Roger Access Control System

Kontrolery serii PRxx1
Opis funkcjonalny oraz programowanie

Oprogramowanie firmowe:
Wersja dokumentu: Rev.C
Dokument dotyczy następujących typów urządzeń:
PR311SE, PR311SE-BK, PR611, PR621, PR411DR

CE

Spis treści:

I. DEFINICJE I KONWENCJE

1.1 Stosowane pojęcia

Kontroler dostępu (ang. ACU – Access Control Unit)	Urządzenie logiczne najczęściej mikroprocesorowe, którego zadaniem jest elektroniczna weryfikacja osób i sterowanie dostępem do pomieszczenia.
Zintegrowany system kontroli dostępu (ang. IACS – Integrated Access Control System)	System kontroli dostępu złożony z wielu kontrolerów połączonych ze sobą magistralą komunikacyjną, która umożliwia monitorowanie systemu w trybie online a także realizację pewnych złożonych funkcji sterowania wymagających wymiany informacji pomiędzy urządzeniami podłączonymi do magistrali.
System kontroli dostępu RACS (ang. RACS - Roger Access Control System)	System kontroli dostępu składający się z kontrolerów dostępu serii PR (Roger) i zarządzanych przez program PR Master (Roger).
Centrala systemu KD	Specjalizowany kontroler pełniący pewne funkcje zarządzające w Zintegrowanym Systemie Kontroli Dostępu (ang. IACS). Funkcja centrali KD zależy od tego, z jakimi urządzeniami ono współpracuje. W odniesieniu do kontrolerów serii PRxx1 centrala (CPR32-SE) 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, który dla odróżnienia od innych standardów tego typu jest oznaczany jako RACS Clock & Data. Standard RACS Clock & Data jest protokołem adresowalnym (adresy ID=0-15) i umożliwia transmisję danych na odległość do 150m przy wykorzystaniu dowolnych kabli sygnałowych.
Magistrala komunikacyjna	Struktura elektryczna złożona z dwóch przewodów elektrycznych, która jest wykorzystywana do komunikacji pomiędzy różnymi podłączonymi do niej urządzeniami. System RACS wykorzystuje magistralę RS485.
Tryb Drzwi	Sposób sterowania elementem wykonawczym odpowiedzialnym za blokowanie/odblokowywanie drzwi. Kontroler PRxx1 udostępnia następujące Tryby Drzwi: Normalny, Odblokowane, Warunkowo Odblokowane oraz Zablokowane.
Element wykonawczy lub zamek drzwiowy	Urządzenie elektryczne, które zwalnia drzwi umożliwiając dostęp do kontrolowanego pomieszczenia bądź obszaru. Zwykle jest to elektro-zaczep lub zwora magnetyczna.

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

Flagi Systemowe	Stany logiczne w pamięci kontrolera, które reprezentują pewne określone zjawiska lub stany urządzenia.
Licznik (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.
Strefa Alarmowa	Jest to wybrany obszar systemu kontroli dostępu obejmujący grupę kontrolerów współbieżnie zmieniających swój aktualny stan uzbrojenia/rozbrojenia.
Strefa anti-passback (Strefa APB)	Jest to wybrany obszar systemu kontroli dostępu, do którego dostęp jest nadzorowany przez wiele punktów identyfikacji (czytników). Użytkownik jest zmuszony do naprzemiennej identyfikacji na wejściu i wyjściu ze strefy APB.

1.2 Przyjęta konwencja

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

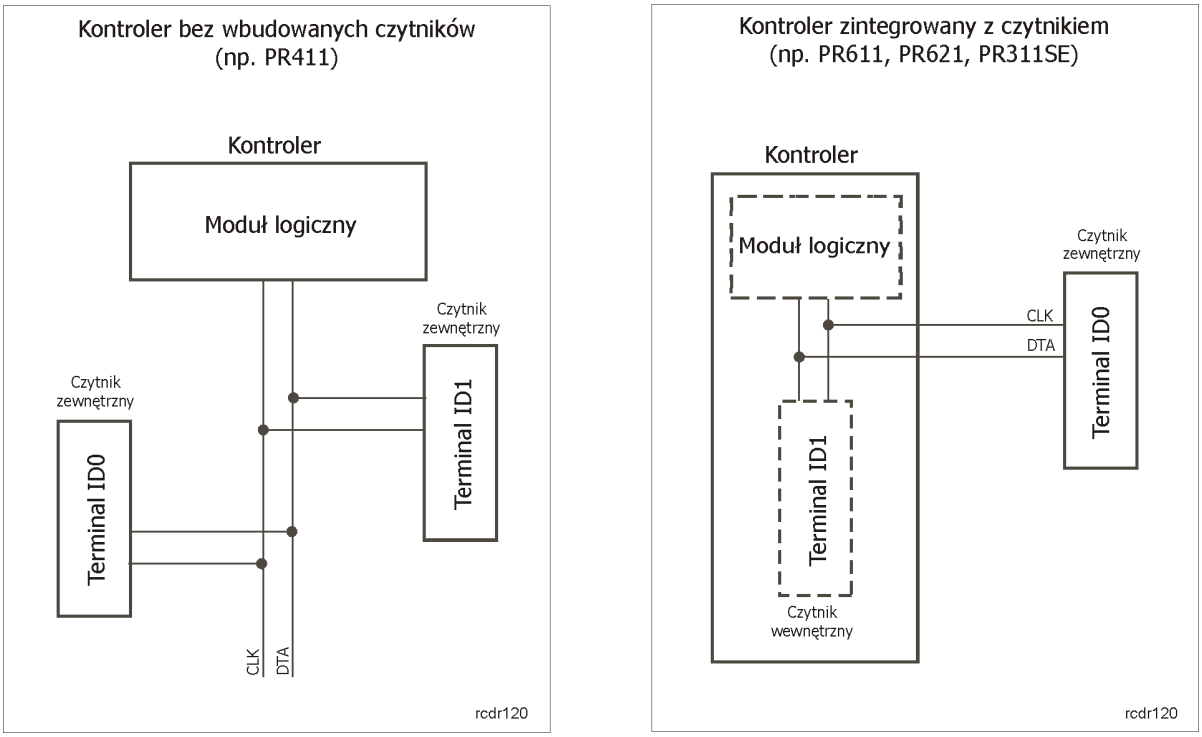
II. CHARAKTERYSTYKA OGÓLNA

2.1 Wstęp

Niniejsza instrukcja nie może być wykorzystywana w odniesieniu do starszych typów kontrolerów: PR401, PR301 oraz PR201. Kontroler PR411DR jest wyposażony w obudowę z tworzywa sztucznego przystosowaną do montażu na standardowej szynie DIN 35mm. Pozostałe kontrolery serii PRxx1 są przystosowane do montażu naściennego.

2.2 Budowa i przeznaczenie

Kontrolery serii PRxx1 są kontrolerami dostępu przeznaczonymi do dozoru jednego przejścia, przy czym może ono być kontrolowane po jednej lub po dwóch stronach. Kontroler serii PRxx1 obsługuje logicznie dwa punkty identyfikacji (czytniki) zwane odpowiednio Terminalem ID0 oraz Terminalem ID1. Kontrolery PR311SE, PR311SE-BK, PR611 oraz PR621 posiadają wbudowany czytnik, który jest logicznie traktowany jako Terminal ID1, natomiast kontroler PR411DR nie posiada wbudowanego czytnika i współpracuje wyłącznie z czytnikami zewnętrznymi przy czym mogą to być czytniki pracujące w standardzie RACS (terminale serii PRT) lub czytniki z interfejsami Wiegand 26-66bit.



Rys. 1 Ogólna koncepcja współpracy kontrolera z czytnikiem/czytnikami

W kontrolerze PRxx1 można zarejestrować do 1000 użytkowników standardowych oraz 8 użytkowników specjalnych, tzw. Gości. W systemie RACS każdy użytkownik posiada swój unikalny numer ID oraz może posiadać kartę i/lub kod PIN.
Przesyłanie oprogramowania do kontrolera odbywa się za pośrednictwem magistrali komunikacyjnej RS485 i nie wymaga demontażu urządzenia z miejsca jego zainstalowania.
Kontroler serii PRxx1 może działać całkowicie samodzielnie (Tryb autonomiczny) lub być elementem zintegrowanego systemu kontroli dostępu wyposażonego w centralę CPR32-SE (Tryb Sieciowy).
Kontrolery PRxx1 mogą być programowane manualnie lub zdalnie za pomocą komputera PC. Programowanie manualne można przeprowadzić lokalnie z poziomu klawiatury (PR311SE, PR611) lub z poziomu dodatkowego czytnika serii PRT dołączonego do kontrolera (czytnik ten powinien posiadać klawiaturę i być skonfigurowany do trybu RACS o adresie ID0 – patrz IV. Programowanie).

Później, do programowania urządzenia można używać tak zwanych Kart Funkcyjnych.
Programowanie zdalne można przeprowadzić z poziomu komputera PC z zainstalowanym programem PR Master (Roger)
Komunikacja z pojedynczymi kontrolerami jak też zarządzanie systemem KD wymaga zastosowania odpowiedniego interfejsu komunikacyjnego np.:

- RUD-1 (USB <-> RS485),
- UT-2 (RS-232 <-> RS485),
- UT-2USB (USB <-> RS485),
- UT-4 (RS232, RS422, RS485 <-> Ethernet).

Tabela 1. Zestawienie kontrolerów serii PRxx1

Kontroler	PR311SE	PR311SE-BK	PR411DR	PR611	PR621
Zasilanie	10-15VDC	10-15VDC	18VAC lub 12VDC	10-15VDC	10-15VDC
Wejścia NO/NC	3	3	8	3	3
Wyjścia przekaźnikowe	1	1	2	1	1
Wyjścia tranzystorowe	2	2	2	2	2
Wbudowany czytnik	Tak	Tak	Nie	Tak	Tak
Zewnętrzny czytnik	1	1	2	1	1
Zewnętrzny czytnik Wiegand 26-66bit	Nie	Nie	2	Nie	Nie
Klawiatura	Tak	Nie	Nie	Tak	Nie
Klawisze funkcyjne	Tak	Nie	Nie	Nie	Nie
Inne	Praca w warunkach zewnętrznych, w zestawie kabel podłączeniowy (45 cm)	Praca w warunkach zewnętrznych, w zestawie kabel podłączeniowy (45 cm)	Wbudowany zasilacz 1.2 A z podtrzymaniem bateryjnym	Praca w warunkach zewnętrznych, w zestawie kabel podłączeniowy (45 cm) lub zaciski śrubowe	Praca w warunkach zewnętrznych, kabel podłączeniowy (45 cm) lub zaciski śrubowe

2.3 Skrócona charakterystyka kontrolerów serii PRxx1

Cechy kontrolerów serii podstawowej PRxx1:

- Jednostronna lub dwustronna kontrola jednego przejścia
- Praca w Trybie Autonomicznym lub Trybie Sieciowym z centralą CPR32-SE
- 1000 użytkowników
- 250 Grup Dostępu (*)
- 99 Harmonogramów Ogólnego Przeznaczenia (*)

- 128 stref czasowych w obrębie jednego Harmonogramu (*)
- 4 Harmonogramy Świąteczne (H1-H4) (*)
- Automatyczna zmiana czasu lato-zima (*)
- Rejestracja zdarzeń dla celów RCP (*)
- Wbudowana klawiatura (PR311SE, PR611)
- Programowalne linie wejściowe i wyjściowe
- Wbudowane wyjście przekaźnikowe 1.5A/30V
- Wbudowane wyjście przekaźnikowe 1.5A/230V (wyłącznie PR411DR)
- Interfejs komunikacyjny RS485 (dowolna topologia)
- Możliwość aktualizacji oprogramowania wbudowanego (firmware)
- Oprogramowanie zarządzające (Windows XP/Vista/7)
- Praca w warunkach zewnętrznych (PR311SE, PR311SE-BK, PR611 oraz PR621)
- Możliwość montażu na szynie DIN 35mm (wyłącznie PR411DR)
- Zarządzanie systemem przez sieć komputerową LAN/WAN (wymagany interfejs UT-4)
- Zasilanie 10-15 VDC (PR311SE, PR311SE-BK, PR611 oraz PR621)
- Zasilanie 18VAC lub 12VDC (wyłącznie PR411DR)
- Znak CE

(*) – funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE

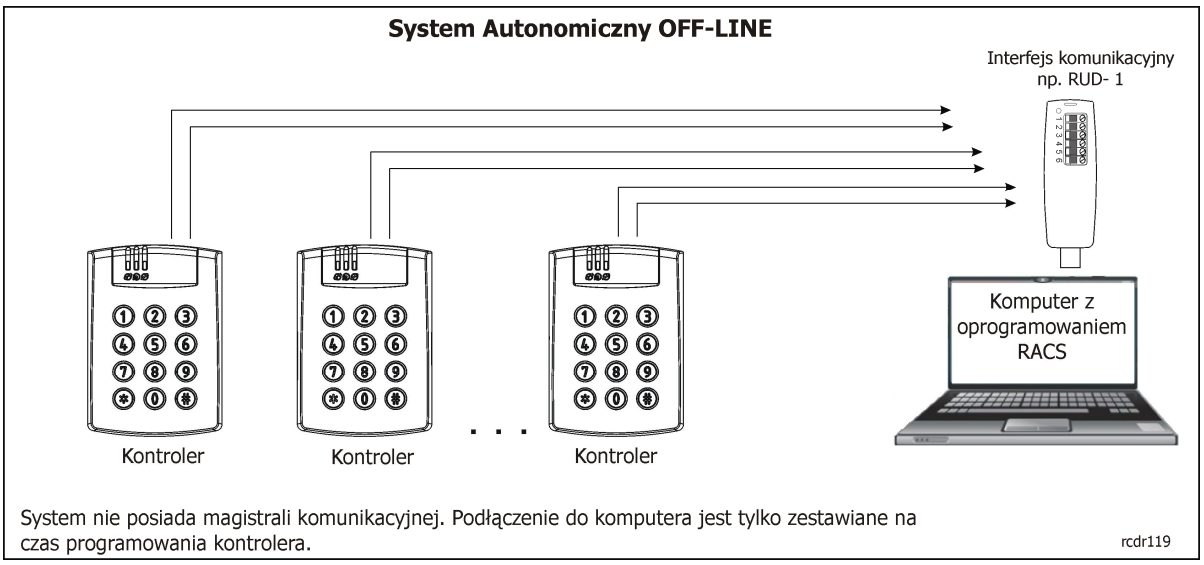
III OPIS FUNKCJONALNY

3.1 Tryby pracy kontrolerów serii PRxx1

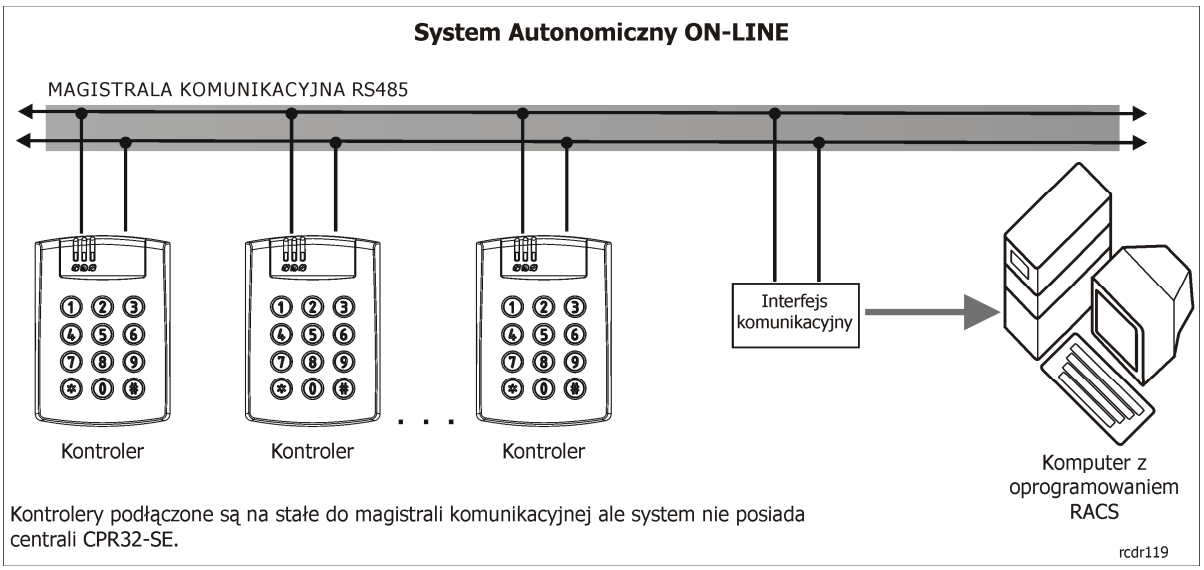
3.1.1 Praca w Trybie Autonomicznym

W Trybie Autonomicznym off-line (bez centrali CPR32-SE) kontrolery serii PRxx1 nie udostępniają możliwości definiowania Harmonogramów dostępu ani nie mają możliwości samodzielnego rejestrowania zdarzeń. W tym trybie możliwy jest podział użytkowników na Grupy Dostępu, ale bez przypisania im zmiennych w czasie praw dostępu. Cecha ta powoduje, że wszyscy użytkownicy danego kontrolera (przejścia) mają permanentne prawo dostępu przez 24h na dobę lub nie mają go w ogóle w zależności od ustawień administratora. W tym trybie można definiować Strefy Dostępu. Kontrolery można programować ręcznie lub z komputera za pomocą programu PR Master.

