzane zarówno z terminala ID1 jak i ID0 niemniej można w procesie konfiguracji kontrolera wskazać z których czytników (ID0 i/lub iD1) można wprowadzać komendy.

Komendy klawiaturowe mogą być typu *binarnego* lub *parametrycznego*. Komenda binarna nie wymaga podania żadnego dodatkowego parametru (np. komenda **F15: Zeruj Rejestr APB**), komenda typu parametrycznego wymaga od użytkownika wprowadzenia dodatkowych danych które określą szczegółowy sposób jej wykonania (np. komenda **F01: Ustaw datę**).

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.

Zapis [Logowanie] występujący w definicji komend w tabelce zamieszczonej poniżej oznacza, że w miejscu tym należy dokonać logowania użytkownika (Karta i/lub kod PIN) przy czym logowanie jest konieczne tylko wtedy o ile dana funkcja ma załączoną opcję autoryzacji. Żądanie autoryzacji można uaktywnić indywidualnie dla każdej komendy.

W ramach autoryzacji komendy kontroler akceptuje identyfikatory tylko tych użytkowników którym nadano odpowiedni atrybut (patrz: Użytkownicy uprawnieni do wprowadzania komend). Dla każdego kontrolera w systemie można zdefiniować osobną listę użytkowników uprawnionych do wprowadzania komend z klawiatury.

Tabela nr 14: Komendy klawiaturowe	
Komenda	**Opis**
F00: Ustaw adres (numer ID)	[*][0][0][#][Logowanie][nowy adres ID][#] Komenda nadaje nowy numer ID (adres) kontrolerowi, ID=00-99

F01: Ustaw datę	[*][0][1][#][Logowanie][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][#][Logowanie][GG][MM][#] Polecenie ustawia nową godzinę GG: godzina (00-23) MM: Minuta (00-59)
F07: Ustaw drzwi w tryb Normalny	[*][0][7][#][Logowanie] Komenda załącza tryb drzwi Normalny
F08: Ustaw drzwi w tryb Zablokowane	[*][0][8][#][Logowanie] Komenda załącza tryb drzwi Zablokowane
F09: Ustaw drzwi w tryb Odblokowane	[*][0][8][#][Logowanie] Komenda załącza tryb drzwi Odblokowane
F10: Ustaw drzwi w tryb War. Odblokowane	[*][1][0][#][Logowanie] Komenda załącza tryb drzwi Warunkowo Odblokowane
F11: Ustaw kontroler w tryb Rozbrojony	[*][1][1][#][Logowanie] Komenda przełącza kontroler do trybu Rozbrojony
F12: Ustaw kontroler w tryb Uzbrojony	[*][1][2][#][Logowanie] Komenda przełącza kontroler do trybu Uzbrojony
F13: Zmień stan uzbrojenia (przezbrój kontroler	[*][1][3][#][Logowanie] Komenda zmienia aktualny stan uzbrojenia
F14: Restartuj kontroler	[*][1][4][#][Logowanie] Komenda powoduje restart kontrolera
F15: Zeruj Rejestr APB	[*][1][5][#][Logowanie] Komenda powoduje inicjalizację (wyzerowanie) Rejestru APB na kontrolerze
F16: Ustaw tryb RCP o kodzie NNN - zmiana trwała	[*][1][6][#][Logowanie][NNN][#] Komenda przełącza terminal ID1 do trybu RCP wskazanego przez wartość NNN=000-254, zmiana trybu RCP ma charakter trwały i odnosi się do terminala ID1
F17: Ustaw tryb RCP o kodzie NNN - zmiana chwilowa	[*][1][7][#][Logowanie][NNN][#] Komenda przełącza terminal ID1 do trybu RCP wskazanego przez wartość NNN=000-254, zmiana trybu

	RCP ma charakter chwilowy i odnosi się do terminala ID1
F18: Załącz dodatkową zwłokę czasową przed samouzbrojeniem	[*][1][8][#][Logowanie] Komenda przesuwa moment samouzbrojenia o czas określony przez parametr: **Dodatkowa zwłoka czasowa przed samouzbrojeniem**, poprzednie zwłoki czasowe zostają unieważnione
F19: Załącz definiowane opóźnienie NNN min. przed samouzbrojeniem	[*][1][9][#][Logowanie][NNN][#] Komenda przesuwa samouzbrojenie o czas NNN minut, poprzednie zwłoki czasowe zostają unieważnione
F20: Wyłącz opóźnienie przed samouzbrojeniem	[*][2][0][#][Logowanie] Komenda kasuje zwłokę czasową przed samouzbrojeniem (o ile jest ona w toku)
F21: Załącz flagę ŚWIATŁO	[*][2][1][#][Logowanie] Komenda załącza flagę ŚWIATŁO
F22: Wyłącz flagę ŚWIATŁO	[*][2][2][#][Logowanie] Komenda wyłącza flagę ŚWIATŁO
F23: Przełącz flagę ŚWIATŁO	[*][2][3][#][Logowanie] Komenda przełącza flagę ŚWIATŁO to stanu przeciwnego
F24: Załącz flagę AUX1	[*][2][4][#][Logowanie] Komenda załącza flagę ŚWIATŁO
F25: Wyłącz flagę AUX1	[*][2][5][#][Logowanie] Komenda wyłącza flagę AUX1
F26: Przełącz flagę AUX1	[*][2][6][#][Logowanie] Komenda przełącza flagę AUX1 to stanu przeciwnego
F27: Załącz flagę AUX2	[*][2][7][#][Logowanie] Komenda przełącza flagę AUX2
F28: Wyłącz flagę AUX2	[*][2][8][#][Logowanie] Komenda wyłącza flagę AUX2
F29: Przełącz flagę AUX2	[*][2][9][#][Logowanie] Komenda przełącza flagę AUX2 to stanu przeciwnego
F30: Załącz flagę WŁAMANIE	[*][3][0][#][Logowanie] Komenda załącza flagę WŁAMANIE
F31: Wyłącz flagi WŁAMANIE oraz TAMPER	[*][3][1][#][Logowanie] Komenda wyłącza flagi WŁAMANIE oraz TAMPER
F32: Ustaw tryb identyfikacji dla term.ID1	[*][3][2][#][Logowanie][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][#][Logowanie][N][#] Komenda przełącza terminal ID0 do trybu identyfikacji wskazanego przez cyfrę N=0..3, kodowanie N jak dla komendy F32

