

PR302LCD v2.0

Firmware 106.5

KONTROLER DOSTĘPU JEDNEGO PRZEJŚCIA Z ZINTEGROWANYM CZYTNIKIEM RFID/PIN ORAZ WYŚWIETLACZEM LCD

Budowa i przeznaczenie.

Kontroler typu PR302LCD przewidziany jest do zastosowania w układach kontroli dostępu opartych na elektrycznym sterowaniu otwarciem drzwi oraz w systemach *Rejestracji Czasu Pracy (RCP)*. Funkcję rejestracji czasu pracy kontroler może pełnić równolegle z funkcją kontroli dostępu, może być również zastosowany jako autonomiczny terminal *RCP* nie będący elementem systemu kontroli dostępu (w skr. KD). Kontroler oferuje kilka mechanizmów programowych specjalnie dedykowanych do funkcji rejestracji czasu pracy, między innymi udostępnia mechanizmy manualnego sterowania aktualnym trybem rejestracji za pośrednictwem klawiatury bądź z linii zewnętrznych a także możliwość automatycznej zmiany trybu rejestracji zgodnie z zadeklarowanym harmonogramem czasowym. PR302LCD posiada wbudowaną głowicę do odczytu kart zbliżeniowych, metalową klawiaturę numeryczną oraz wyświetlacz LCD, obudowa urządzenia wykonana jest z metalu i pokryta lakierem proszkowym. Kontroler posiada trzy wejścia i trzy wyjścia w tym jedno wyjście przekaźnikowe. Zarówno wejścia jak i wyjścia kontrolera mogą być skonfigurowane do kilku predefiniowanych funkcji w tym do obsługi przycisku wyjścia oraz kontaktu drzwiowego. Kontroler może dozorować jedno przejście, sygnalizuje stany alarmowe w tym próbę siłowego wejścia lub pozostawienie drzwi w stanie otwarcia. W kontrolerze można zarejestrować do 4000 użytkowników, użytkownicy mogą być identyfikowani za pomocą kart zbliżeniowych lub kodów PIN, możliwe jest również założenie podwójnego trybu identyfikacji (tzw. *Karta + PIN*) oraz funkcji *anti-passback* (blokowanie wielokrotnego przejścia w tym samym kierunku). Kontroler wyposażony jest w wewnętrzną pamięć zdarzeń oraz układ zegara czasu rzeczywistego, umożliwiają podział użytkowników na grupy i zdefiniowanie czasowych stref dostępu. Do kontrolera można dołączyć dodatkowy zewnętrzny terminal identyfikacji (czytnik serii PRT), który wraz z kontrolerem umożliwi obustronną kontrolę przejścia, dodatkowy terminal identyfikacji stosuje się również wtedy, gdy istnieje konieczność umieszczenia członu decyzyjnego (kontroler) w miejscu chronionym albo oddalonym od punktu identyfikacji. Terminale serii PRT są wyposażone w klawiaturę i/lub głowicę zbliżeniową, dostępne są zarówno wykonania przeznaczone do wewnątrz jak i na zewnątrz budynków. Oprogramowanie kontrolera może być uaktualniane (*fleszowane*) za pośrednictwem dedykowanego do tego celu programu *RogerISP*. PR302LCD może pracować w trybie autonomicznym lub być zintegrowany z sieciowym systemem kontroli dostępu typu *RACS* pracującym pod kontrolą komputera PC. Programowanie urządzenia przeprowadza się z poziomu komputera PC, przesyłanie ustawień do kontrolera odbywa się w sposób „*transakcyjny*”, oznacza to że w przypadku gdy programowanie nowych ustawień nie zakończy się sukcesem w kontrolerze będą obowiązywać ustawienia stare. Cecha ta ma szczególnie istotne znaczenie w doniesieniu do kontrolerów rozlokowanych w odległych obiektach gdzie wystąpienie awarii w trakcie konfiguracji kontrolera mogło by wywołać znaczne niedogodności w ruchu osób.

Uwaga: Przeznaczeniem niniejszego dokumentu jest przedstawienie **podstawowych** zasad funkcjonowania kontrolera oraz zasad jego instalacji. **Szczegółowe zasady funkcjonowania** kontrolera zależą od aktualnie załadowanej wersji oprogramowania firmowego oraz od cech oprogramowania sterującego zainstalowanego na PC dlatego też każdorazowo należy odwołać się do dokumentacji technicznej dostarczanej z programem zarządzającym oraz opisem oprogramowania firmowego.