Uwaga: Scenariusz pracy autonomicznej nie wyklucza możliwości podłączenia kontrolera do magistrali RS485 i programowania go z poziomu komputera PC.



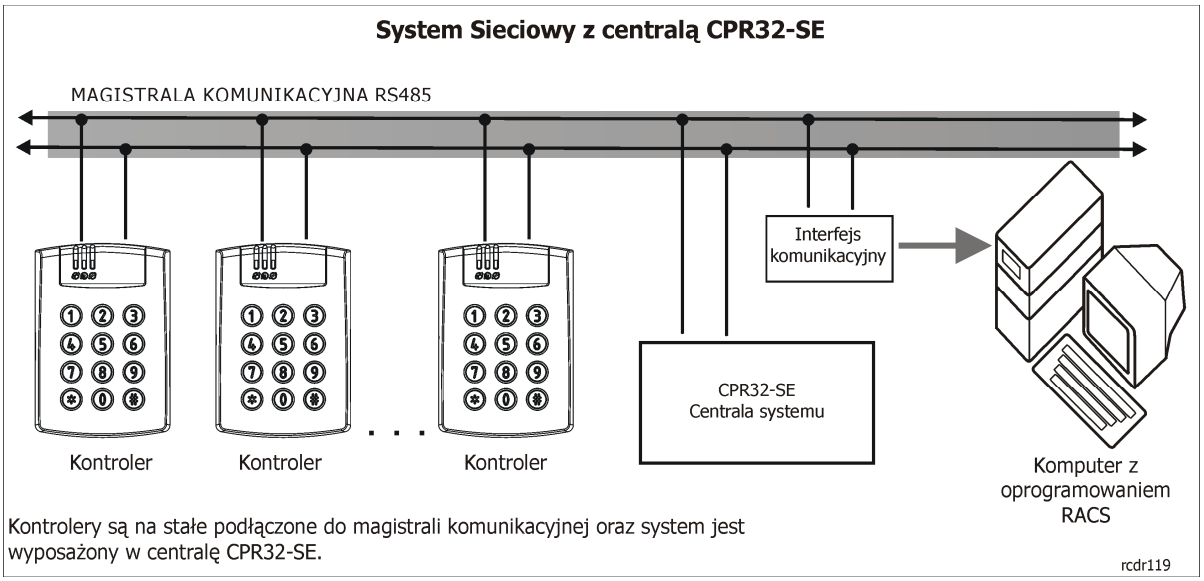
Rys. 2 Praca w Trybie Autonomicznym (offline)



Rys. 3 Praca w Trybie Autonomicznym (online)

3.1.2 Praca w Trybie Sieciowym (z centralą CPR32-SE)

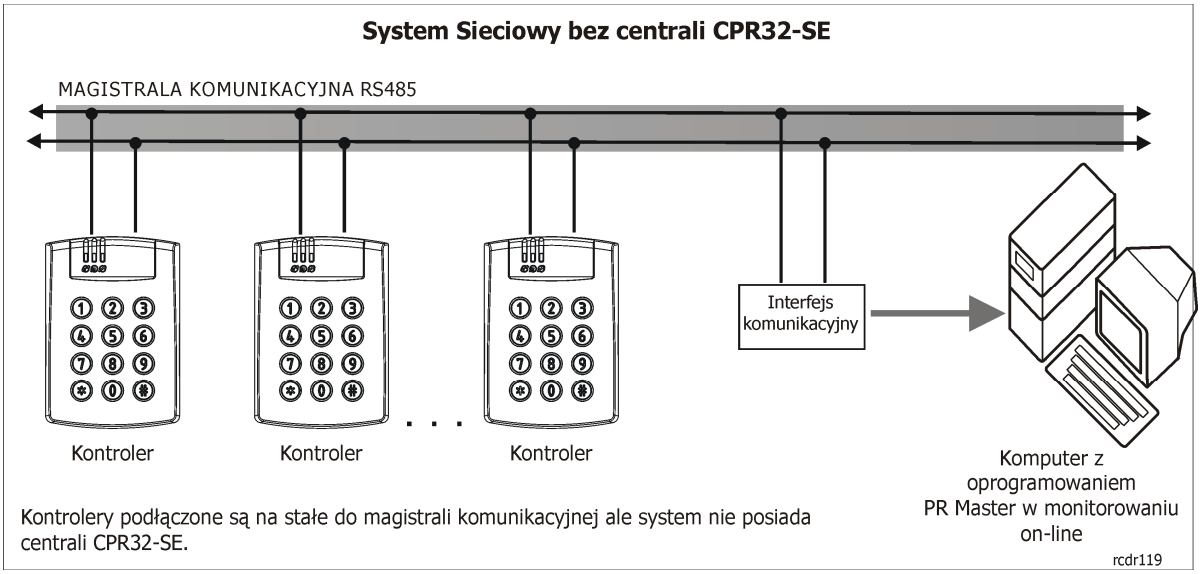
Kiedy system kontroli dostępu posiada magistralę komunikacyjną i jest ona wykorzystywana do wymiany danych pomiędzy urządzeniami (kontrolerami) do niej podłączonymi to taki system nosi nazwę Sieciowego Systemu Kontroli Dostępu. W systemie RACS warunkiem koniecznym działania takiego systemu kontroli dostępu jest obecność centrali CPR32-SE. Istnieje wtedy możliwość podziału użytkowników na 250 Grup Dostępu, przypisanie im odpowiednich Harmonogramów i Stref Dostępu a także zdefiniowanie specjalnych harmonogramów sterujących Trybem Identyfikacji oraz Trybem Drzwi. Centrala CPR32-SE gromadzi zdarzenia w swoim buforze pamięci oraz jest odpowiedzialna za wszelkie funkcje o charakterze globalnym tj. Strefy Alarmowe oraz Strefy APB (ang. anti-passback). Do programowania oraz zarządzania w Trybie Sieciowym wymagane jest podłączenie do komputera.



Rys. 4 Praca w Trybie Sieciowym (z centralą CPR32-SE)

3.1.3 Praca w Trybie Sieciowym (bez centrali CPR32-SE)

W tym trybie komputer PC wraz z programem PR Master uruchomionym do monitorowaniu on-line pełni rolę urządzenia, które emuluje obecność centrali CPR32-SE. W systemie takim istnieje zatem możliwość podziału użytkowników na Grupy Dostępu, przypisanie im odpowiednich Harmonogramów oraz Stref Dostępu a także zdefiniowanie specjalnych harmonogramów sterujących Trybem Identyfikacji oraz Trybem Drzwi. Dostępne są również funkcje o charakterze globalnym takie jak Strefy Alarmowe oraz Strefy APB. Aby system realizował wszystkie wymienione funkcje komputer PC musi być na stałe włączony i podłączony za pośrednictwem interfejsu komunikacyjnego do magistrali komunikacyjnej systemu RACS (praca w trybie monitorowania online). W przypadku awarii komputera lub jego wyłączenia kontrolery automatycznie przechodzą do Trybu Autonomicznego i kontynuują kontrolę dostępu do pomieszczeń na takich zasadach, jak miało to miejsce w momencie wystąpienia awarii. Po powrocie komunikacji z komputerem PC następuje automatyczne przejście kontrolerów do Trybu Sieciowego i wznowienie wszystkich zawieszonych funkcji w tym odnowienie ustawień Harmonogramów dostępu.



Rys. 5 Praca w Trybie Sieciowym (bez centrali CPR32-SE)

3.2 Komunikacja

3.2.1 Interfejs RS485

Kontroler PRxx1 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 Sieciowego Systemu Kontroli Dostępu. Każdy kontroler podłączony do magistrali komunikacyjnej musi posiadać swój niepowtarzalny adres (numer ID=00-99). Do jednej magistrali komunikacyjnej można dołączyć maksymalnie 32 kontrolery dostępu oraz jedną centralę CPR32-SE (centrala nie wymaga ustawienia adresu). Topologia magistrali komunikacyjnej w systemie RACS może być kształtowana bardzo elastycznie, dopuszczalne są struktury typu „drzewo", „gwiazda" a także dowolne 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. Kable w ekranie należy stosować tylko w warunkach silnych zakłócających pól elektromagnetycznych. 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 CPR32-SE: 1200m
- pomiędzy dowolnym kontrolerem a interfejsem komunikacyjnym: 1200m
- pomiędzy centralą CPR32-SE a interfejsem komunikacyjnym: 1200m

---

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

Struktura złożona z magistrali komunikacyjnej, kontrolerów dostępu (maks. 32) oraz opcjonalnie występującej centrali CPR32-SE 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 - VCP). W tym ostatnim przypadku komunikacja z podsystemem KD może odbywać się za pośrednictwem interfejsów emulujących port szeregowy np. RUD-1, UT-2USB, UT-4 (Ethernet) i inne.
Każdy kontroler serii PRxx1 może zarządzać pojedynczym przejściem kontrolowanym jedno lub dwustronnie. W ramach jednego systemu RACS można zintegrować do 250 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 LAN/WAN a także sieci bezprzewodowych Wi-Fi.

Uwaga: Interfejsy komunikacyjne można stosować tymczasowo jedynie na czas programowania kontrolera bądź też można podłączyć je na stałe po to by umożliwić zarządzanie systemem KD (patrz 3.1 Tryby pracy kontrolerów serii PRxx1). Do programowania zalecane jest wykorzystanie interfejsu RUD-1, ponieważ dostarcza wbudowane wyjście DC, które może być użyte do zasilania programowanego urządzenia.

3.2.2 Adresy Kontrolerów

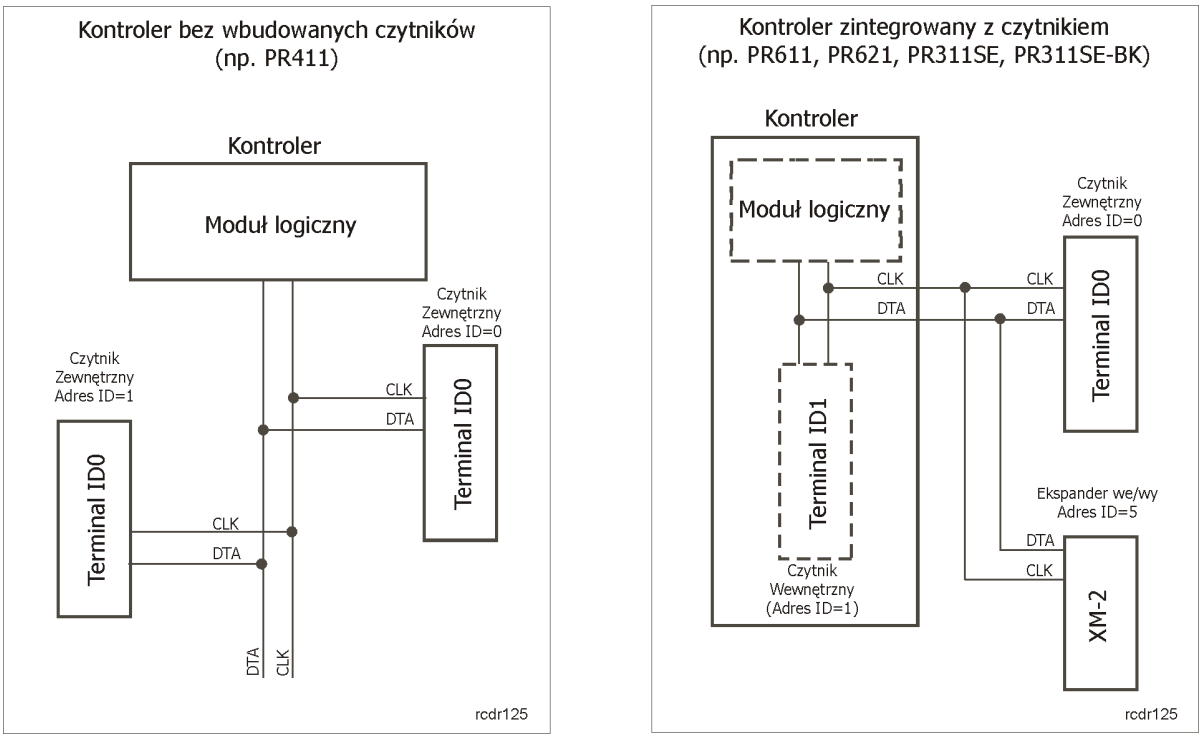
Każdy kontroler podłączony do magistrali komunikacyjnej musi posiadać swój niepowtarzalny adres z zakresu 00-99, przy czym każdy nowy fabrycznie kontroler posiada adres ID=00. O ile zachodzi taka potrzeba to adres ten można zmienić manualnie w czasie procedury resetu pamięci (patrz 4.1 Reset Ustawień – Programowanie Identyfikatora MASTER oraz Adresu ID) lub z poziomu programu zarządzającego (PR Master). W kontrolerach serii PRxx1 istnieje możliwość zaprogramowania stałego adresu ID kontrolera (tzw. FixedID). Stały adres ID można ustawić w trakcie procesu aktualizacji oprogramowania wbudowanego (firmware) w urządzenie, za pomocą programu Roger ISP. Ustawienie FixedID wyklucza inne metody programowania adresu takie jak programowe ustawianie adresu ID za pomocą programu PR Master na komputerze PC oraz manualne ustawienie adresu ID (w trakcie resetu pamięci lub za pomocą zworek w przypadku kontrolera PR411DR). Aby dokonać zmiany adresu stałego należy zatem dokonać ponownej aktualizacji oprogramowania wbudowanego (firmware) w urządzenie. W przypadku kontrolera PR411DR jak już wspomniano wcześniej adres ID można również ustawić za pomocą zworek umieszczonych na płycie modułu. Całkowity zakres adresów ID dla takiego ustawienia mieści się w przedziale 0-127. Przy czym jeśli ustawiony adres zawiera się w przedziale 00-99 to czytnik nie zezwala na zmianę tego adresu ID na drodze programowej za pomocą komputera PC czy manualnie. Z kolei dla adresów ID powyżej 99 można wprowadzać zmiany na drodze programowej. Szczegółowe informacje na temat różnych sposobów ustawień adresu dostępne są w instrukcjach instalacji poszczególnych kontrolerów.

Uwaga: Stały adres ID posiada najwyższy priorytet – po jego zaprogramowaniu zarówno adres nadany z poziomu programu PR Master jak i ustawiony za pomocą zworek są ignorowane.

3.2.3 Interfejs RACS Clock & Data

Oprócz interfejsu RS485 kontroler PRxx1 jest wyposażony w interfejs komunikacyjny RACS Clock & Data. Interfejs ten jest przeznaczony do komunikacji z zewnętrznymi czytnikami oraz modułami rozszerzeń f-my Roger i składa się z dwóch linii: CLK i DTA. Do tych linii można dołączyć następujące urządzenia zewnętrzne:

- podstawowy czytnik dostępu (Terminal ID0, adres ID=0)
- dodatkowy czytnik dostępu (Terminal ID1, adres ID=1) (tylko PR411DR)
- moduł rozszerzeń we/wy XM-2 (adres ID=5)



Rys. 6 Interfejs RACS Clock&Data

Uwaga: Jeśli do linii CLK i DTA nie podłączono żadnych urządzeń (czytników bądź modułów rozszerzeń) to linie te można skonfigurować jako zwykłe wyjścia tranzystorowe o obciążalności 150mA i napięciu do 15V DC.