Sygnały Akustyczne i Optyczne

Sygnały optyczne

W kontrolerach PRxx2 sygnalizacja optyczna jest realizowana na wskaźnikach LED dostępnych na terminalach ID1/ID0. W kontrolerze PR402 sygnalizacja optyczna jest realizowana równolegle na wskaźnikach LED dostępnych na płycie kontrolera.

Tabela nr 15: Wskaźniki LED na terminalach ID0 i ID1

Nazwa	Kolor	Funkcja
LED STAN	Wskaźnik dwukolorowy czerwono-zielony	Świeci na czerwono gdy kontroler jest w trybie uzbrojenia lub na zielono gdy jest w trybie rozbrojenia
LED OTWARTE	Wskaźnik zielony	Wskaźnik ten świeci przez cały czas kiedy drzwi są odblokowane, gdy pulsuje oznacza że kontroler oczekuje na dalszy ciąg logowania (odczyt karty lub wprowadzenie kodu PIN)
LED SYSTEM	Wskaźnik pomarańczowy	Pulsowanie sygnalizuje że kontroler oczekuje na następną część polecenia lub komendy. Gdy zapalony na stałe sygnalizuje problemy techniczne. W przypadku wykrycia technicznych problemów kontroler zatrzymuje swoje działanie do czasu ich rozwiązania.

Tabela nr 16: Wskaźniki LED na płycie PR402

Nazwa	Funkcja
LED1: Ładowanie	Świecenie diody oznacza ładowanie rezerwowej baterii dołączonej do kontrolera. Jeśli dioda jest wyłączona oznacza to że bateria jest naładowana lub jej nie ma
LED2: Tryb Rozbrojony	Kontroler jest w stanie rozbrojenia
LED3: Tryb Uzbrojony	Kontroler jest w stanie uzbrojenia
LED 4: Otwarte	Wskaźnik ten świeci przez cały czas kiedy drzwi są odblokowane, gdy pulsuje oznacza że kontroler oczekuje na dalszy ciąg logowania (odczyt karty lub wprowadzenie kodu PIN)
LED 5: System	Pulsowanie sygnalizuje że kontroler oczekuje na następną część polecenia lub komendy. Gdy zapalony na stałe sygnalizuje problemy techniczne. W przypadku

	wykrycia technicznych problemów kontroler zatrzymuje swoje działanie do czasu ich rozwiązania.
LED 6: Głośnik	Jest zapalany w takt załączania sygnału akustycznego na głośniku

Sygnały akustyczne
W kontrolerach PR302 i PR602LCD sygnały akustyczne są generowane przez wewnętrzny głośnik kontrolera oraz na zewnętrznych czytnikach serii PRT. W kontrolerze PR402 sygnalizacja akustyczna jest realizowana jedynie na zewnętrznych czytnikach serii PRT. Opcjonalnie, we wszystkich typach kontrolerów serii PRxx2 sygnalizacja akustyczna może być realizowana na zewnętrznym głośniku dołączonym do linii wyjściowej **[23]: Głośnik zewnętrzny**. Należy zwrócić uwagę że głośnik taki powinien posiadać wbudowany generator akustyczny i być przystosowany do zasilania z napięcia stałego 12V.

Tabela nr 17: Sygnały akustyczne

Rodzaj	**Znaczenie**
Jeden krótki sygnał (1 x BEEP)	Odczyt karty lub naciśnięcie klawisza
Dwa krótkie sygnały (2 x BEEP)	Sygnał zachęty, kontroler oczekuje na dalszą część komendy
Trzy krótkie sygnały (3 x BEEP)	Sygnał OK, polecenie wykonane prawidłowo
Jeden długi sygnał	Nieznana karta lub nieznany PIN kod
Dwa długie sygnały	Karta/PIN poprawny lecz w danej chwili brak uprawnienia do wejścia
Sygnał długi powtarzany cyklicznie	Uszkodzenie danych w pamięci, wymagany jest Reset Pamięci

Kontakt
Roger sp. j.
82-416 Gościszewo
Gościszewo 59
Tel.: 055 272 0132
Fax: 055 272 0133
e-mail: biuro@roger.pl