RACS – to skrót od angielskojęzycznego zwrotu *Roger Access Control System* co w wolnym tłumaczeniu oznacza system kontroli dostępu skonstruowany i dostarczany przez firmę *Roger*.

Oprogramowanie Firmowe

W procesie produkcji kontroler jest programowany najbardziej aktualną w danej chwili wersją oprogramowania firmowego, niemniej już po instalacji istnieje możliwość przesłania do urządzenia nowszych, ulepszonych wersji programu sterującego. Operacja ta nazywana jest potocznie *fleszowaniem* i może być dokonywana w funkcjonującej instalacji bez konieczności demontażu urządzenia lub wymiany układów pamięciowych. Proces fleszowania nie wymaga żadnych dodatkowych kabli lub interfejsów, proces przesyłania nowego oprogramowania firmowego dokonuje się za pośrednictwem standardowego interfejsu komunikacyjnego systemu *RACS* (układ UT-2) oraz programu *RogerISP*. W większości przypadków nowsze wersje oprogramowania firmowego wymagają nowszych wersji oprogramowania zarządzającego na PC, każdorazowo przed operacją fleszowania należy upewnić się czy operacja fleszowania nie będzie wymagała aktualizacji pakietu oprogramowania *RACS*.

Uwaga: Na specjalne życzenie, producent urządzenia dopuszcza możliwość wykonania zmian w oryginalnym oprogramowaniu kontrolera celem dopasowania go do indywidualnych potrzeb klienta. Wykonanie zmienionego oprogramowania każdorazowo wymaga uzgodnień z działem technicznym producenta i może wiązać się z dodatkowymi kosztami.

Charakterystyka kontrolera

- praca autonomiczna lub sieciowa pod kontrolą komputera PC,
- transakcyjny sposób przesyłania ustawień,
- metalowa obudowa oraz klawiatura, zegar czasu rzeczywistego, nie ulotna pamięć ustawień i zdarzeń,
- identyfikacja zbliżeniowa oraz PIN,
- trzy uniwersalne wejścia NO/NC,
- możliwość definiowania własnych typów linii wejściowych,
- dwa uniwersalne wyjścia tranzystorowe o obciążalności 1A z zabezpieczeniem elektronicznym,
- wyjście przekaźnikowe z jedną parą styków przełączalnych 1.5A,
- wejścia i wyjścia pod kontrolą harmonogramów czasowych,

- obsługa do 4000 użytkowników,
- cztery typy użytkowników z podziałem uprawnień do sterowania trybami ZAŁ/WYŁ,
- możliwość deklarowania limitów krotności użycia identyfikatorów,
- możliwość definiowania okresu ważności identyfikatorów,
- 127 grup dostępu,
- 99 harmonogramów ogólnego przeznaczenia,
- harmonogramy świąteczne,
- pamięć 32 000 zdarzeń,
- obsługa czujnika otwarcia drzwi oraz przycisku wyjścia,
- funkcja *anti-passback* z możliwością jej zerowania według harmonogramu czasowego lub z linii wejściowej,
- rozszerzone tryby funkcjonowania drzwi, w tym tryb permanentnego otwarcia oraz tryb blokady,
- zwykły [Karta/PIN] lub podwójny [Karta + PIN] tryby identyfikacji,
- tryby specjalne: tryb wejścia komisyjnego [Karta + Karta] oraz tryb [Wejście warunkowe],
- tryby pracy drzwi, tryby identyfikacji oraz tryby specjalne pod kontrolą harmonogramów czasowych,
- rejestracja zdarzeń dla celów RCP,
- definicja własnych typów rejestracji RCP,
- możliwość dynamicznej zmiany trybu RCP czytnika za pomocą linii wejściowej, klawiatury lub z harmonogramu czasowego,
- możliwość integracji z systemem antywłamaniowym za pośrednictwem linii wyjściowej służącej do przezbrajania systemu lub strefy alarmowej,
- obsługa czujnika ruchu z możliwością automatycznego rozbrajania gdy kontroler jest w trybie ZAŁ,
- współpraca z zewnętrznym terminalem (czytnikiem) identyfikacji,
- fleszowanie programu sterującego kontrolerem,
- zasilanie 12VDC/120mA,
- obsługa kart standardu UNIQUE (EM4001/2),
- zasięg czytania do 7 cm (dla kart typu ISO),
- oprogramowanie Windows 95/98/2K/NT/XP, darmowe dla systemów do 8 przejść,
- kontrolka ActiveX (OCX) dla celów integracji programowej,
- zgodność z normą EN50133-1,
- znak CE