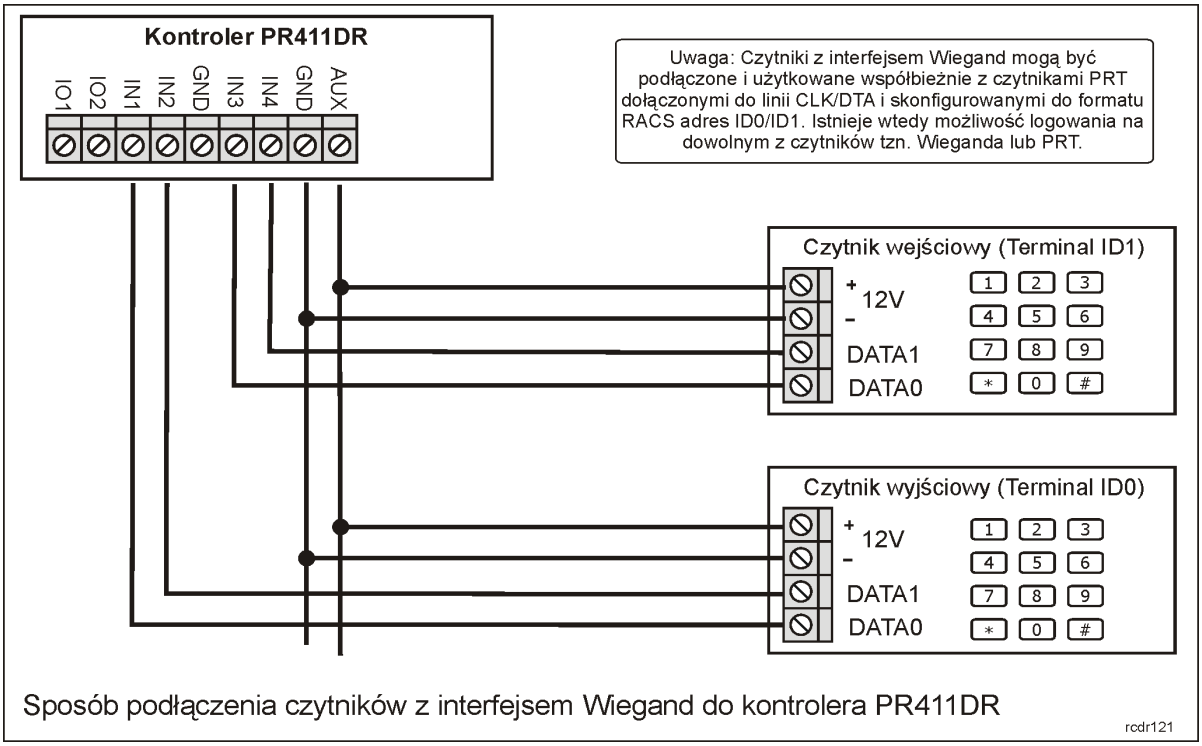
Maksymalna odległość liczona po kablu pomiędzy kontrolerem a dowolnym czytnikiem/modułem dołączonym do magistrali CLK/DTA nie może przekraczać 150m. Struktura oraz rodzaje kabli stosowane w tej magistrali są całkowicie dowolne, jedynym warunkiem stawianym kablom jest to aby ich całkowita rezystancja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

3.2.4 Współpraca z modułem XM-2

Kontroler PRxx1 może współpracować z jednym modułem we/wy typu XM-2 o adresie ID=5. Zastosowanie tego modułu powoduje z jednej strony zwiększenie ogólnej ilości wszystkich linii we/wy jak również umożliwia fizyczne odseparowanie linii we/wy od kontrolera. Potrzeba separacji linii we/wy od kontrolera zachodzi głównie w odniesieniu do kontrolerów z wbudowanymi czytnikami (np. PR311SE, PR611), które w przypadku instalacji w miejscach ogólnodostępnych są narażone na ingerencję osób postronnych. W wyniku tego zagrożenia osoby, które uzyskały dostęp do wnętrza kontrolera mogą w prosty sposób obejść styki wewnętrznego przekaźnika i odblokować drzwi. Komunikacja pomiędzy kontrolerem a modułem XM-2 odbywa się na drodze cyfrowej.

3.2.5 Dołączanie czytników Wiegand

Spośród kontrolerów serii PRxx1 jedynie kontroler PR411DR może współpracować z czytnikami pracującymi w standardzie Wiegand. Sposób dołączania czytników tego typu został przedstawiony na rysunku poniżej.



Rys. 7 Podłączenie czytników z interfejsem Wiegand

Czytniki Wiegand-a mogą być podłączone do kontrolera PR411DR niezależnie od czytników serii PRT. Zatem użytkownicy mogą dokonać identyfikacji na czytniku Wiegand lub na czytniku PRT.

3.3 Użytkownicy

3.3.1 Użytkownicy zwykli i Goście

Każdy z zaprogramowanych w systemie RACS użytkowników posiada swój numer identyfikacyjny i może być identyfikowany za pomocą karty zbliżeniowej i/lub kodu PIN. Kody PIN mogą składać się z 3 do 6 cyfr a ich wprowadzanie należy zawsze zakańczać za pomocą przycisku #. Ponadto każdy użytkownik systemu może mieć nadane specjalne uprawnienia zwane Opcjami Użytkowników. Lista wszystkich użytkowników kontrolera składa się z podanych poniżej kategorii:

Tabela 2. Typy użytkowników

Nazwa	Numer ID	Opis
MASTER	000	Uprawnienie do otwierania drzwi oraz przezbrajania. Użytkownik MASTER ma niezmiennie ustawioną opcję Op.1= Nie i wszystkie inne opcje Op.2-Op.8 = Tak (patrz Tabela 3)
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=050-099	Uprawnienie tylko do przezbrajania kontrolera, przezbrojenie następuje w następstwie jednokrotnego użycia identyfikatora
NORMAL	ID=100-999	Uprawnienie tylko do otwierania drzwi
GOŚĆ	ID=4000-4007	Użytkownicy definiowani indywidualnie na każdym kontrolerze osobno. Użytkownicy tego typu posiadają uprawnienie do otwierania drzwi oraz przezbrajania kontrolera

Użytkownicy Standardowi (ID=000-999), to lista tysiąca użytkowników wspólna dla wszystkich kontrolerów wchodzących w skład systemu. Natomiast Goście to lista 8 użytkowników zaprogramowanych indywidualnie na każdym kontrolerze.
Poza standardową listą użytkowników, w kontrolerze można zdefiniować dodatkową listę 8 użytkowników specjalnych tak zwanych Gości. Programowanie i zarządzanie listą gości odbywa się za pomocą specjalnych procedur programujących. W przeciwieństwie do standardowych użytkowników (ID=000-999) goście definiowani są indywidualnie na każdym kontrolerze osobno. Opcjonalnie do zarządzania użytkownikami goście można wykorzystać specjalny interfejs programisty (API), który pozwala na tworzenie specjalnego oprogramowania dedykowanego do zarządzania tego typu użytkownikami. Każdy gość może być identyfikowany za pomocą karty zbliżeniowej i/lub kodu PIN. Ponadto, tak jak każdy standardowy użytkownik systemu może mieć nadane specjalne uprawnienia zwane Opcjami użytkowników. Jeśli kontroler pracuje w Trybie Sieciowym (patrz3.1.2 Praca w Trybie Sieciowym (z centralą CPR32-SE)) to istnieje możliwość podziału gości na Grupy Dostępu i przypisanie im odpowiednich Harmonogramów.

3.3.2 Opcje (uprawnienia) użytkowników

Dla każdego użytkownika systemu niezależnie od tego czy należy do kategorii Użytkowników Standardowych, Gości czy użytkowników z Kodem Obiektu można ustawić 8 specjalnych opcji (oznaczanych skrótowo Op.1-Op.8). Definiują one pewne dodatkowe uprawnienia związane z programowaniem i obsługą kontrolera.

Tabela 3. Opcje (uprawnienia) użytkowników

Opcja	Nazwa	Opis
Op.1	Całkowita blokada dostępu	Załączenie opcji całkowicie blokuje dostęp danemu użytkownikowi bez względu na inne jego uprawnienia
Op.2	Autoryzacja użycia klawisza F1 na terminalu ID0	Załączenie opcji uprawnia użytkownika do autoryzacji użycia klawisza F1 na terminalu ID0 (patrz 3.10 Klawisze funkcyjne)
Op.3	Autoryzacja użycia klawisza F2 na terminalu ID0	Załączenie opcji uprawnia użytkownika do autoryzacji użycia klawisza F2 na terminalu ID0 (patrz 3.10 Klawisze funkcyjne)
Op.4	Autoryzacja użycia klawisza F1 na terminalu ID1	Załączenie opcji uprawnia użytkownika do autoryzacji użycia klawisza F1 na terminalu ID1 (patrz 3.10 Klawisze funkcyjne)
Op.5	Autoryzacja użycia klawisza F2 na terminalu ID1	Załączenie opcji uprawnia użytkownika do autoryzacji użycia klawisza F2 na terminalu ID1 (patrz 3.10 Klawisze funkcyjne)
Op.6	Autoryzacja użycia Funkcji Użytkownika	Załączona opcja uprawnia użytkownika do stosowania tzw. Funkcji Użytkownika (patrz 4.2 Funkcje Użytkownika
Op.7	Uprawnienie do przezbrajania kontrolera	Załączenie opcji uprawnia użytkownika do przezbrajania kontrolera
Op.8	Autoryzacja użycia Kart Funkcyjnych	Załączenie opcji uprawnia użytkownika do użycia Kart Funkcyjnych (patrz 3.11 Karty Funkcyjne)

3.3.3 Grupy Dostępu

Użytkownicy kontrolera mogą być przypisywani do jednej z predefiniowanych grup tj. Bez Grupy, Grupy bez Dostępu lub przynależeć do dowolnej Grupy Dostępu zdefiniowanej przez użytkownika systemu. Przynależność do danej Grupy Dostępu determinuje prawa użytkownika w ramach danego

systemu KD. Wszyscy użytkownicy należący do tej samej Grupy Dostępu mają takie same (identyczne) uprawnienia dostępu, 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. Użytkownicy posiadający status Bez Grupy posiadają dostęp do wszystkich Stref Dostępu bez żadnych ograniczeń czasowych – tzn. mają dostęp do wszystkich pomieszczeń będących pod kontrolą systemu przez całą dobę i w każdym dniu tygodnia. Natomiast użytkownicy przypisani do Grupy bez Dostępu nie mają prawo otwierać żadnych drzwi.

3.4 Tryby Identyfikacji

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

Tabela 4. Tryby Identyfikacji	
Nazwa	Opis
Karta lub PIN	Kontroler wymaga odczytu karty lub podania kodu PIN
Karta i PIN	Kontroler wymaga odczytu karty i podania kodu PIN, kolejność nie gra roli
Tylko Karta	Kontroler akceptuje tylko karty
Tylko PIN	Kontroler akceptuje tylko kody PIN

Tryby Identyfikacji definiuje się niezależnie dla każdej strony przejścia. O ile Tryb Identyfikacji nie zostanie zmieniony to kontroler stosuje tzw. Domyślny Tryb Identyfikacji. Tryb Identyfikacji dotyczy wszystkich użytkowników niezależnie od ich typu lub kategorii. Sterowanie Trybami Identyfikacji może odbywać się z poziomu:

- Harmonogramu (gdy kontroler pracuje w Trybie Sieciowym)
- Linii wejściowej,
- Klawisza funkcyjnego

3.5 Tryby Drzwi

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

Tabela 5. Tryby Drzwi	
Tryb Drzwi	Opis
Normalny	Normalnie drzwi są zablokowane, zwolnienie drzwi następuje tylko na czas przyznania dostępu
Odblokowane	Drzwi są odblokowane na stałe, wejście może się odbywać bez użycia identyfikatorów i przejście jest niekontrolowane
Warunkowo Odblokowane	Początkowo drzwi są w stanie Normalnym, z chwilą przyznania dostępu pierwszej osobie drzwi przechodzą samoczynnie do trybu Odblokowane
Zamknięte	Drzwi są permanentnie zablokowane niezależnie od tego czy użytkownik, który próbuje wejść jest uprawniony do wejścia czy nie

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

- Harmonogramu (gdy kontroler pracuje w Trybie Sieciowym).
- Klawisza funkcyjnego
- Linii wejściowej

3.6 Tryby Uzbrojenia

3.6.1 Koncepcja Trybów Uzbrojenia

Kontroler PRxx1 ma dwa stany uzbrojenia: Uzbrojony i Rozbrojony. Aktualny stan uzbrojenia jest sygnalizowany na dwukolorowym wskaźniku LED STATUS przy czym stanowi uzbrojenia odpowiada kolor czerwony natomiast stanowi rozbrojenia odpowiada kolor zielony.
Sterowanie trybem uzbrojenia kontrolera może być realizowane na kilka sposobów:

- Manualnie przy pomocy identyfikatorów użytkowników (karty i/lub PIN)
- Automatycznie z poziomu Harmonogramu (*)
- Z linii wejściowej
- Z klawisza funkcyjnego
- Zdalnie z poziomu centrali CPR32-SE (logika Stref Alarmowych) (*)
- Zdalnie z komputera zarządzającego

(*) - funkcja dostępna tylko w systemach w Trybie Sieciowym (patrz 3.1.2 Praca w Trybie Sieciowym (z centralą CPR32-SE)

3.6.2 Przezbrajanie kontrolera

Kontroler może być przezbrajany przy pomocy identyfikatorów użytkowników kart/PIN kodów: MASTER, SWITCHER Full oraz SWITCHER Limited (patrz 3.3.1 Użytkownicy zwykli i Goście).
Sposób przezbrajania dla użytkowników SWITCHER Full i MASTER:

- Zalogować się (tzn. odczytaj kartę lub wprowadź PIN w zależności od aktualnego Trybu Identyfikacji – patrz 3.4 Tryby Identyfikacji)
- Poczekać aż wskaźnik LED SYSTEM zacznie pulsować
- Gdy wskaźnik LED SYSTEM pulsuje dokonać powtórnego logowania, przy czym jeśli na kontrolerze obowiązuje w danej chwili Tryb Karta i PIN to wystarczy użyć tylko jednej z form identyfikacji tzn. karty lub PIN-u

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

3.6.3 Przezbrajanie kontrolera przez harmonogram

Kiedy kontroler pracuje w Trybie Sieciowym istnieje możliwość zmiany stanu jego uzbrojenia samoczynnie wg zdefiniowanego harmonogramu zwanego Harmonogramem Przezbrajania. Jeśli kontroler należy do Strefy Alarmowej to będzie on automatycznie zmieniał swój aktualny stan uzbrojenia wg Harmonogramu Przezbrajania zdefiniowanego dla danej Strefy Alarmowej. Jeśli jednak kontroler nie należy do żadnej Strefy Alarmowej to można mu przypisać dowolny harmonogram, który będzie sterował jego stanem uzbrojenia. Wskazanie Harmonogramu Nigdy powoduje, że kontroler na stałe będzie pracował w trybie Uzbrojony, natomiast wskazanie Harmonogramu Zawsze powoduje, że kontroler przez cały czas pracy będzie w trybie Rozbrojony. Harmonogram 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 będzie samoczynnie powracać do stanu uzbrojenia.
Automatyczne uzbrojenie kontrolera może zostać uniemożliwione, jeśli linia wejściowa **[13]:Blokada uzbrojenia** jest wyzwolona albo drzwi są otwarte (linia wejściowa **[01]:Czujnik otwarcia** wskazuje, że drzwi nie są zamknięte).

3.6.4 Opcja: Harmonogram Przezbrajania

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, gdy kontroler nie należy do żadnej Strefy Alarmowej. Gdy opcja jest wyłączona przezbrajanie za pośrednictwem haromonogramów.

3.7 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
- Zdefiniowanie Stref Dostępu
- Przydzielenie punktów identyfikacji (terminali) do konkretnych Stref Dostępu
- Definiowanie Harmonogramów (tzw. kalendarzy)
- Powiązanie Grup Użytkowników ze Strefami Dostępu oraz Harmonogramami. Etap ten polega na wskazaniu Harmonogramu, 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 punkt identyfikacji (czytnik)
- Sprawdzenie dodatkowych mechanizmów sterujących dostępem (APB, opcje użytkownika, tryb drzwi itd.)
- Decyzja o dostępie
- Odblokowanie drzwi

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

3.7.1 Sygnalizacja dostępu

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

3.7.2 Sterowanie elementem wykonawczym

W praktyce spotyka się cztery podstawowe sposoby sterowania elementem wykonawczym:

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

Kontroler może sterować elementem wykonawczym (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 Terminala ID0 czy Terminala ID1 natomiast wyjścia **[97]** i **[98]** są aktywowane w zależności od tego, na którym czytniku (ID0 czy ID1) nastąpiło logowanie użytkownika. W praktyce, wyjścia **[97]** i **[98]** znajdują zastosowanie do sterowania bramką obrotową w sytuacji, gdy wymagane jest rozróżnienie kierunku obrotu bramki.
W momencie przyznania dostępu drzwi zostają odblokowane na czas określony przez parametr Czas na Wejście, który to może być zdefiniowany w zakresie od 1 do 99 sekund. Opcjonalnie, sterowanie zamkiem drzwiowym może być realizowane w trybie zatrzask (tryb bistabilny), wtedy drzwi zostają odblokowane na czas nieograniczony tzn. aż do momentu wystąpienia kolejnego przyznania dostępu (praca bistabilna).

3.7.3 Opcja: 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 tej opcji użytkownicy uprawnieni do przezbrajania kontrolera mogą czasowo blokować i odblokowywać dostęp dla pozostałych użytkowników systemu bez względu na ustawienia Harmonogramów dostępu.

3.7.4 Opcja: Praca bistabilna (typu zatrzask)

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.

3.7.5 Opcja: Skracanie czasu otwarcia (ang. auto-relock)

Stosowanie tej opcji ma sens tylko wtedy kontroler współpracuje z czujnikiem otwarcia drzwi. Załączenie tej opcji powoduje, że kontroler może skrócić czas odblokowania drzwi. Opcja ta ma dwa warianty:

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

W pierwszym przypadku kontroler wyłącza wyjście sterujące zamkiem elektrycznym w momencie, gdy rozpozna, że drzwi zostały już otwarte. Wariant ten stosuje się w odniesieniu do urządzeń, które odblokowują drzwi przez podanie napięcia zasilania (np. elektrozaczep). W drugim przypadku kontroler wyłącza wyjście sterujące zamkiem w momencie rozpoznania, że po otwarciu drzwi zostały ponownie domknięte, wariant ten stosuje się w odniesieniu do urządzeń, które odblokowują drzwi poprzez zdjęcie napięcia zasilania (np. zwora elektromagnetyczna, elektrozaczep odwrotny).

3.7.6 Kod Obiektu (ang. Facility Code)

Kod Obiektu to charakterystyczna część kodu karty, która wskazuje na przynależność danej karty do pewnej (większej) grupy kart wytworzonych zwykle dla konkretnego systemu lub klienta. W kontrolerze PRxx1 kod obiektu to bity na pozycjach 16-24 kodu karty, które po przetworzeniu na postać dziesiętną dają liczbę z zakresu od 000-255.
Przykład (kod karty w postaci binarnej): 00010000000000001110111000100010101101111 to podkreślona część kodu 11101110 jest traktowana jako Kod Obiektu.
Kody kart ISO, PCV oraz breloków dostarczanych przez f-mę Roger drukowane są w dwóch postaciach: z pełnym kodem karty w systemie dziesiętnym np. 68735083191 i w skróconej formie, która jest generowana na podstawie pierwszych 24 bitów pełnego kodu karty. Ta skrócona wartość kodu jest przedstawiona w postaci trzech cyfr (z zakresu 000-255) oddzielonych przecinkiem od pozostałych 5 cyfr np. 238,08887. Pierwsze 3 cyfry przed przecinkiem stanowią Kod Obiektu. Załączenie opcji Kod Obiektu powoduje, że kontroler przyznaje dostęp wszystkim kartom, które mają ten sam Kod Obiektu. Dzięki tej funkcji kontroler może umożliwiać dostęp do pomieszczenia dla znacznie większej ilości użytkowników pod warunkiem, że użytkownicy ci posiadają karty zgodne ze zdefiniowanym Kodem obiektu.

Także grupę kart, które są zgodne z Kodem Obiektu można przypisać do określonej Grupy. W wyniku tego wszyscy użytkownicy posiadający kartę z określonym Kodem Obiektu będą mieli takie same prawa dostępu. Ponadto, użytkownicy posiadający karty z Kodem Obiektu mogą mieć nadane Opcje Użytkowników (Op.1 - Op.8) – patrz 3.3.2 Opcje (uprawnienia) użytkowników).

3.7.7 Opcja: Nie sygnalizuj użycia kodu PIN pod przymusem

Celem tej funkcji jest sygnalizacja sytuacji, gdy kod PIN został wprowadzony pod przymusem. Gdy ta opcja jest niezałączona to wprowadzenie kodu PIN różniącego się o jedność („1") na ostatniej pozycji jest interpretowane, jako wprowadzenie kodu pod przymusem, co następnie wywołuje sygnalizację stanu WYMUSZENIE.
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 różniły się one więcej niż o jedność na ostatniej pozycji. Program PR Master samoczynnie sprawdza czy ten warunek jest spełniony. Można również wyłączyć tą funkcję i wtedy program będzie dopuszczał definiowanie kodów PIN różniących się między sobą o dowolną wartość

3.7.8 Opcja: Zakaz programowania manualnego

Załączenie opcji blokuje możliwość manualnego programowania Funkcji Użytkownika (patrz 4.2 Funkcje Użytkownika) oraz Kart Funkcyjnych (patrz 3.11 Karty Funkcyjne) w kontrolerze.

3.7.9 Flagi Systemowe

Flagi Systemowe to stany logiczne w pamięci kontrolera, które odzwierciedlają pewne określone stany (sytuacje) występujące w kontrolerze. Niektóre flagi posiadają ściśle zdefiniowane znaczenie i są związane z określonymi zdarzeniami (np. ŚWIATŁO, TAMPER, WŁAMANIE) inne, mają charakter uniwersalny i mogą być użyte do dowolnie wybranych celów (np. AUX1, AUX2).
Normalnie, domyślnym stanem każdej flagi jest stan wyłączenia. Załączenie flagi może nastąpić jedynie w następstwie wystąpienia pewnych, specyficznych dla danej flagi przyczyn. Powrót flagi do stanu normalnego następuje samoczynnie po upływie czasu określonego przez jej licznik lub pod wpływem innego, charakterystycznego dla danej flagi 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 sygnalizowany na linii wyjściowej.

Tabela 6. Flagi Systemowe

Flaga	Załączenie flagi	Wyłączenie flagi
AUX1	Karty Funkcyjne: **[F12]:Załącz AUX1** **[F14]:Przełącz AUX1** Linie wejściowe: **[71]:Załącz AUX1** **[73]:Przełącz AUX1** Klawisze funkcyjne: **[71]:Załącz AUX1** **[73]:Przełącz AUX1**	Karty Funkcyjne: **[F13]:Wyłącz AUX1** **[F14]:Przełącz AUX1** Linie wejściowe: **[72]:Wyłącz AUX1** **[73]:Przełącz AUX1** Klawisze funkcyjne: **[72]:Wyłącz AUX1** **[73]:Przełącz AUX1** Z chwilą upłynięcia czasu określonego przez jej licznik

AUX2	Karty Funkcyjne: **[F20]:Załącz AUX2** **[F22]:Przełącz AUX2** Linie wejściowe: **[74]:Ustaw AUX2** **[76]:Przełącz AUX2** Klawisze funkcyjne: **[74]:Załącz AUX2** **[76]:Przełącz AUX2**	Karty Funkcyjne: **[F21]:Wyłącz AUX2** **[F22]:Przełącz AUX2** Linie wejściowe: **[75]:Wyłącz AUX2** **[76]:Przełącz AUX2** Klawisze funkcyjne: **[75]:Wyłącz AUX2** **[76]:Przełącz AUX2** Z chwilą upłynięcia czasu określonego przez jej licznik
ŚWIATŁO	Karty Funkcyjne: **[F15]:Załącz ŚWIATŁO** **[F17]:Przełącz ŚWIATŁO** Linie wejściowe: **[68]:Załącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** Klawisze funkcyjne: **[78]:Załącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO**	Karty Funkcyjne: **[F16]:Wyłącz ŚWIATŁO** **[F17]:Przełącz ŚWIATŁO** Linie wejściowe: **[69]:Wyłącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** Klawisze funkcyjne: **[69]:Wyłącz ŚWIATŁO** **[70]:Przełącz ŚWIATŁO** Z chwilą upłynięcia czasu określonego przez jej licznik
TAMPER	Linia wejściowa: **[08]:TAMPER**	Rozbrojenie kontrolera Z chwilą upłynięcia czasu określonego przez jej licznik
WŁAMANIE	Linie wejściowe: **[09]:WŁAMANIE** **[08]:TAMPER** Klawisz funkcyjny: **[09]:WŁAMANIE**	Rozbrojenie kontrolera Z chwilą upłynięcia czasu określonego przez jej licznik
WYMUSZENIE	Wprowadzenie kodu pod przymusem (ang. Duress) – patrz 3.7.7 Opcja: Nie sygnalizuj użycia kodu PIN pod przymusem	Z chwilą upłynięcia czasu określonego przez jej licznik
PROBLEM	Linie wejściowe: **[05]:Dozór napięcia sieci AC** **[06]: Dozór stanu akumulatora** Utrata komunikacji z modułem XM-2	Przezbrojenie kontrolera Z chwilą upłynięcia czasu określonego przez jej licznik

ZWŁOKA NA WEJŚCIE	Linia wejściowe: **[15]:Włamanie–linia zwłoczna**	Rozbrojenie kontrolera Z chwilą upłynięcia czasu określonego przez jej licznik
ZWŁOKA NA WYJŚCIE	Przejście kontrolera do trybu Uzbrojony	Rozbrojenie kontrolera Z chwilą upłynięcia czasu określonego przez jej licznik

3.7.10 Alarm Drzwi

Przez pojęcie Alarm Drzwi w kontrolerach PRxx1 rozumie się wystąpienie przynajmniej jednego z trzech wymienionych poniżej stanów:

- PREALARM
- DRZWI OTWARTE
- WEJŚCIE SIŁOWE

Alarm Drzwi może być sygnalizowany na wewnętrznym głośniku oraz na liniach wyjściowych. Rozróżnienie typu sygnalizowanego alarmu następuje poprzez rozpoznanie sposobu modulacji linii wyjściowej lub tonu głośnika, przy czym w przypadku wystąpienia więcej niż jednego stanu kontroler sygnalizuje alarm o najwyższym priorytecie.

Tabela 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 (patrz 3.7.7 Opcja: Nie sygnalizuj użycia kodu PIN pod przymusem).	Najwyższy	Pojedynczy impuls trwający 1 sekundę, powtarzany co 1 sekundę.

3.7.11 Opcja: Sygnalizuj Alarm Drzwi na wewnętrznym głośniku

Załączenie opcji powoduje sygnalizację wystąpienia dowolnego z trzech alarmów szczegółowych: PREALARM, DRZWI OTWARTE I WEJŚCIE SIŁOWE na wewnętrznym głośniku kontrolera.
Stan PREALARM informuje, że ktoś w czasie pięciu minut dokonał pięciu kolejnych prób użycia niedozwolonego identyfikatora (karty/PIN-u). Stan PREALARM może być sygnalizowany indywidualnie na wyjściu **[01]: Prealarm**, na wyjściu **[03]:Prealarm+Drzwi Otwarte**, na wyjściu **[05]:Prealarm+Wejście Siłowe** lub na wyjściu **[07]:Prealarm+Drzwi Otwarte+Wejście Siłowe.**

3.7.12 Opcja: Czasowa blokada kontrolera po 5 próbach identyfikacji

Po załączeniu tej opcji kontroler blokuje na czas pięciu kolejnych minut odczyt kart oraz kodów PIN w następstwie wystąpienia stanu PREALARM.

3.7.13 Opcja: Podtrzymanie Wyjścia 1 (REL1) przez kartę przy czytniku

Po załączeniu tej opcji kontroler podtrzymuje wyjście REL1 (umożliwiając w ten sposób podtrzymania otwarcia drzwi) tak długo jak karta uprawniona do otwierania drzwi znajduję się w pobliżu danego kontrolera z wbudowanym czytnikiem.

3.7.14 Anti-passback (APB)

W przypadku załączenia funkcji Anti-passback użytkownik jest zobligowany do logowania się naprzemiennie na czytniku wejściowym i wyjściowym z pomieszczenia/strefy. Kontroler w sposób ciągły rejestruje, na którym czytniku użytkownik się ostatnio zalogował i dane te przechowuje w tzw. Rejestrze APB. Stan tego rejestru wskazuje ostatnie miejsce logowania użytkowników.
Ze względu na sposób reakcji kontrolera na naruszanie zasad APB rozróżnia się:

- APB Twardy
- APB Miękki

Gdy na kontrolerze obowiązuje Anti-passback Miękki to każda próba naruszenia zasad APB wywołuje jedynie rejestrację zdarzenia Naruszenie APB, które informuje o fakcie naruszenia zasad APB, ale kontroler nie blokuje dostępu. Gdy na kontrolerze obowiązuje Anti-passback Twardy to próba naruszenia zasad APB wywołuje odmowę dostępu (dwa długie sygnały dźwiękowe) oraz rejestrację odpowiedniego zdarzenia (Naruszenie APB).

Opcja: APB z obsługą czujnika wejścia (ang. True APB)
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, z kolei gdy to nie nastąpi to kontroler nie zmienia stanu Rejestru APB i uznaje że użytkownik nie wszedł pomimo tego że kontroler przyznał mu dostęp. Działanie tej opcji wymaga, aby kontroler współpracował z czujnikiem otwarcia drzwi.

Harmonogram zerowania Rejestru APB
Operacja zerowania Rejestru APB powoduje, że wszyscy użytkownicy zarejestrowani w kontrolerze otrzymują status: Niezalogowany. Istnieje możliwość zdefiniowania dwóch godzin zerowania rejestru APB (w ciągu jednego dnia), lecz wyłącznie wtedy, gdy kontroler pracuje w Trybie Sieciowym z centralą CPR32-SE.

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

---

3.7.15 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 PRxx1 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 PRxx1 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 (ang. 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 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) miało miejsce ostatnie logowanie użytkowników. Każdy z użytkowników zarejestrowanych w kontrolerze posiada swój Status APB, który może przybierać cztery stany wymienione poniżej:

Tabela 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)
Zerowanie Rejestru APB powoduje, że wszyscy użytkownicy zarejestrowani w kontrolerze otrzymują status: Niezalogowany. Po tej operacji każdy użytkownik może dokonać pierwszego logowania na dowolnym z czytników (wejściowym lub wyjściowym), lecz potem, od momentu pierwszego logowania musi się już stosować do zasad APB, czyli logować się naprzemiennie raz na wejściu raz na wyjściu.
Zerowanie Rejestru APB jest wykonywane automatycznie po włączeniu zasilania, może być również wykonane następującymi metodami:

- Z poziomu linii wejściowej **[60]:Zeruj Rejestr APB**
- Z klawisza funkcyjnego **[60]:Zeruj Rejestr APB**
- Zdalnie (komendą) z komputera zarządzającego
- Automatycznie za pomocą Harmonogramu (tylko Tryb Sieciowy z CPR32-SE)

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.

3.7.16 Strefy Alarmowe

Strefa Alarmowa to grupa kontrolerów współbieżnie zmieniających swój aktualny stan uzbrojenia. Gdy dowolny kontroler należący do danej Strefy Alarmowej zmieni swój stan uzbrojenia (przy czym nie jest istotne co było przyczyną zmiany trybu uzbrojenia) reszta kontrolerów wchodzących w skład tej samej Strefy Alarmowej zostaje automatycznie przezbrojona w ten sam sposób. Funkcja współbieżnego przezbrajania jest realizowana przez centralę CPR32-SE. Centrala ta w sposób ciągły monitoruje stany uzbrojenia wszystkich kontrolerów w systemie i gdy jeden z nich zmieni swój stan uzbrojenia centrala przezbraja w ten sam sposób pozostałe kontrolery wchodzące w skład tej samej Strefy Alarmowej. W efekcie działania tego mechanizmu wszystkie kontrolery wchodzące w skład tej samej Strefy Alarmowej posiadają w każdej chwili działania systemu ten sam stan uzbrojenia.