Użytkownicy

Kontroler umożliwi zarejestrowanie do 4000 użytkowników, każdy z użytkowników zarejestrowanych w kontrolerze posiada swój numer identyfikacyjny (numer ID) i może przynależeć do jednego z czterech predefiniowanych typów. Kontroler dokonuje identyfikacji użytkowników za pośrednictwem przypisanych im indywidualnych identyfikatorów. W systemie *RACS* identyfikatorem może być transponder zbliżeniowy (karta, brelok itp.) lub kod PIN, możliwe jest również założenie trybu podwójnej identyfikacji (tryb **[Karta+PIN]**) który wymusza na użytkownikach stosowanie obydwu wymienionych wcześniej form identyfikacji jednocześnie. Każdy identyfikator może być zarejestrowany w kontrolerze na czas nieokreślony lub na czas ograniczony w obrębie okresu 12 miesięcy, nie jest możliwe definiowanie okresów ważności identyfikatorów na czas powyżej 12 miesięcy. Oprócz definicji ważności identyfikatora która dotyczy wszystkich kontrolerów możliwe jest zdefiniowanie limitu krotności użycia identyfikatora. Deklarację limitów użycia identyfikatorów przeprowadza się indywidualnie dla każdego z kontrolerów w systemie. Po upływie „terminu ważności” identyfikatora lub przekroczeniu limitu krotności użycia kontroler samoczynnie usuwa go z listy ważnych identyfikatorów, nie jest możliwe dalsze jego używanie.

Typy Użytkowników - Tabela

Typ Użytkownika	Numer ID	Cechy i uprawnienia
INSTALLER	Bez numeru ID	Użytkownik tego typu posiada uprawnienie do wejścia do trybu programowania instalatorskiego urządzenia (o ile urządzenie dopuszcza manualne programowanie ustawień instalatorskich).
MASTER	0	Użytkownik tego typu posiada uprawnienie do otwierania drzwi, sterowania trybem ZAŁ/WYŁ oraz do manualnego programowania urządzenia (o ile taki sposób programowania jest osiągalny w urządzeniu).
SWITCHER Full (Pełny)	001..049	Użytkownicy tego typu posiadają uprawnienie do otwierania drzwi oraz do sterowania trybem ZAŁ-WYŁ kontrolera.
SWITCHER Limited (Ograniczony)	050..099	Użytkownicy tego typu posiadają uprawnienie jedynie do sterowania trybem ZAŁ/WYŁ kontrolera, nie posiadają uprawnienia do otwierania drzwi.
NORMAL	100..4000	Użytkownicy tego typu posiadają uprawnienie do otwierania drzwi lecz nie posiadają prawa do sterowania trybem ZAŁ-WYŁ kontrolera.

Nazwa *Swicher* pochodzi od słowa angielskiego *switch* które oznacza czynność przełączania, sterowania itp. Użytkownik typu *Switcher* to w rozumieniu twórców systemu *RACS* osoba obdarzona uprawnieniem do pewnego typu dodatkowego sterowania w tym przypadku sterowania trybem ZAŁ.-WYŁ.

Identyfikatory

PR302LCD akceptuje transpondery zbliżeniowe (karty, breloki itp.) standardu UNIQUE opartych na module V4001/2 lub kompatybilnych z tym modulem oraz kody PIN o długości od 3 do 6 cyfr dziesiętnej. Każde wprowadzenie kodu PIN w kontrolerze musi być zakończone naciśnięciem klawisza [#].

Specyfikacja identyfikatorów zbliżeniowych standardu UNIQUE:

- pamięć ROM, 64 bity.
- Modulacja amplitudowa typu Manchester,
- Częstotliwość pracy 125 kHz.
- Szybkość transmisji 2kB/sek.

Uwaga: Jak już wcześniej wspomniano pod pojęciem identyfikatora (w skr. **Ident.**) rozumie się transponder zbliżeniowy, PIN-kod lub obydwa te elementy jednocześnie.

Przykłady:

- | | | |
|----|-----------------------------|-----|
| 1. | [Ident.] = [PIN][#]+[Karta] | lub |
| 2. | [Ident.] = [Karta]+[PIN][#] | lub |
| 3. | [Ident.] = [PIN] [#] | lub |
| 4. | [Ident.] = [Karta] | |

Przykłady [1] i [2] odnoszą się do sytuacji gdy aktywny jest tryb identyfikacji [Karta+PIN].

Użycie Kodu PIN Pod Przemusem (Funkcja DURESS)

Jeżeli użytkownik wprowadził kod zwiększony lub zmniejszony o jedność na ostatniej pozycji to kontroler może interpretować to jako wprowadzenie kodu pod przemusem. Wprowadzenie kodu pod przemusem oprócz normalnej reakcji kontrolera (otwarcie drzwi, przełączenie pomiędzy stanem ZAŁ-WYŁ) powoduje dodatkowo zarejestrowanie zdarzenia [Wejście pod przemusem] oraz może wywoływać sygnalizację na wyjściu alarmowym kontrolera.

Przykład: kod użytkownika ma postać [4569], wprowadzenie kodu [4568][#] lub [4560][#] traktowane jest przez kontroler jako użycie kodu pod przemusem.

Uwaga: Aby kontroler mógł poprawnie rozpoznawać wprowadzenie kodu pod przemusem, PIN kody poszczególnych użytkowników powinny różnić się między sobą co najmniej o wartość +/- [2]. Działanie kodów DURESS może zostać zablokowane w ustawieniach programu PR Master indywidualnie dla każdego kontrolera. Program PR Master uniemożliwia zdefiniowanie nowego kodu PIN który pokrywał by się z kodem DURESS innego użytkownika. W przypadku gdy stosowanie kodów DURESS w systemie KD nie jest celowe można w programie PR Master włączyć opcję *Narzędzia/Opcje/Inne/Wyłącz funkcje DURESS* co spowoduje że program będzie dopuszczał definiowanie kodów PIN o dowolnej postaci.

Grupy Użytkowników (Grupy Dostępu)

W systemie RACS użytkownicy mogą być podzieleni na wiele grup, w przypadku ogólnym grupę dostępu może tworzyć nawet jedna osoba. Wszyscy użytkownicy należący do tej samej grupy posiadają identyczne prawa dostępu do pomieszczeń. Definiowanie praw dostępu w systemie RACS (zwanych również poziomami dostępu) polega na określeniu zasad kiedy i gdzie użytkownicy poszczególnych grup będą posiadali prawo dostępu. Domyślnie każdy nowo zarejestrowany w systemie użytkownik nie jest przypisany do żadnej z istniejących w systemie grup dostępu. **Użytkownicy nie należący do żadnej grupy (tzw. Bez grupy) posiadają prawo dostępu do wszystkich pomieszczeń bez żadnych ograniczeń czasowych.**

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

- gdy wyzwolona jest linia wejścia skonfigurowana jako [Blokuje dostęp]
- gdy na kontrolerze ustawiony jest tryb drzwiowy [Drzwi Zamknięte]
- gdy kontroler znajduje się w trybie WYŁ. oraz jednocześnie załączona jest opcja [Blokada dostępu gdy kontroler w trybie WYŁ.]

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

Strefy Dostępu (Strefy)

Strefa dostępu to zbiór wybranych punktów identyfikacji (kontrolerów z wbudowanymi czytnikami lub terminali dostępu) które są interpretowane jako pewien spójny obszar w systemie KD, przykładami stref dostępu mogą być obszary w rodzaju: Hala produkcyjna, Szatnia, Biura, Korytarze, Piętra itp. Zasadniczo pojęcie strefy dostępu ma celu uproszczenie sposobu definiowania praw dostępu, dzięki temu pojęciu definiowanie praw dostępu przeprowadza się nie dla pojedynczego punktu identyfikacji (pojedynczych drzwi) lecz dla grupy urządzeń które kontrolują dostęp do pewnego obszaru w obiekcie. W ogólnym przypadku każdy punkt identyfikacji (każde pomieszczenie) może stanowić osobną strefę dostępu, w takiej sytuacji definiowanie praw dostępu będzie w praktyce odnosiło się do indywidualnych drzwi lub przejścia.

Harmonogramy Czasowe

Przez pojęcie harmonogramu czasowego rozumie się zbiór deklaracji przedziałów czasowych typu *Od ... Do....*, przedziały czasowe definiuje się dla każdego dnia tygodnia (od poniedziałku do niedzieli) oraz dla osobno dla dni świątecznych (H1, H2, H3 i H4). W systemie RACS występują cztery typy harmonogramów:

- Harmonogramy ogólnego przeznaczenia
- Harmonogramy sterujące trybem pracy drzwi
- Harmonogramy sterujące trybem rejestracji RCP
- Harmonogramy sterujące zerowaniem funkcji APB

Harmonogram ogólnego przeznaczenia może być dedykowany do jednej lub więcej funkcji sterujących w kontrolerze, dla przykładu ten sam harmonogram może być wykorzystywany do sterowania dostępem, do sterowania linią wyjściową lub blokowania odczytu linii wejściowej. W kontrolerze PR302LCD można zdefiniować do 99 harmonogramów tego typu.