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

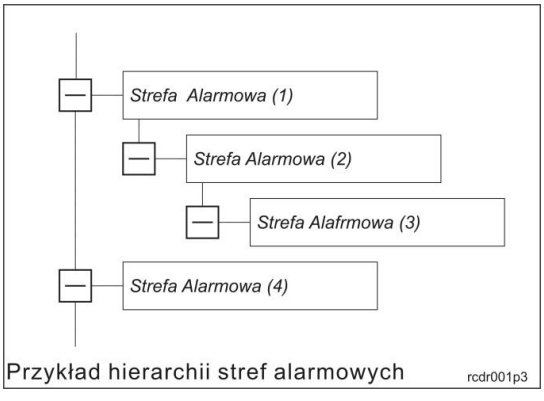
Gdy sterowanie stanem uzbrojenia kontrolera jest realizowane za pośrednictwem linii wejściowej **[03]:Przezbrajanie – klucz stały**, to stan uzbrojenia danego kontrolera nie może być zdalnie zmieniany przez urządzenie nadrzędne (centrala CPR32-SE) ani przez żaden inny mechanizm. Kontroler taki co prawda może należeć do jakiejś Strefy Alarmowej lecz należy mieć na uwadze że stan jego uzbrojenia będzie zależał jedynie od stanu linii wejściowej.

Hierarchia Stref Alarmowych

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

- Uzbrojenie strefy nadrzędnej powoduje uzbrojenie wszystkich stref względem niej podrzędnych
- Rozbrojenie strefy nadrzędnej nie ma wpływu na stan uzbrojenia stref podrzędnych
- Uzbrojenie strefy podrzędnej nie powoduje uzbrojenia strefy nadrzędnej
- Rozbrojenie strefy podrzędnej nie powoduje rozbrojenia strefy nadrzędnej

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



Rys. 8 Hierarchia stref alarmowych

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

3.8 Linie wejściowe

Kontroler PR411DR posiada osiem wbudowanych linii wejściowych (IN1-8), natomiast pozostałe kontrolery serii PRxx1 (PR311SE, PR611, PR621) posiadają po trzy wejścia (IN1-3). Opcjonalnie kontrolery tej serii mogą posiadać dwa dodatkowe wejścia znajdujące się na zewnętrznym module rozszerzeń XM-2 (IN1 i IN2 na XM-2). Każdą linię wejściową można indywidualnie skonfigurować, co do sposobu wyzwalania (NO/NC). 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. Wewnętrznie, każda linia wejściowa jest połączona z plusem zasilania za pośrednictwem rezystora 15kΩ. Średnie napięcie progowe pomiędzy logicznym stanem niskim a wysokim na wejściu wynosi około 3V względem masy (minusa zasilania). Każdej linii wejściowej można przypisać dowolną funkcję z listy poniżej:

Tabela 9. Linie wejściowe

Kod	Nazwa funkcji	Opis działania
[00]	**Wejście wyłączone**	Linia nie jest obsługiwana
[01]	**Czujnik otwarcia**	Linia jest dedykowana do podłączenia czujnika otwarcia drzwi. Gdy linia jest wyzwolona kontroler uznaje, że drzwi są otwarte, w przeciwnym razie uznaje, że drzwi są zamknięte
[02]	**Przycisk wyjścia**	Wyzwolenie linii powoduje zwolnienie drzwi na zasadach identycznych jak po przyznaniu dostępu. Wejście takie jest przeznaczone do podłączenia tzw. przycisku wyjścia lub innego typu kontaktu, którego użycie ma zwalniać drzwi
[03]	**Przezbrajanie – klucz stały**	Linia ta służy do sterowania stanem uzbrojenia kontrolera. 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
[04]	**Tylko rejestracja**	Stany elektryczne na tym wejściu nie wywołują żadnej reakcji z wyjątkiem zarejestrowania odpowiedniego zdarzenia
[05]	**Dozór napięcia sieci AC**	Wyzwolenie wejścia powoduje zarejestrowanie zdarzenia oraz załączenie flagi PROBLEM (patrz 3.7.9 Flagi Systemowe)
[06]	**Dozór stanu akumulatora**	Wyzwolenie wejścia powoduje zarejestrowanie zdarzenia oraz załączenie flagi PROBLEM (patrz 3.7.9 Flagi Systemowe)
[07]	**Dzwonek**	Wyzwolenie linii załącza sygnalizację dzwonka na wewnętrznym głośniku i opcjonalnie na linii wyjściowej **[15]:Dzwonek**
[08]	**Tamper**	Wyzwolenie linii jest interpretowane jako naruszenie obwodu antysabotażowego i powoduje załączenie flagi TAMPER (patrz 3.7.9 Flagi Systemowe)
[09]	**Włamanie**	Wyzwolenie linii jest interpretowane jako zadziałanie czujnika alarmowego i powoduje załączenie flagi WŁAMANIE (patrz 3.7.9 Flagi Systemowe)

[11]	**Blokada dostępu**	Gdy linia jest wyzwolona kontroler bezwarunkowo blokuje możliwość przyznania dostępu
[13]	**Blokada uzbrojenia**	Gdy linia jest wyzwolona kontroler nie może być uzbrojony
[14]	**Zwolnij drzwi – klucz stały**	Przez cały czas jak linia jest wyzwolona kontroler bezwarunkowo odblokowuje drzwi tzn. aktywuje wyjście sterujące elementem wykonawczym
[15]	**Włamanie – linia zwłoczna**	Jeśli kontroler jest w stanie uzbrojenia to wyzwolenie tej linii w stanie uzbrojenia uruchamia licznik ZWŁOKA NA WEJŚCIE. Jeśli przed upływem tego licznika nie nastąpi rozbrojenie to kontroler aktywuje flagę WŁAMANIE
[60]	**Zeruj rejestr APB**	Wyzwolenie linii zeruje Rejestr APB, wszystkim użytkownikom systemu zostaje nadany Status APB: Niezalogowany – patrz 3.7.15 Strefy Anti-passback (Strefy APB).
[61]	**Przezbrajanie – klucz chwilowy**	Wyzwolenie linii powoduje zmianę aktualnego stanu uzbrojenia kontrolera na przeciwny (patrz 3.6 Tryby Uzbrojenia)
[64]	**Ustaw drzwi w tryb Normalny**	Wyzwolenie linii ustawia tryb drzwi: Normalny (patrz 3.5 Tryby Drzwi)
[65]	**Ustaw drzwi w tryb Odblokowane**	Wyzwolenie linii ustawia tryb drzwi: Odblokowane (patrz 3.5 Tryby Drzwi)
[66]	**Ustaw drzwi w tryb War. Odblokowane**	Wyzwolenie linii ustawia tryb drzwi: War. Odblokowane (patrz 3.5 Tryby Drzwi)
[67]	**Ustaw drzwi w tryb Zablokowane**	Wyzwolenie linii ustawia tryb drzwi: Zablokowane (patrz 3.5 Tryby Drzwi)
[68]	**Załącz ŚWIATŁO**	Wyzwolenie linii załącza flagę ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
[69]	**Wyłącz ŚWIATŁO**	Wyzwolenie linii wyłącza flagę ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
[70]	**Przełącz ŚWIATŁO**	Wyzwolenie linii przełącza flagę ŚWIATŁO do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[71]	**Załącz AUX1**	Wyzwolenie linii załącza flagę AUX1 (patrz 3.7.9 Flagi Systemowe)
[72]	**Wyłącz AUX1**	Wyzwolenie linii wyłącza flagę AUX1 (patrz 3.7.9 Flagi Systemowe)
[73]	**Przełącz AUX1**	Wyzwolenie linii przełącza flagę AUX1 do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[74]	**Załącz AUX2**	Wyzwolenie linii załącza flagę AUX2 (patrz 3.7.9 Flagi Systemowe)
[75]	**Wyłącz AUX2**	Wyzwolenie linii wyłącza flagę AUX2 (patrz 3.7.9 Flagi Systemowe)
[76]	**Przełącz AUX2**	Wyzwolenie linii przełącza flagę AUX2 do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[78]	**Ustaw tryb Rozbrojony – klucz chwilowy**	Wyzwolenie linii przełącza kontroler do trybu rozbrojenia (patrz 3.6 Tryby Uzbrojenia)

[79]	**Ustaw tryb Uzbrojony – klucz chwilowy**	Wyzwolenie linii przełącza kontroler do trybu uzbrojenia (patrz 3.6 Tryby Uzbrojenia)
[80]	**Ustaw tryb Karta lub PIN**	Wyzwolenie linii ustawia tryb Karta lub PIN (patrz 3.4 Tryby Identyfikacji)
[81]	**Ustaw tryb Tylko Karta**	Wyzwolenie linii ustawia tryb Tylko Karta (patrz 3.4 Tryby Identyfikacji)
[82]	**Ustaw tryb Tylko PIN**	Wyzwolenie linii ustawia tryb Tylko PIN (patrz 3.4 Tryby Identyfikacji)
[83]	**Ustaw tryb Karta i PIN**	Wyzwolenie linii ustawia tryb Karta i PIN (patrz 3.4 Tryby Identyfikacji)

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

3.9 Linie wyjściowe

Kontrolery serii PRxx1 posiadają dwa wyjścia tranzystorowe (IO1 i IO2) oraz jedno wyjście przekaźnikowe (REL1). Zastosowanie modułu XM-2 zwiększa ilość wyjść przekaźnikowych o kolejne dwa. Wyjścia tranzystorowe IO1 oraz IO2 w stanie normalnym reprezentują stan wysokiej impedancji (rozwarcia), a w stanie wyzwolenia podają minus zasilania. Jeśli kontroler nie współpracuje z zewnętrznym czytnikiem PRT ani modułem rozszerzeń XM-2 to również linie CLK i DTA można wykorzystać jako linie wyjściowe. Wszystkie wyjścia są liniami o programowanej funkcji:

Uwaga: Kontroler PR411DR oferuje dodatkowe wyjście przekaźnikowe (REL2), które można programować na identycznych zasadach jak pozostałe wyjścia.

Tabela 10. Linie wyjściowe

Kod	Nazwa funkcji	Opis działania
[00]	**Tryb Rozbrojony**	Gdy kontroler jest uzbrojony linia ta jest wyłączona, gdy kontroler jest rozbrojony linia ta jest załączona (patrz 3.6 Tryby Uzbrojenia)
[01]	**PREALARM**	Wyjście sygnalizuje stan PREALARM (patrz 3.7.10 Alarm Drzwi)
[02]	**DRZWI OTWARTE**	Wyjście sygnalizuje stan DRZWI OTWARTE (patrz 3.7.10 Alarm Drzwi)
[03]	**PREALARM + DRZWI OTWARTE**	Wyjście sygnalizuje stan PREALARM + DRZWI OTWARTE (patrz 3.7.10 Alarm Drzwi)
[04]	**WEJŚCIE SIŁOWE**	Wyjście sygnalizuje stan WEJŚCIE SIŁOWE (patrz 3.7.10 Alarm Drzwi)
[05]	**PREALARM + WEJŚCIE SIŁOWE**	Wyjście sygnalizuje stan PREALARM + WEJŚCIE SIŁOWE (patrz 3.7.10 Alarm Drzwi)
[06]	**DRZWI OTWARTE + WEJŚCIE SIŁOWE**	Wyjście sygnalizuje stan DRZWI OTWARTE + WEJŚCIE SIŁOWE (patrz 3.7.10 Alarm Drzwi)
[07]	**PREALARM +DRZWI OTWARTE + WEJŚCIE SIŁOWE**	Wyjście sygnalizuje stan PREALARM + DRZWI OTWARTE+ WEJŚCIE SIŁOWE (patrz 3.7.10 Alarm Drzwi)

[09]	**Przyznanie dostępu**	Wyjście to zostaje załączone w momencie, gdy kontroler przyzna dostęp, czas załączenia wyjścia określa parametr Czas 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 2 sekund każdorazowo, gdy kontroler odmówi przyznania dostępu
[14]	**Logowanie na terminalu ID0**	Wyjście zostaje załączone w momencie zalogowania na terminalu ID0 i trwa w tym stanie do momentu, gdy wystąpi logowanie na terminalu ID1. Zazwyczaj funkcja ta jest wykorzystywana do sterowania kierunkiem obrotu bramki typu obrotowej (tripod) lub sterowania przejściem dwukierunkowym wtedy wskazuje ono kierunek przejścia
[15]	**Dzwonek**	Wyjście jest załączane na czas 2 sekund w momencie wystąpienia sygnalizacji dzwonka. Sygnalizację dzwonka można wyzwolić przy pomocy klawisza funkcyjnego lub linii wejściowej
[18]	**Tryb drzwi – Normalne**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Normalny (patrz 3.5 Tryby Drzwi)
[19]	**Tryb drzwi - Odblokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Odblokowane (patrz 3.5 Tryby Drzwi)
[20]	**Tryb drzwi – War. Odblokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: War. Odblokowane (patrz 3.5 Tryby Drzwi)
[21]	**Tryb drzwi - Zablokowane**	Wyjście jest załączone przez cały czas jak na kontrolerze obowiązuje tryb drzwi: Zablokowane (patrz 3.5 Tryby Drzwi)
[25]	**Impuls na rozbrojenie**	Wyjście jest wyzwalane na czas ok. 2s za każdym razem gdy kontroler przejdzie do stanu rozbrojenia (patrz 3.6 Tryby Uzbrojenia)
[26]	**Impuls na uzbrojenie**	Wyjście jest wyzwalane na czas ok. 2s za każdym razem, gdy kontroler przejdzie do stanu uzbrojenia (patrz 3.6 Tryby Uzbrojenia)
[37]	**Utrata napięcia sieci AC**	Wyjście przechodzi do stanu aktywnego, gdy brak napięcia sieci występuje przez czas dłuższy niż ok. 6minut. Zanik sygnalizacji na wyjściu następuje po upływie ok. 1 min od powrotu napięcia sieci. Funkcja dostępna jedynie w PR411DR.
[38]	**Niski stan baterii**	Wyjście przechodzi do stanu aktywnego gdy napięcie na akumulatorze osiągnie wartość poniżej ok. 11,7 V i występuje przez czas dłuższy niż ok. 8minut. Zanik sygnalizacji na wyjściu następuje po upływie ok. 6 min od powrotu napięcia sieci. Funkcja dostępna jedynie w PR411DR.
[64]	**ŚWIATŁO**	Wyjście to sygnalizuje aktualny stan flagi ŚWIATŁO. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone (patrz 3.7.9 Flagi Systemowe)

[65]	**TAMPER**	Wyjście to sygnalizuje aktualny stan flagi TAMPER. Jeśli flaga jest załączona, wyjście jest załączone, jeśli flaga jest wyłączona, wyjście też jest wyłączone (patrz 3.7.9 Flagi Systemowe)
[66]	**AUX1**	Wyjście to sygnalizuje aktualny stan flagi AUX1 (patrz 3.7.9 Flagi Systemowe)
[67]	**AUX2**	Wyjście to sygnalizuje aktualny stan flagi AUX2 (patrz 3.7.9 Flagi Systemowe)
[68]	**WŁAMANIE**	Wyjście to sygnalizuje aktualny stan flagi WŁAMANIE (patrz 3.7.9 Flagi Systemowe)
[69]	**WYMUSZENIE**	Wyjście to sygnalizuje aktualny stan flagi WYMUSZENIE (patrz 3.7.9 Flagi Systemowe)
[70]	**PROBLEM**	Wyjście to sygnalizuje aktualny stan flagi PREALARM (patrz 3.7.9 Flagi Systemowe)
[71]	**ZWŁOKA NA WEJŚCIE**	Wyjście jest załączone przez cały czas, w którym licznik ZWŁOKA NA WEJŚCIE jest w trakcie odliczania (patrz 3.7.9 Flagi Systemowe)
[72]	**ZWŁOKA NA WYJŚCIE**	W Wyjście jest załączone przez cały czas, w którym licznik ZWŁOKA NA WYJŚCIE jest w trakcie odliczania (patrz 3.7.9 Flagi Systemowe)
[80]	**Tryb Karta lub PIN**	Wyjście załączone, gdy na kontrolerze obowiązuje tryb Karta lub PIN (patrz 3.4 Tryby Identyfikacji)
[81]	**Tryb Tylko Karta**	Wyjście załączone, gdy na kontrolerze obowiązuje tryb Tylko Karta (patrz 3.4 Tryby Identyfikacji)
[82]	**Tryb Tylko PIN**	Wyjście załączone, gdy na kontrolerze obowiązuje tryb Tylko PIN (patrz 3.4 Tryby Identyfikacji)
[83]	**Tryb Karta i PIN**	Wyjście załączone, gdy na kontrolerze obowiązuje tryb Karta i PIN (patrz 3.4 Tryby Identyfikacji)
[97]	**Zamek drzwi – wejście**	Wyjście jest wyzwalane na czas określony przez parametr Czas na Wejście gdy dostęp został przyznany 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 przyznany z poziomu terminala ID1. 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

3.10 Klawisze funkcyjne

Klawisze funkcyjne dostępne są na niektórych czytnikach serii PRT (Roger) jak też na kontrolerach PR311SE. Użytkownik może korzystać z czterech klawiszy funkcyjnych (jeżeli klawisze funkcyjne są dostępne na obu Terminalach ID0 oraz ID1) lub dwóch klawiszy funkcyjnych (jeżeli są one

dostępne jedynie na Terminalu ID0 albo ID1). W systemie RACS nie jest istotne czy Klawisze Funkcyjne znajdują się na Terminalu ID0 czy ID1 i mogą one być indywidualnie zaprogramowane za pomocą funkcji podanych w Tabeli 11.