Harmonogram sterowani trybem pracy drzwi umożliwia automatyczne przełączanie kontrolera pomiędzy różnymi trybami pracy drzwi. Definiowanie tego harmonogramu polega na określeniu ram przedziałów czasowych oraz wskazaniu jaki tryb drzwi ma w danym przedziale czasowym obowiązywać. W czasie pomiędzy zdefiniowanymi przedziałami czasowymi kontroler automatycznie przywraca *Normalny* tryb sterowania drzwiami.

Harmonogram sterowania trybem rejestracji umożliwia automatyczne przełączanie kontrolera pomiędzy różnymi trybami rejestracji RCP. Definiowanie tego harmonogramu polega na określeniu przedziałów czasowych oraz wskazaniu jaki tryb drzwi ma w każdym z przedziałów obowiązywać. W czasie pomiędzy zdefiniowanymi przedziałami czasowymi kontroler automatycznie przywraca *Domyślny* tryb rejestracji RCP.

Harmonogram sterujący zerowaniem funkcji APB umożliwia automatyczne zerowanie rejestru funkcji APB o określonych porach czasu. Każdorazowo po wyzerowaniu rejestru funkcji APB kontroler akceptuje użycie identyfikatorów zarówno po stronie wejściowej jak i wyjściowej kontrolowanego przejścia lecz z chwilą pierwszego użycia identyfikatora zaczyna egzekwować zasady APB czyli oczekuje na to aby użytkownik używał swojego identyfikatora naprzemiennie raz na wejściu raz na wyjściu z pomieszczenia.

Ustawienia Świąteczne

Zasadniczo, definiowanie harmonogramów czasowych (a w tym praw dostępu) przeprowadza się w obrębie jednego tygodnia (od poniedziałku do niedzieli), niemniej poza tymi regulami możliwe jest zdefiniowanie ustawień zastępczych (świątecznych) które będą obowiązywały w określonych dniach w obrębie jednego roku. Kontroler umożliwia zdefiniowanie czterech rodzajów dni świątecznych (*H1, H2, H3 i H4*), definicja dnia świątecznego składa się wskazania jaki typ ustawień (od *H1 do H4*) będzie obowiązywał w wskazanym dniu świątecznym.

Prawa Dostępu

Definiowanie praw dostępu polega na określeniu według jakiego harmonogramu czasowego poszczególne grupy użytkowników będą posiadały prawo dostępu do każdej z zdefiniowanych w systemie stref dostępu.

Przykład:

Grupa	Strefa	Harmonogram	Uwagi
Prac. biurowi	Biuro	Harmonogram typu A	Pracownicy należący do grupy <i>Prac. biurowi</i> będą posiadali prawo dostępu do strefy <i>Biuro</i> według harmonogramu typu A
Prac. biurowi	Kantyna	Harmonogram typu B	Pracownicy należący do grupy <i>Prac. biurowi</i> będą posiadali prawo dostępu do strefy <i>Kantyna</i> według harmonogramu typu B
Prac. biurowi	Hala produkcyjna	Harmonogram typu C	Pracownicy należący do grupy <i>Prac. biurowi</i> będą posiadali prawo dostępu do strefy <i>Hala produkcyjna</i> według harmonogramu typu C

Uwaga: Definiowanie praw dostępu polega na określeniu warunków kiedy dostęp będzie przydzielany z czego wynika że poza zdefiniowanymi przedziałami czasowymi zdefiniowanymi w harmonogramie czasowym dostęp nie będzie przydzielany.

W przypadku gdy dostęp ma być całodobowy należy wybrać predefiniowany harmonogram czasowy typu *Zawsze*, gdy dostęp ma być kompletnie zablokowany należy wybrać harmonogram *Nigdy*, w pozostałych przypadkach należy zdefiniować własny harmonogram czasowy. Zasadniczo ten sam harmonogram czasowy może być stosowany do sterowania czasowego w wielu funkcjach (np. może służyć do sterowania dostępem oraz do sterowania wyjściem programowalnym) niemniej zaleca się aby jeden harmonogram był wykorzystywany do sterowania jedną funkcją.