Tabela 11. Klawisze funkcyjne		
Kod	Nazwa funkcji	Opis działania
[00]	**Brak funkcji**	Klawisz funkcyjny, do którego nie przypisano żadnych działań
[01]	**Dzwonek**	Użycie klawisza powoduje załączenie sygnalizacji dzwonka
[02]	**Zwolnij drzwi**	Użycie klawisza zwalnia kontrolowane drzwi na identycznych zasadach jak po przyznaniu dostępu
[04]	**Tylko rejestracja**	Każde użycie przycisku zostaje rejestrowane w pamięci zdarzeń, lecz kontroler nie podejmuje żadnych dodatkowych działań
[09]	**WŁAMANIE**	Użycie klawisza włącza flagę WŁAMANIE (patrz 3.7.9 Flagi Systemowe)
[60]	**Zeruj rejestr APB**	Użycie klawisza zeruje (resetuje) rejestr APB (patrz 3.7.15 Strefy Anti-passback (Strefy APB))
[61]	**Zmień stan uzbrojenia – klucz chwilowy**	Użycie klawisza przezbraja kontroler, użycie klawisza nie implikuje jednak, że kontroler zmieni stan a jedynie, że dokona próby zmiany swojego stanu uzbrojenia i jeśli nie będzie żadnych przeszkód logicznych dokona zmiany stanu uzbrojenia
[64]	**Ustaw drzwi w tryb Normalny**	Użycie klawisza ustawia tryb drzwi: Normalny (patrz 3.5 Tryby Drzwi)
[65]	**Ustaw drzwi w tryb Odblokowane**	Użycie klawisza ustawia tryb drzwi: Odblokowane (patrz 3.5 Tryby Drzwi)
[66]	**Ustaw drzwi w tryb War. Odblokowane**	Użycie klawisza ustawia tryb drzwi: Warunkowo Odblokowane (patrz 3.5 Tryby Drzwi)
[67]	**Ustaw drzwi w tryb Zablokowane**	Użycie klawisza ustawia tryb drzwi: Zablokowane (patrz 3.5 Tryby Drzwi)
[68]	**Załącz ŚWIATŁO**	Użycie klawisza załącza flagę ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
[69]	**Wyłącz ŚWIATŁO**	Użycie klawisza wyłącza flagę ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
[70]	**Przełącz ŚWIATŁO**	Użycie klawisza przełącza flagę ŚWIATŁO do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[71]	**Załącz AUX1**	Użycie klawisza załącza flagę AUX1 (patrz 3.7.9 Flagi Systemowe)
[72]	**Wyłącz AUX1**	Użycie klawisza wyłącza flagę AUX1 (patrz 3.7.9 Flagi Systemowe)
[73]	**Przełącz AUX1**	Użycie klawisza przełącza flagę AUX1 do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[74]	**Załącz AUX2**	Użycie klawisza załącza flagę AUX2 (patrz 3.7.9 Flagi Systemowe)
[75]	**Wyłącz AUX2**	Użycie klawisza wyłącza flagę AUX2 (patrz 3.7.9 Flagi Systemowe)

[76]	**Przełącz AUX2**	Użycie klawisza przełącza flagę AUX2 do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)
[78]	**Ustaw tryb Rozbrojony**	Użycie klawisza przełącza kontroler do trybu rozbrojenia (patrz 3.6 Tryby Uzbrojenia)
[79]	**Ustaw tryb Uzbrojony**	Użycie klawisza przełącza kontroler do trybu uzbrojenia (patrz 3.6 Tryby Uzbrojenia)
[80]	**Ustaw tryb Karta lub PIN**	Użycie klawisza ustawia tryb Karta lub PIN (patrz 3.4 Tryby Identyfikacji)
[81]	**Ustaw tryb Tylko Karta**	Użycie klawisza ustawia tryb Tylko Karta (patrz 3.4 Tryby Identyfikacji)
[82]	**Ustaw tryb Tylko PIN**	Użycie klawisza ustawia tryb Tylko PIN (patrz 3.4 Tryby Identyfikacji)
[83]	**Ustaw tryb Karta i PIN**	Użycie klawisza ustawia tryb Karta i PIN (patrz 3.4 Tryby Identyfikacji)

3.11 Karty Funkcyjne

Karty Funkcyjne to zwykłe karty zbliżeniowe, którym przypisano w trakcie konfiguracji specyficzne funkcje programujące. Karty Funkcyjne mogą być definiowane manualnie z klawiatury (patrz IV. Programowanie) lub zdalnie z poziomu komputera PC (patrz instrukcja programu PR Master). Do jednej funkcji programowania użytkownika można przypisać jedną lub więcej kart zbliżeniowych. Każda Karta funkcyjna może mieć przypisaną jedną i tylko jedną funkcję programującą:

- Funkcja [01]:Dodaj kartę NORMAL (patrz 3.3 Użytkownicy)
- Funkcja [03]:Dodaj kartę SWITCHER FULL (patrz 3.3 Użytkownicy)
- Funkcja [05]:Dodaj kartę SWITCHER LIMITED (patrz 3.3 Użytkownicy)
- Funkcja [06]:Usuń kartę
- Funkcja [07]:Usuń wszystkie karty
- Funkcja [08]:Ustaw drzwi w tryb Normalny (patrz 3.5 Tryby Drzwi)
- Funkcja [09]:Ustaw drzwi w tryb Odblokowane (patrz 3.5 Tryby Drzwi)
- Funkcja [10]:Ustaw drzwi w tryb Warunkowo Odblokowane (patrz 3.5 Tryby Drzwi)
- Funkcja [11]:Ustaw drzwi w tryb Zablokowane (patrz 3.5 Tryby Drzwi)
- Funkcja [12]:Załącz AUX1 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [13]:Wyłącz AUX1 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [14]:Przełącz AUX1 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [15]:Załącz ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
- Funkcja [16]:Wyłącz ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
- Funkcja [17]:Przełącz ŚWIATŁO (patrz 3.7.9 Flagi Systemowe)
- Funkcja [19]:Dodaj wiele kart
- Funkcja [20]:Załącz AUX2 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [21]:Wyłącz AUX2 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [22]:Przełącz AUX2 (patrz 3.7.9 Flagi Systemowe)
- Funkcja [24]:Dodaj kartę gościa (patrz 3.3 Użytkownicy)
- Funkcja [25]:Usuń karty wszystkich gości (patrz 3.3 Użytkownicy)

IV. PROGRAMOWANIE

Kontrolery serii PRxx1 mogą być programowane manualnie z klawiatury lub zdalnie z poziomu komputera PC. Więcej informacji na temat programowania zdalnego można znaleźć w instrukcji programu PR Master. Programowanie manualne można przeprowadzić lokalnie z poziomu klawiatury (PR611 oraz PR311SE) lub z poziomu dodatkowego czytnika serii PRT dołączonego do kontrolera (czytnik ten powinien posiadać klawiaturę i być skonfigurowany do trybu RACS adres ID0 – patrz 3.2.3 Interfejs RACS Clock & Data). Programowanie urządzenia polega na określeniu Funkcji Użytkownika (patrz 4.2 Funkcje Użytkownika) oraz wprowadzaniu poleceń w trybie Programowania Instalatora (patrz 4.3 Programowanie Instalatora). Funkcje Użytkownika umożliwiają administrowanie kartami oraz kodami PIN a także mogą być wykorzystane do sterowania niektórymi funkcjami kontrolera (np. sterowanie Trybem Identyfikacji oraz Trybem Drzwi). Programowanie Instalatora służy do szczegółowej konfiguracji urządzenia a w szczególności do określenia funkcji linii wejściowych oraz wyjściowych oraz innych opcji jego działania.
Jeżeli system kontroli dostępu jest zarządzany i konfigurowany z komputera PC za pomocą oprogramowania PR Master to nie należy stosować równolegle żadnych innych metod programowania gdyż konfiguracja systemu może w ten sposób zostać uszkodzona w wyniku desynchronizacji bazy danych PR Master z ustawieniami wprowadzonymi ręcznie.

Uwaga: Programowanie Instalatora jak też Funkcje Użytkownika mogą być wprowadzane zarówno na klawiaturze kontrolera (terminal ID1) jak i z poziomu czytnika zewnętrznego (terminal ID0) dołączonego do kontrolera.

4.1 Reset Ustawień – Programowanie Identyfikatora MASTER oraz Adresu ID

Reset Ustawień zeruje aktualne ustawienia kontrolera, przywraca ustawienia fabryczne oraz umożliwia zaprogramowanie nowej karty i/lub PIN-u MASTER a także nowego adresu kontrolera. Po wykonaniu Resetu Ustawień kontroler automatycznie przechodzi do normalnego trybu pracy i wchodzi do stanu Uzbrojony (LED STATUS świeci na czerwono).

Uwaga: Jeśli użytkownikowi MASTER nie zostanie zaprogramowany żaden identyfikator (tzn. ani karta ani PIN) to później nie będzie możliwe wejście do trybu Programowania Instalatora.

Uproszczona procedura resetu ustawień bez programowania adresu
Metoda ta umożliwia zaprogramowanie identyfikatora MASTER (karta) bez możliwości programowania numeru ID kontrolera.

- Usuń wszystkie zewnętrzne podłączenia z linii CLK i DTA
- Wykonaj mostek pomiędzy liniami CLK i DTA
- Dokonaj restartu urządzenia (wyłącz/załącz napięcie zasilania lub zewrzyj na moment kontakty RST) – kontroler zapali wszystkie wskaźniki LED
- Usuń mostek pomiędzy liniami CLK i DTA – kontroler zgasi LED-y, po czym zacznie pulsować wskaźnik LED OTWARTE (zielony)
- Gdy wskaźnik LED OTWARTE pulsuje odczytaj dowolną kartę – będzie to nowa karta MASTER
- Kontroler się samoczynnie zrestartuje i powróci do normalnej pracy a dalsze ustawienia (włączając w to adres ID kontrolera) można kontynuować w trybie Programowania Instalatora (patrz 4.3 Programowanie Instalatora) lub za pomocą Funkcji Użytkownika (patrz 4.2 Funkcje Użytkownika).

Uproszczona procedura resetu pamięci dla kontrolera bez klawiatury
Metoda ta umożliwia wyzerowanie ustawień kontrolera, zaprogramowanie nowej karty MASTER oraz ustawienie adresu kontrolera.

- Usuń wszystkie zewnętrzne podłączenia z linii CLK i IN3

- Wykonaj mostek pomiędzy liniami CLK i IN3
- Dokonaj restartu urządzenia (wyłącz/załącz napięcie zasilania lub zewrzyj na moment kontakty RST) – kontroler zapali wszystkie wskaźniki LED
- Usuń mostek pomiędzy liniami CLK i IN3 – kontroler zgasi LED-y, po czym wskaźniki LED STATUS (czerwony) i LED OTWARTE (zielony) będą pulsowały
- Gdy wskaźniki LED STATUS i LED OTWARTE pulsują odczytaj dowolną kartę – będzie to nowa karta MASTER, kontroler zapamięta nową kartę i przejdzie do kolejnego kroku, w którym będzie programowany jego adres
- Zbliż do czytnika kontrolera nową kartę MASTER tyle razy ile ma wynosić pierwsza cyfra adresu ID kontrolera, odczekaj na dwa krótkie sygnały i przejdź do kolejnego kroku
- Zbliż do czytnika kontrolera nową kartę MASTER tyle razy ile ma wynosić druga cyfra adresu ID kontrolera
- Kontroler się samoczynnie zrestartuje i powróci do normalnej pracy

Pełna procedura resetu pamięci

Procedura ta może być wykonana bezpośrednio z poziomu klawiatury kontrolera (o ile ją posiada) lub z poziomu dodatkowego czytnika serii PRT dołączonego do kontrolera za pośrednictwem linii CLK i DTA, przy czym czytnik ten musi być skonfigurowany do trybu **RACS adres ID0** i posiadać klawiaturę. Pełna procedura Resetu Pamięci umożliwia zaprogramowanie karty i PIN-u MASTER oraz umożliwia ustawienie nowego adresu (numeru ID).

- Usuń wszystkie zewnętrzne podłączenia z linii CLK i DTA
- Wykonaj mostek pomiędzy liniami CLK i DTA
- Dokonaj restartu urządzenia (wyłącz/załącz napięcie zasilania lub zewrzyj na moment kontakty RST) – kontroler zapali wszystkie wskaźniki LED
- Usuń mostek pomiędzy liniami CLK i DTA – kontroler zgasi LED-y, po czym zacznie pulsować wskaźnik LED OTWARTE (zielony)
- Jeśli dany kontroler nie posiada klawiatury to nie wyłączając zasilania podłącz do niego zewnętrzny czytnik serii PRT skonfigurowany do trybu RACS adres ID0 lub ID1, po czym dalsze kroki wykonuj z poziomu tego czytnika. Jeśli kontroler posiada jednak klawiaturę to pomiń ten krok i przejdź do kroku następnego
- Wprowadź nowy kod MASTER PIN (3-6 cyfr) i zakończ go klawiszem [#] lub pomiń ten krok naciskając tylko klawisz [#]
- Odczytaj dowolną kartę – będzie to nowa karta MASTER lub pomiń ten krok naciskając klawisz [#]
- Wprowadź dwie cyfry (od 00 do 99), cyfry te programują nowy adres ID kontrolera lub naciśnij tylko [#] a kontroler samoczynnie przyjmie adres ID=00
- Kontroler się samoczynnie zrestartuje i powróci do normalnej pracy

---

Uwagi:
1. Do momentu zaprogramowania nowego identyfikatora INSTALLER identyfikator MASTER pełni również role identyfikatora INSTALLER (MASTER=INSTALLER). Może zatem służyć do wejścia do trybu Programowania Instalatora (patrz 4.3 Programowanie Instalatora).
2. Adres kontrolera musi się zawierać w przedziale ID=00-99

W kontrolerach serii PRxx1 istnieje możliwość zaprogramowania stałego adresu ID kontrolera (tzw. FixedID). Stały adres ID można ustawić w trakcie procesu aktualizacji oprogramowania wbudowanego (firmware) w urządzenie za pomocą programu Roger ISP (dostępnego na stronie internetowej www.roger.pl). Ustawienie FixedID wyklucza inne metody programowania adresu takie jak programowe ustawianie adresu ID za pomocą programu PR Master na komputerze PC oraz manualne ustawienie adresu ID (w trakcie resetu pamięci lub za pomocą zworek w przypadku kontrolera PR411DR). Aby dokonać zmiany adresu stałego należy zatem dokonać ponownej aktualizacji oprogramowania wbudowanego (firmware) w urządzenie.
W przypadku kontrolera PR411DR jak już wspomniano wcześniej adres ID można również ustawić za pomocą zworek umieszczonych na płycie modułu. Całkowity zakres adresów ID dla takiego ustawienia mieści się w przedziale 0-127. Przy czym jeśli ustawiony adres zawiera się w przedziale 00-99 to czytnik nie zezwala na zmianę tego adresu ID na drodze programowej za pomocą

komputera PC czy manualnie. Z kolei dla adresów ID powyżej 99 można wprowadzać zmiany na drodze programowej.