Alarmy Kontrolera

Wystąpienie pewnych sytuacji na kontrolerze jest uznawane jako stan alarmowy. Stan alarmowy wywołuje zarejestrowanie w pamięci kontrolera pewnego typu zdarzenia oraz wywołać pewien określony typ sygnalizacji na linii wyjściowej której nadano funkcje [Wyjście alarmowe]. Linia wyjściowa może służyć do sygnalizacji jednego lub więcej alarmu. W procesie konfiguracji deklaruje się które z sytuacji alarmowych mają być sygnalizowane na linii wyjściowej. Kontroler umożliwia sygnalizację następujących alarmów:

Nazwa Alarmu	Powstawanie	Priorytet	Sposób sygnalizacji
PREALARM	Alarm powstaje w następstwie wystąpienia trzech nieudanych prób identyfikacji w okresach nie większych niż co jedna minuta.	Niski	Pojedynczy impuls 0.5 sek. powtarzany co dwie sekundy.
DRZWI OTWARTE	Alarm powstaje w wyniku przekroczenia dopuszczalnego czasu na domknięcie drzwi.	Średni	Dwa impulsy po 0.5 sek. powtarzane co dwie sekundy.
WEJŚCIE SIŁOWE	Alarm powstaje w momencie otwarcia drzwi które nastąpiło bez udziału kontrolera.	Wysoki	Sekwencja impuls 0.5 sek. - pauza 0.5 sek. powtarzana przez czas trwania alarmu.

Sygnalizacja każdego alarmu trwa trzy minuty poczym samoczynnie zanika. Alarm można skasować szybciej (przed upływem trzech minut) poprzez użycie dowolnego zarejestrowanego w kontrolerze identyfikatorów lub za pomocą zdalnej komendy z poziomu programu zarządzającego systemem KD. W przypadku jednoczesnego wystąpienia dwóch lub więcej alarmów sygnalizowany jest tylko alarm o najwyższym priorytecie, niemniej każdy z alarmów jest odnotowywany w historii zdarzeń przez zarejestrowanie odpowiadającego mu zdarzenia.

Tryb ZAŁ.-WYŁ.

Kontroler posiada dwa robocze tryby pracy: tryb **ZALAŻONE** oraz tryb **WYŁĄCZONE**, tryby te sygnalizowane są na dwukolorowym wskaźniku LED oznaczonym ZAŁ/WYŁ, gdy kontroler jest w trybie ZALAŻONE wskaźnik ZAŁ/WYŁ świeci kolorem zielonym, gdy znajduje się w trybie WYŁĄCZONE wskaźnik ten świeci na czerwono. Sterowanie trybem ZAŁ/WYŁ może być realizowane na kilka wymienionych poniżej sposobów:

- lokalnie za pomocą identyfikatorów typu MASTER lub SWITCHER,
- lokalnie za pomocą linii wejściowej skonfigurowanej do funkcji [Steruje trybem ZAŁ/WYŁ – klucz trwały],
- lokalnie za pomocą linii wejściowej skonfigurowanej do funkcji [Steruje trybem ZAŁ/WYŁ – klucz chwilowy],
- zdalnie z poziomu operatora systemu w następstwie interaktywnej komendy z PC,
- automatycznie wg zdefiniowanego harmonogramu czasowego (Harmonogram trybu ZAŁ/WYŁ).

Zasadniczo tryby ZAŁ/WYŁ służą do powiązania funkcji kontroli dostępu z funkcją automatycznego uzbrajania/rozbrajania systemu alarmowego w pomieszczeniu do którego dostęp przynajmniej kontroler, niemniej w ogólnym przypadku istnienie trybów ZAŁ/WYŁ można wykorzystać do kontrolowanego sterowania dowolnym zewnętrznym urządzeniem lub systemem (np. oświetleniem, ogrzewaniem lub klimatyzacją). Dzięki opcji [Dostęp tylko w trybie ZALAŻONE] istnieje możliwość powiązania prawa do otwarcia drzwi z trybem ZAŁ/WYŁ kontrolera. Jeśli opcja ta jest wyłączona dostęp do kontrolowanego pomieszczenia **nie zależy** od tego czy kontroler jest aktualnie w stanie ZALAŻONE czy WYŁĄCZONE, gdy jednak opcja ta jest załączona kontroler przyznaje prawo dostępu osobom uprawnionym tylko wtedy gdy znajduje się aktualnie w trybie ZALAŻONE. Dzięki temu mechanizmowi istnieje możliwość interaktywnego (czasowego) blokowania dostępu do pomieszczenia poprzez przełączenie kontrolera pomiędzy trybem ZALAŻONE-WYŁĄCZONE. Tryb ZALAŻONE może być sygnalizowany na liniach wyjściowych kontrolera, linię wyjściową tak skonfigurowaną można użyć np. do uzbrajania/rozbrajania strefy alarmowej, blokowania czujki ruchu lub sterowania innym urządzeniami.

Sterowanie Otwarcie Drzwi

Zasadniczo kontroler zezwala na otwarcie drzwi (aktywuje wyjście przekaźnikowe DOOR) w następstwie zidentyfikowania użytkownika który aktualnie posiada prawo dostępu do pomieszczenia. Aktywacja zamka następuje na czas określony przez parametr [Czas aktywacji zamka] i może zawierać się w przedziale od 1 sekundy do 255 minut. Istnieje również możliwość załączenia trybu „Bi-stabilnego” sterowania zamkiem, w tym przypadku każde wyzolenie zamka powoduje przejście wyjścia przekaźnikowego do stanu przeciwnego aż do momentu wystąpienia kolejnego przyznania dostępu. W przypadku załączenia opcji [Automatyczna dezaktywacja zamka po otwarciu] po zwolnieniu zamka kontroler obserwuje stan czujnika otwarcia i z chwilą rozpoznania otwarcia drzwi wyłącza wyjście przekaźnikowe nie czekając aż uplynie cały dopuszczalny czas zdefiniowany przez parametr [Czas aktywacji zamka]. Zwolnienie drzwi może również nastąpić w wyniku wydania interaktywnej komendy z poziomu programu zarządzającego systemem KD lub w wyniku funkcjonowania harmonogramu czasowego który może o pewnych zdefiniowanych porach ustawiać drzwi w stanie permanentnego otwarcia.

Obustronna Kontrola Przejścia

Obustronna kontrola przejścia wymaga obecności urządzeń identyfikujących (terminali dostępu) po obydwu stronach drzwi. Domyślnie w systemie RACS przyjęto że terminal o adresie zerowym (ID0) znajduje się na wejściu do pomieszczenia (*terminal wejściowy*) natomiast terminal o adresie pierwszym (ID1) znajduje się po stronie wyjścia (*terminal wyjściowy*). Kontroler PR302LCD posiada wbudowany czujnik RFID/PIN który logicznie traktowany jest jak terminal o adresie jeden czyli ID1. Terminal zewnętrzny dołączony do kontrolera za pośrednictwem interfejsu Clock&Data posiada adres pierwszy czyli ID0. Ten sposób przyporządkowania jest korzystny z względów bezpieczeństwa gdyż powoduje że kontroler dostępu znajduje się wewnątrz pomieszczenia i jest przez to sterowany przed dostępem osób postronnych, które mogłyby podjąć próbę otwarcia jego obudowy i zwarcia styków przekaźnika sterującego zamkiem elektrycznym. Domyślny sposób przyporządkowania terminali (ID0 na wejściu i ID1 na wyjściu) może ulec zmianie poprzez załączenie opcji *Terminal ID=1 umieszczony na "wejściu"*.

Uwaga: Pojęcia *terminal wejściowy* i *terminal wyjściowy* w odniesieniu do obustronnej kontroli przejścia odnoszą się do funkcji jakie terminale pełnią w kontroli ruchu osób w obrębie jednego przejścia i nie mają związku z trybami rejestracji *wejść/wyjść* dla celów RCP.

Funkcja Anti-passback (w skr. APB)