4.2 Funkcje Użytkownika

Funkcje Użytkownika w kontrolerach PRxx1 to pewne czynności programujące dostępne z poziomu wbudowanej klawiatury kontrolera lub klawiatury znajdującej się na zewnętrznym czytniku, przy czym czytnik ten musi pracować w standardzie RACS. Użycie Funkcji Użytkownika może nastąpić zarówno wtedy, gdy kontroler znajduje się w stanie uzbrojenia jak i rozbrojenia (patrz 3.6 Tryby Uzbrojenia). Domyślnie, wprowadzenia każdej Funkcji Użytkownika wymaga użycia identyfikatora MASTER niemniej wymóg ten może zostać usunięty w odniesieniu do wybranych (lub wszystkich) Funkcji Użytkownika (patrz 4.3 Programowanie Instalatora, funkcja [69]). Każda Funkcja Użytkownika posiada swój dwu-cyfrowy identyfikator (numer funkcji). Z chwilą wprowadzenia (naciśnięcia) pierwszej cyfry identyfikującej konkretną komendę zaczynają pulsować wskaźnik LED SYSTEM oraz LED OTWARTE i pozostają w tym stanie aż do momentu poprawnego ukończenia komendy lub wystąpienia błędu programowania.

Oznaczenia:
<AUTH> - autoryzacja poprzez podanie identyfikatora MASTER lub identyfikatora użytkownika, który posiada prawo autoryzacji. Prawa do autoryzacji można ustawić za pomocą oprogramowania PR Master lub funkcji [69] w trybie Instalatora (patrz 4.3 Programowanie Instalatora)
INSTALLER - identyfikator INSTALLER (karta lub PIN). Jeżeli nie został zdefiniowany to w zamian można stosować identyfikator MASTER
MASTER - identyfikator MASTER (karta lub PIN)
[NNN] - trzycyfrowy numer ID użytkownika 001-999 (patrz 3.3 Użytkownicy)
<Karta> - kod karty zbliżeniowej lub podany z klawiatury numer karty zakończony [#]
<PIN> - kod PIN (3 do 6 znaków), wprowadzenie zawsze zakańczać klawiszem [#]
(SK) - sygnał kontynuacji/zachęty (dwa krótkie sygnały akustyczne), zwykle oznaczają oczekiwanie na dalszy ciąg komendy (naciśnięcie kolejnego klawisza, odczyt kodu lub wprowadzenie karty)
OK – sygnał OK. (trzy bardzo krótkie sygnały akustyczne), zwykle potwierdzają poprawne zakończenie wprowadzenie komendy
Error – sygnał błędu (jeden długi sygnał akustyczny)

[10#]<AUTH> (SK) [10] - Usuwanie wszystkich użytkowników z pamięci kontrolera
Komenda kasuje wszystkie karty i kody PIN wszystkich użytkowników (w tym użytkowników typu Gość).

[11#]<AUTH> (SK) [NNN] <karta> - Programowanie karty dla użytkownika o ID=NNN
Odczytana karta będzie przypisana użytkownikowi o numerze identyfikacyjnym ID=NNN.

[12#]<AUTH> (SK) [NNN]<PIN> - Programowanie kodu PIN dla użytkownika o ID=NNN
Wprowadzony kod PIN będzie przypisany do użytkownika o numerze identyfikacyjnym ID=NNN.

[13#]<AUTH> (SK) [NNN] - Usuwanie użytkownika o ID=NNN z pamięci kontrolera
Użytkownik o ID=NNN zostanie usunięty z pamięci kontrolera.

[14#]<AUTH> (SK) [NNN] - Sprawdzenie czy numer ID=NNN jest wolny
Jeżeli użytkownik o numerze ID=NNN nie posiada ani karty ani kodu PIN kontroler wygeneruje sygnał OK. (trzy bardzo krótkie sygnały akustyczne), jeśli jednak użytkownik ten posiada już kartę lub kod PIN to urządzenie wygeneruje sygnał błędu (sygnał długi).

[15#]<AUTH> (SK) <Karta-1>(SK) <Karta-2>(SK)…<Karta-N> [#] - Seryjne dodawanie wielu kart
Funkcja ta dodaje nowych użytkowników typu NORMAL z kartami. Każdorazowo po wczytaniu kolejnej karty czytnik generuje sygnał zachęty (¤ ¤), zakończenie funkcji następuje po naciśnięciu

[#] lub automatycznie po czasie ok. 20 sekund od momentu ostatnio odczytanej karty. Nowo dodani użytkownicy są wpisywani na pierwsze znalezione wolne pozycje pamięci z zakresu 100-999.

[16#]<AUTH> (SK) [NNN][P] - Załączanie opcji P (nadawanie uprawnienia) użytkownikowi ID=NNN.
Wartość P może być z zakresu 1-8 (patrz również 3.3.2 Opcje (uprawnienia) użytkowników) i oznacza:
P = [1] Całkowitą blokada dostępu
P = [2] Uprawnienie do autoryzacji użycia klawisza F1 na terminalu ID0
P = [3] Uprawnienie do autoryzacji użycia klawisza F2 na terminalu ID0
P = [4] Uprawnienie do autoryzacji użycia klawisza F1 na terminalu ID1
P = [5] Uprawnienie do autoryzacji użycia klawisza F2 na terminalu ID1
P = [6] Uprawnienie do wykonywania Funkcji Użytkownika
P = [7] Uprawnienie do przezbrajania kontrolera
P = [8] Uprawnienie do autoryzacji użycia Kart Funkcyjnych

[17#]<AUTH> (SK) [NNN][P] - Wyłączanie opcji P (pozbawianie uprawnienia) użytkownikowi NNN.
Znaczenie parametru [P] jak w wcześniejszej funkcji.

[18#]<AUTH> (SK) [P] - Wyłączanie opcji P (pozbawianie uprawnienia) u wszystkich użytkowników.
Znaczenie parametru [P] jak w wcześniejszej funkcji.

[20#]<AUTH> (SK) [20] - Kasowanie wszystkich użytkowników typu Gość
Komenda kasuje wszystkie karty i kody PIN należące do użytkowników typu Gość (patrz 3.3.1 Użytkownicy zwykli i Goście).

[21#]<AUTH> (SK) [G] <Karta> - Definiowanie karty dla użytkownika typu GOŚĆ
Parametr [G] może przybierać wartość z zakresu 0-7 i oznacza numer Gościa na liście (patrz 3.3.1 Użytkownicy zwykli i Goście).

[22#]<AUTH> (SK) [G]<PIN> - Definiowanie kodu PIN dla Gościa
Parametr [G] może przybierać wartość z zakresu 0-7 i oznacza numer Gościa na liście (patrz 3.3.1 Użytkownicy zwykli i Goście).

[23#]<AUTH> (SK) [G] - Kasowanie Gościa
Parametr [G] może przybierać wartość z zakresu 0-7 i oznacza numer Gościa na liście (patrz 3.3.1 Użytkownicy zwykli i Goście).

[31#]<AUTH> (SK) [F] - Sterowanie flagą AUX1
Programuj: [F] = [0] aby wyłączyć flagę, [F] = [1] aby załączyć flagę lub [F] = [2] aby przełączyć flagę do stanu przeciwnego (patrz 3.7.9 Flagi Systemowe)

[32#]<AUTH> (SK) [F] - Sterowanie flagą AUX2
Znaczenie parametru [F] jak w funkcji [31] (patrz 3.7.9 Flagi Systemowe).

[33#]<AUTH> (SK) [F] - Sterowanie flagą ŚWIATŁO
Znaczenie parametru [F] jak w funkcji [31] (patrz 3.7.9 Flagi Systemowe).

[34#]<AUTH> (SK) [T] - Sterowanie Trybem Drzwi
Programuj (patrz również 3.5 Tryby Drzwi):
[T] = [0] aby ustawić tryb Normalny,
[T] = [1] aby ustawić tryb Odblokowane,
[T] = [2] aby ustawić tryb Warunkowo Odblokowane,
[T] = [3] aby ustawić tryb Zamknięte

[35#]<AUTH> (SK) [A] - Sterowanie Trybem Identyfikacji
Programuj: [A] = [0] aby ustawić tryb Karta lub PIN, [A] = [1] aby ustawić tryb Tylko Karta, [A] = [2] aby ustawić tryb Tylko PIN, [A] = [3] aby ustawić tryb Karta i PIN (patrz również 3.4 Tryby Identyfikacji)

Uwaga: Po ustawieniu trybu Tylko PIN karta MASTER nie działa natomiast po ustawieniu trybu Tylko Karta nie działa PIN MASTER.

[39#]<AUTH> - **Załącza flagę WŁAMANIE**
Polecenie załącza flagę WŁAMANIE (patrz 3.7.9 Flagi Systemowe).

4.3 Programowanie Instalatora

W trybie tym możliwe jest szczegółowe skonfigurowanie urządzenia celem dopasowania go do indywidualnych warunków instalacji. Wejście do tego trybu może nastąpić zarówno z trybu Uzbrojony jak i z trybu Rozbrojony (patrz 3.6 Tryby Uzbrojenia) przez podanie komendy:

[01#](SK) <MASTER> (SK) <INSTALLER> Wejście do trybu Programowania Instalatora
Po wejściu do trybu Programowanie Instalatora świecą wskaźniki LED SYSTEM (na pomarańczowo) i LED STATUS (na czerwono). Z chwilą naciśnięcia pierwszego klawisza wskazującego numer funkcji obydwa zapalone wskaźniki LED zaczynają pulsować i trwają w tym stanie do momentu zakończenia funkcji programującej lub do momentu wystąpienia błędu w programowaniu. Po wystąpieniu błędu programowania kontroler wychodzi z funkcji nie opuszcza jednak trybu Programowania Instalatora. Wystąpienie błędu w funkcji sygnalizowane jest długim sygnałem akustycznym i powoduje zanik pulsowania wskaźników LED. Gdy funkcja programująca zostanie prawidłowo ukończona kontroler generuje sygnał OK (trzy krótkie sygnały akustyczne) i wyłącza pulsowanie wskaźników LED, nadal pozostaje w trybie Programowania Instalatora i jest gotowy do przyjęcia kolejnej funkcji programującej. Po wyjściu z trybu Programowania Instalatora urządzenie powraca do takiego trybu pracy (Uzbrojony/Rozbrojony) w jakim znajdowało się przed wejściem do trybu programowania. Wyjście z trybu programowania następuje automatycznie, gdy w czasie 4 minut nie nastąpi użycie jakiegokolwiek klawisza lub może nastąpić w następstwie użycia komendy: **[00#]Wyjście z trybu Programowania Instalatora**

[40][MN] - Programowanie adresu kontrolera (numeru ID)
Cyfry [MN] wskazują nowy numer ID kontrolera z dozwolonego zakresu 00-99. Wartość domyślna: <ID=00> lub inna zaprogramowana w trakcie resetu pamięci (patrz 4.1 Reset Ustawień – Programowanie Identyfikatora MASTER oraz Adresu ID).

[41][P][FW] - Programowanie funkcji dla linii wejściowej IN1
Parametr [P] określa typ linii: [P]=0 dla linii NO lub [P]=1 dla linii NC, natomiast parametr [FW] określa funkcję wejścia (patrz 3.8 Linie wejściowe). Wartość domyślna: <FW=01>, Czujnik otwarcia, NC.

[42][P][FW] - Programowanie funkcji dla linii wejściowej IN2
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=02>, Przycisk wyjścia, NO.

[43][P][FW] - Programowanie funkcji dla linii wejściowej IN3
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=04>, Wejście raportujące, NO.

[44][P][FW] - Programowanie funkcji dla linii wejściowej IN4 (jedynie PR411DR)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście wyłączone, NO.

[45][P][FW] - Programowanie funkcji dla linii wejściowej IN5 (jedynie PR411DR)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście wyłączone, NO.

[46][P][FW] - Programowanie funkcji dla linii wejściowej IN6 (jedynie PR411DR)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście wyłączone, NO.

[47][P][FW] - Programowanie funkcji dla linii wejściowej IN7 (jedynie PR411DR)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście wyłączone, NO.

[48][P][FW] - Programowanie funkcji dla linii wejściowej IN8 (jedynie PR411DR)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście wyłączone, NO.

[49][P][FW] - Programowanie funkcji dla linii wejściowej IN1 na module XM-2 (linia dodatkowa)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście Wyłączone, NO.

[50][P][FW] - Programowanie funkcji dla linii wejściowej IN2 na module XM-2 (linia dodatkowa)
Zasady programowania jak dla wejścia IN1. Wartość domyślna: <FW=00>, Wejście Wyłączone, NO.

[51][FW] - Programowanie funkcji dla wyjścia przekaźnikowego REL1
Parametr [FW] określa funkcję linii wyjściowej (patrz 3.9 Linie wyjściowe). Wartość domyślna: <FW=99>, Zamek drzwi.

[52][FW] - Programowanie funkcji dla wyjścia tranzystorowego IO1
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=07>, Sygnalizuje: PREALARM +DRZWI OTWARTE + WEJŚCIE SIŁOWE.

[53][FW] - Programowanie funkcji dla wyjścia tranzystorowego IO2
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=00>, Kontroler Rozbrojony.

[54][FW] - Programowanie funkcji dla wyjścia tranzystorowego CLK
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=100>, Zarezerwowane (do funkcji komunikacyjnych).

[55][FW] - Programowanie funkcji dla wyjścia tranzystorowego DTA
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=100>, Zarezerwowane (do funkcji komunikacyjnych).

Uwaga: Linie CLK i DTA (patrz 3.2.3 Interfejs RACS Clock & Data) są dostępne, jako linie wyjściowe wyłącznie wtedy gdy nie są one używane do komunikacji z zewnętrznym czytnikiem PRT ani modułem rozszerzeń XM- 2.

---

[56][FW] - Programowanie funkcji dla wyjścia przekaźnikowego REL2 (jedynie PR411DR)
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=07>, Sygnalizuje: PREALARM +DRZWI OTWARTE + WEJŚCIE SIŁOWE.

[59][FW] - Programowanie funkcji dla linii wyjściowej REL1 na module XM-2 (linia dodatkowa)
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=99>, Zamek drzwi.

[60][FW] - Programowanie funkcji dla linii wyjściowej REL2 na module XM-2 (linia dodatkowa)
Zasady programowania jak dla wyjścia REL1. Wartość domyślna: <FW=07>, Sygnalizuje: PREALARM +DRZWI OTWARTE + WEJŚCIE SIŁOWE.

[61][PP][QQ] – Ustawienie czytników RACS podłączonych do kontrolera
[PP]=[00] – Terminal ID0 z interfejsem RACS jest wyłączony
[PP]=[01] – Terminal ID0 z interfejsem RACS jest włączony
[QQ]=[00] – Terminal ID1 z interfejsem RACS jest wyłączony
[QQ]=[01] – Terminal ID1 z interfejsem RACS jest włączony
Patrz również 3.2.3 Interfejs RACS Clock & Data

[61][RR][SS] – Ustawienie formatu transmisji czytników Wiegand podłączonych do kontrolera PR411DR
[RR] – Terminal ID0 z interfejsem Wiegand
[SS] – Terminal ID1 z interfejsem Wiegand

Tabela 12. Format transmisji czytników Wiegand	
Kod =[RR] i [SS]	Nazwa trybu
[00]	Czytnik wyłączony
[03]	Wiegand 26-66 bit, podaje kod PIN (HEX)
[24]	Wiegand 26-66 bit, podaje kod PIN (BIN)
[04]	Wiegand 26-66 bit, podaje kod karty
[05]	Wiegand 26-66 bit, podaje ID użytkownika (HEX)
[17]	Wiegand 26-66 bit, podaje ID użytkownika (BIN)
[15]	Wiegand 26-66 bit, podaje kod karty lub PIN (HEX)
[16]	Wiegand 26-66 bit, podaje kod karty lub PIN (BIN)
[20]	Wiegand 26-66 bit, podaje kod PIN (HEX), bez parzystości
[25]	Wiegand 26-66 bit, podaje kod PIN (BIN), bez parzystości
[21]	Wiegand 26-66 bit, podaje kod karty, bez parzystości
[22]	Wiegand 26-66 bit, podaje ID użytkownika (HEX), bez parzystości
[23]	Wiegand 26-66 bit, podaje ID użytkownika (BIN), bez parzystości
[18]	Wiegand 26-66 bit, podaje kod karty lub PIN (HEX), bez parzystości

Uwaga: Załączenie RACS ID0 lub ID1 powoduje automatyczne wyłączenie linii CLK i DTA jako wyjść ogólnego przeznaczenia. Ponadto załączenie terminala Wiegand ID0 powoduje wyłączenie funkcji wejść IN1 oraz IN2 w PR411DR, natomiast załączenie terminala Wiegand ID1 skutkuje wyłączeniem funkcji wejść IN3 oraz IN4 w PR411DR.

[62][X] – Obsługa modułu XM-2
Programuj [X]=0 aby wyłączyć obsługę modułu
Programuj [X]=1 aby załączyć obsługę modułu
Wartość domyślna: <X=0>, obsługa wyłączona

[63][OT] - Programowanie Czasu na Otwarcie
Parametr [OT] określa w sekundach, na jaki czas kontroler będzie aktywował zamek elektryczny po tym jak zostanie przyznany dostęp. Wartość [OT] musi zawierać się w zakresie od 0 do 99 sekund. Zaprogramowanie wartości 0 powoduje, że wyjście będzie pracowało w trybie bistabilnym tzn. każdorazowo, gdy zostanie przyznany dostęp linia wyjściowa zmieni swój stan na czas nieograniczony, aż do momentu, kiedy jakieś inne zdarzenie przywróci jej stan poprzedni (patrz 3.7.2 Sterowanie elementem wykonawczym oraz 3.7.4 Opcja: Praca bistabilna (typu zatrzask)).
Wartość domyślna: <OT=04>.

[64][CT] - Programowanie Czasu na Zamknięcie
Parametr [CT] określa w sekundach w ciągu jakiego czasu drzwi powinny zostać zamknięte aby nie nastąpił alarm Drzwi Otwarte (patrz 3.7.10 Alarm Drzwi). Wartość [CT] musi zawierać się w zakresie od 1 do 99 sekund . Funkcja Czas na Zamkniecie działa tylko wtedy, gdy kontroler współpracuje z czujnikiem otwarcia drzwi. Wartość domyślna: <CT=09>.

[65][A] - Sterowanie Trybem Identyfikacji
W zależności od wartości parametru [A] Tryb Identyfikacji może przybierać formy: Tylko Karta, Tylko PIN, Karta lub PIN, Karta i PIN (patrz również 3.4 Tryby Identyfikacji).
Programuj: [A] = [0] aby ustawić tryb Karta lub PIN
Programuj: [A] = [1] aby ustawić tryb Tylko Karta
Programuj: [A] = [2] aby ustawić tryb Tylko PIN
Programuj: [A] = [3] aby ustawić tryb Karta i PIN

[66][F] – Programowanie opcji: Czasowa blokada kontrolera po 5 błędnych próbach identyfikacji
Programuj [F]=0 by wyłączyć funkcję, [F]=1 by ją załączyć. Wartość domyślna: <F=0>. Patrz również 3.7.12 Opcja: Czasowa blokada kontrolera po 5 próbach identyfikacji.

[67][F] – Programowanie opcji: Włącz Funkcję DURESS (użycie kodu pod przymusem)
Programuj [F]=0 aby wyłączyć funkcję lub [F]=1 aby ją załączyć. Wartość domyślna: <F=1>. Patrz również 3.7.7 Opcja: Nie sygnalizuj użycia kodu PIN pod przymusem.

[68][F] – Programowanie opcji: Samoczynne blokowanie drzwi (Auto-relock)
Programuj [F]=0 aby wyłączyć funkcję lub [F]=1 aby załączyć blokowanie zamka niezwłocznie po otwarciu drzwi lub [F]=2 aby załączyć blokowania zamka niezwłocznie po zamknięciu drzwi. Wartość domyślna: <F=0>, opcja wyłączona. Patrz również 3.7.5 Opcja: Skracanie czasu otwarcia (ang. auto-relock).

[69][NF][F] – Programowanie autoryzacji dla Funkcji Użytkownika
Parametr [NF] wskazuje funkcję użytkownika z zakresu 10-39. Programuj [F]=0 aby wyłączyć konieczność autoryzacji dla danej funkcji lub [F]=1 jeśli chcesz załączyć konieczność autoryzacji. Wartość domyślna:<F=1>, opcja załączona. Patrz 4.2 Funkcje Użytkownika.

[69][*][0] - Wyłączenie konieczności autoryzacji dla Funkcji Użytkownika
Wyłącza konieczność posiadania identyfikatora AUTH dla wszystkich Funkcji Użytkownika.

[69][*][1] - Załączenie konieczności autoryzacji dla wszystkich Funkcji Użytkownika
Załącza konieczność posiadania identyfikatora AUTH dla wszystkich Funkcji Użytkownika.

Uwaga: Domyślnie wszystkie Funkcje Użytkownika (patrz 4.2 Funkcje Użytkownika) wymagają autoryzacji (posiadania identyfikatora MASTER lub uprawnionego użytkownika)

---

[70][X] – Programowanie opcji: Sygnalizuj Alarm drzwi na wewnętrznym głośniku
Programuj [X]=0 aby wyłączyć funkcję lub [X]=1 aby ją załączyć. Wartość domyślna: <X=0>, opcja wyłączona. Patrz również 3.7.11 Opcja: Sygnalizuj Alarm Drzwi na wewnętrznym głośniku.

[71][FF][A] – Programowanie funkcji klawisza F1 na terminalu ID0
Parametr [FF] wskazuje funkcję klawisza z zakresu 66-72 (patrz 3.10 Klawisze funkcyjne). Programuj [A]=0 aby wyłączyć konieczność autoryzacji dla danego klawisza lub [F]=1 jeśli chcesz załączyć konieczność autoryzacji. Wartość domyślna:<F=1>, opcja załączona.

[72][FF][A] – Programowanie funkcji klawisza F2 na terminalu ID0
Zasady programowania klawisza j.w.

[73][FF][A] – Programowanie funkcji klawisza F1 na terminalu ID1
Zasady programowania klawisza j.w.

[74][FF][A] – Programowanie funkcji klawisza F2 na terminalu ID1
Zasady programowania klawisza j.w.

[75][Nowa karta MASTER] – Programowanie nowej karty MASTER
Stara karta MASTER zostaje usunięta a na jej miejsce zostaje zaprogramowana nowa karta MASTER.

[76][Nowy kod PIN MASTER] – Programowanie nowego kodu PIN MASTER
Stary PIN kod MASTER zostaje usunięty a na jego miejsce zostaje zaprogramowany nowy kod PIN MASTER.

[77][Nowa karta INSTALLER] – Programowanie nowej karty INSTALLER
Stara karta INSTALLER zostaje usunięta a na jej miejsce zostaje zaprogramowana nowa karta INSTALLER. Domyślnie karta INSTALLER nie jest definiowana w systemie i wtedy jej rolę pełni karta MASTER.

[78][Nowy kod PIN INSTALLER] – Programowanie nowego kodu PIN INSTALLER
Stary PIN kod INSTALLER zostaje usunięty a na jego miejsce zostaje zaprogramowany nowy kod PIN INSTALLER.

[79][APB] - Programowanie trybu Anti-passback
Wartość domyślna: <APB=0>
Programuj: [APB] = [0] aby wyłączyć APB
Programuj: [APB] = [1] aby ustawić APB Miękki
Programuj: [APB] = [2] aby ustawić APB Twardy
Patrz również 3.7.14 Anti-passback (APB).

[80][TA] - Programowanie trybu Anti-passback z obsługą czujnika otwarcia (True APB)
Programuj [TA]=0 aby wyłączyć tryb lub [TA]=1 aby go załączyć. Patrz również 3.7.14 Anti-passback (APB).

[81][SS] – Programowanie licznika flagi AUX1 w sekundach (SS = 00-99)
Programowanie licznika flagi AUX1 w sekundach. Zaprogramowanie [SS]=00 wyłącza działanie licznika, natomiast gdy licznik jest wyłączony to sterowanie flagą odbywa się w trybie bistabilnym (praca typu zatrzask – ang. LATCH). Patrz również 3.7.9 Flagi Systemowe oraz 3.7.4 Opcja: Praca bistabilna (typu zatrzask).

[81][*][MM] – Programowanie licznika flagi AUX1 w minutach (MM=01-99)
Programowanie [MM]=00 jest zabronione. Wartość domyślna: <SS=00>

[82][SS] – Programowanie licznika flagi AUX2 w sekundach (SS = 00-99)
Zaprogramowanie [SS]=00 wyłącza działanie licznika, natomiast gdy licznik jest wyłączony to sterowanie flaga odbywa się w trybie bistabilnym (praca typu zatrzask – ang. LATCH). Wartość domyślna: <SS=00>. Patrz również 3.7.9 Flagi Systemowe oraz 3.7.4 Opcja: Praca bistabilna (typu zatrzask).

[82][*][MM] – Programowanie licznika flagi AUX2 w minutach (MM=01-99).
Programowanie [MM]=00 jest zabronione. Wartość domyślna: <SS=00>.

[83][SS] – Programowanie licznika flagi ŚWIATŁO w sekundach (SS = 00-99)
Zaprogramowanie [SS]=00 wyłącza działanie licznika, natomiast gdy licznik jest wyłączony to sterowanie flaga odbywa się w trybie bistabilnym (praca typu zatrzask – ang. LATCH). Patrz również 3.7.9 Flagi Systemowe oraz 3.7.4 Opcja: Praca bistabilna (typu zatrzask).

[83][*][MM] – Programowanie licznika flagi ŚWIATŁO w minutach (MM=01-99).
Programowanie [MM]=00 jest zabronione. Wartość domyślna: <SS=00>.

[84][SS] – Programowanie licznika flagi TAMPER w sekundach (SS = 01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <MM=03>. Patrz również 3.7.9 Flagi Systemowe

[84][*][MM] – Programowanie licznika flagi TAMPER w minutach (MM=01-99).
Zaprogramowanie [MM] =0 jest zabronione. Wartość domyślna: <MM=03>

[85][SS] – Programowanie licznika flagi WŁAMANIE w sekundach (SS = 01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <MM=03>. Patrz również 3.7.9 Flagi Systemowe

[85][*][MM] – Programowanie licznika flagi WŁAMANIE w minutach (MM=01-99).
Zaprogramowanie [MM] =0 jest zabronione. Wartość domyślna: <MM=03>.

[86][SS] – Programowanie licznika flagi WYMUSZENIE w sekundach (SS = 01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <MM=03>. Patrz również 3.7.9 Flagi Systemowe

[86][*][MM] – Programowanie licznika flagi WYMUSZENIE w minutach (MM=01-99).
Zaprogramowanie [MM] =0 jest zabronione. Wartość domyślna: <MM=03>

[87][SS] – Programowanie licznika flagi PROBLEM w sekundach (SS = 01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <MM=03>. Patrz również 3.7.9 Flagi Systemowe

[87][*][MM] – Programowanie licznika flagi PROBLEM w minutach (MM=01-99).
Zaprogramowanie [MM] =0 jest zabronione. Wartość domyślna: <MM=03>.

[88][SS] – Programowanie licznika ZWŁOKA NA WEJŚCIE w sekundach (SS=01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <SS=60>. Patrz również 3.7.9 Flagi Systemowe.

[88][*][MM] – Programowanie licznika ZWŁOKA NA WEJŚCIE w minutach (MM=01-99)
Zaprogramowanie [MM] = 0 jest zabronione. Wartość domyślna: <SS>=60>

[89][SS] – Programowanie licznika ZWŁOKA NA WYJŚCIE w sekundach (SS=01-99)
Zaprogramowanie [SS]=00 jest zabronione. Wartość domyślna: <SS=60>. Patrz również 3.7.9 Flagi Systemowe.

[89][*][MM] – Programowanie licznika ZWŁOKA NA WYJŚCIE w minutach (MM=01-99)
Zaprogramowanie [MM] =0 jest zabronione. Wartość domyślna: <SS=60>

[89][*][*] – Wyłącza działanie licznika ZWŁOKA NA WEJŚCIE (wyłączenie opóźnienia)
Komenda umożliwia wyłączenie licznika ZWŁOKA NA WEJŚCIE

[90][*] - Wyłączenie działania funkcji Kod Obiektu (Facility Code).
Polecenie umożliwia wyłączenie funkcji Kodu Obiektu (patrz 3.7.6 Kod Obiektu (ang. Facility Code)).

[90][WCN][ABCDEFGH] - Programowanie Kodu Obiektu (Facility Code).
Parametr [WCD] określa postać Kodu Obiektu, liczba ta jest z zakresu od 000 do 255 (zawsze trzy cyfry). Parametr [ABCDEFGH] określa uprawnienia użytkowników posługujących się kartami z Kodem Obiektu i może przyjmować wartość 0 lub 1 (patrz również 3.7.6 Kod Obiektu (ang. Facility Code) i 3.3.2 Opcje (uprawnienia) użytkowników:

A=1 Całkowicie blokuje dostęp
B=1 Autoryzacja użycia klawisza F1 na terminalu ID0
C=1 Autoryzacja użycia klawisza F2 na terminalu ID0
D=1 Autoryzacja użycia klawisza F1 na terminalu ID1
E=1 Autoryzacja użycia klawisza F2 na terminalu ID1
F=1 Autoryzacja użycia Funkcji Użytkownika
G=1 Uprawnienie do przezbrajania kontrolera
H=1 Uprawnienie do autoryzacji Kart Funkcyjnych

[91][C] - Programowanie opcji: Blokuj dostęp gdy kontroler jest w stanie Uzbrojenia.
Programuj [C]=0 aby wyłączyć funkcję lub [C]=1 aby ją załączyć. Wartość domyślna: <F=0>, opcja wyłączona. Patrz również 3.7.3 Opcja: Blokuj dostęp, gdy kontroler jest w stanie uzbrojenia.

[92][NK][FN][A]<Karta> - Programowanie Karty Funkcyjnej.
Parametr [NK] określa numer Karty Funkcyjnej i może przybierać wartość od 00-31. Parametr [FN] określa funkcję danej Karty Funkcyjnej (patrz 3.11 Karty Funkcyjne). Programuj [A]=0 aby wyłączyć konieczność autoryzacji dla danej Karty lub [A]=1 jeśli chcesz załączyć konieczność autoryzacji

[93]<Karta> - Kasowanie wskazanej Karty Funkcyjnej
Polecenie umożliwia skasowanie danej Karty Funkcyjnej w kontrolerze. Patrz 3.11 Karty Funkcyjne.

[93][NK] - Kasowanie Karty Funkcyjnej o numerze NK (NK=00-31)
Polecenie umożliwia skasowanie Karty Funkcyjnej o danym numerze NK w kontrolerze. Patrz 3.11 Karty Funkcyjne.

[93][*] - Kasowanie wszystkich Kart Funkcyjnych
Polecenie umożliwia skasowanie wszystkich Kart Funkcyjnych w danym kontrolerze. Patrz 3.11 Karty Funkcyjne.

[94][BK] - Ustawienie intensywności podświetlenia klawiatury (wyłącznie dla PR311SE)
[BK] = 0 0%
[BK] = 1 20%
[BK] = 2 40%
[BK] = 3 60%
[BK] = 4 80%
[BK] = 5 100%

[95][BK] - Ustawienie poziomu głośnika (nie dotyczy PR411DR)
[BK] = 0 0%
[BK] = 1 20%
[BK] = 2 40%
[BK] = 3 60%
[BK] = 4 80%
[BK] = 5 100%

[96][F] - Opcja: Podtrzymanie Wyjścia 1 (REL1) przez kartę przy czytniku
Programuj [F]=0 aby wyłączyć opcję lub [F]=1 aby ją załączyć. Wartość domyślna: <F=0>. Patrz również 3.7.13 Opcja: Podtrzymanie Wyjścia 1 (REL1) przez kartę przy czytniku.

4.4 Sygnały Optyczne i Akustyczne

4.4.1 Sygnały optyczne

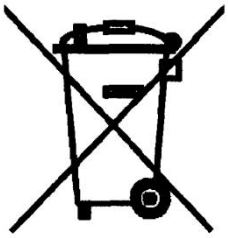
W kontrolerach PRxx1 sygnalizacja optyczna jest realizowana na wskaźnikach LED dostępnych na terminalach ID1/ID0. W kontrolerze PR411DR sygnalizacja optyczna jest realizowana równolegle na wskaźnikach LED dostępnych na płycie kontrolera.

Tabela 13. 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 (patrz 3.6 Tryby Uzbrojenia)
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.

4.4.2 Sygnały akustyczne

W kontrolerach PR311SE, PR611 i PR621 sygnały akustyczne są generowane przez wewnętrzny głośnik kontrolera oraz na zewnętrznych czytnikach serii PRT. W kontrolerze PR411DR sygnalizacja akustyczna jest realizowana jedynie na zewnętrznych czytnikach serii PRT.

Tabela 14. 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	Błąd, 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 (patrz 4.1 Reset Ustawień – Programowanie Identyfikatora MASTER oraz Adresu ID)

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

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