W przypadku ogólnym, funkcja *anti-passback* może mieć wpływ na ruch osób w obrębie jednego przejścia (*anti-passback lokalny*) lub w obrębie jednej strefy dostępu (*anti-passback globalny*). W kontrolerze PR302LCD funkcja *anti-passback* ma charakter lokalny tzn. że oddziałuje na ruch osób w obrębie **jednego** przejścia. Działanie funkcji *anti-passback* ma na celu zablokowanie możliwości wielokrotnego używania identyfikatora na tym samym terminalu wejściowym lub wyjściowym i zobligowaniu użytkowników do odczytu identyfikatorów naprzemiennie raz na wejściu raz na wyjściu z pomieszczenia. W przypadku załączenia funkcji APB próba użycia identyfikatora na tym samym punkcie identyfikacji może wywołać odmowę dostępu (*anti-passback twardy*) lub spowodować jedynie sygnalizację naruszenia zasad *anti-passback* (*anti-passback miękki*). Kontroler rejestruje w pamięci dane które wskazują na którym z terminali (wejściowym lub wyjściowym) każdy z użytkowników zarejestrowanych w kontrolerze ostatnio użył swojego identyfikatora, tablica ta jest zwana *rejestrem funkcji anti-passback* (w skr. *Rejestr APB*). Użytkownik który użył ostatnio swojego identyfikatora na terminalu wejściowym posiada status „Zalogowany na wejściu”. Użytkownik który użył ostatnio swojego identyfikatora na terminalu wyjściowym posiada status „Zalogowany na wyjściu”. W przypadku gdy nieznane jest miejsce ostatniego użycia identyfikatora przez użytkownika posiada on status „Niezalogowany”. Gdy użytkownik posiada status *Niezalogowany* kontroler dopuszcza aby pierwsze użycie identyfikatora odbyło się na czytniku wejściowym lub na czytniku wyjściowym, niemniej z chwilą pierwszego użycia identyfikatora użytkownik traci status *Niezalogowany* i od tej pory jest już zobligowany do stosowania się do zasad *anti-passback* czyli odczytu identyfikatorów naprzemiennie na terminalu wejściowym i wyjściowym. Kontroler umożliwia okresowe zerowanie rejestru APB, zerowanie tego rejestru może się odbywać według zadeklarowanego harmonogramu czasowego (*Harmonogram zerowania rejestru APB*) lub interaktywnie w wyniku wyzolenia linii wejściowej zdefiniowanej jako [Zeruje rejestr APB]. Po wyzerowaniu rejestru APB wszyscy użytkownicy posiadają status *Niezalogowany*, mogą zatem pierwszy raz użyć swojego identyfikatora zarówno na czytniku wejściowym jak i na czytniku wyjściowym.

Tryb Wejścia Warunkowego

Załączenie trybu *wejścia warunkowego* umożliwia wejście do pomieszczenia osobom normalnie nie posiadającym prawa dostępu do danego pomieszczenia pod warunkiem że ktoś inny jest już wewnątrz pomieszczenia czyli innymi słowy mówiąc przynajmniej jeden użytkownik posiada na danym kontrolerze status „zalogowany na wejściu”. Nie jest istotne czy osoba będąca wewnątrz pomieszczenia jest osobą uprawnioną czy też skorzystała wcześniej z trybu wejścia warunkowego jej obecność uprawnia do wejścia innych użytkowników systemu.

Tryby Identyfikacji

Kontroler dopuszcza stosowanie dwóch trybów identyfikacji: [Karta lub PIN] oraz [Karta + PIN]. W przypadku gdy załączony jest tryb [Karta lub PIN] użytkownik może dokonywać identyfikacji zarówno przy użyciu karty zbliżeniowej lub kodu PIN, gdy załączony jest tryb [Karta + PIN] użytkownik zobowiązany jest w celu poprawnej identyfikacji odczytać identyfikator zbliżeniowy oraz wprowadzić swój PIN kod (kolejność wymienionych czynności nie gra roli). Kontroler umożliwia zdefiniowanie *domyślnego trybu identyfikacji* indywidualnie dla każdego z typów użytkowników, możliwe jest zatem że użytkownicy pewnych typów będą mieli na stałe załączony tryb [Karta + PIN] inni natomiast będą mogli posługiwać się kartą lub kodem PIN alternatywnie. Kontroler umożliwia zdefiniowanie harmonogramu czasowego który będzie sterował trybem identyfikacji (*Harmonogram trybu [Karta + PIN]*). W przedziałach czasowych wskazywanych przez ten harmonogram kontroler będzie automatycznie przechodził do trybu [Karta + PIN], tryb ten będzie obowiązywał wtedy wszystkich użytkowników systemu. W okresach poza przedziałami czasowymi zdefiniowanymi przez ww. harmonogram kontroler będzie powracał do domyślnego trybu identyfikacji.

Tryb Wejścia Komisijnego (Karta + Karta)

W trybie *wejścia komisijnego* kontroler przyznaje prawo dostępu dopiero wtedy gdy procesu próbnej identyfikacji dokona dwóch uprawnionych do wejścia użytkowników (jeden bezpośrednio po drugim). Sterowanie trybem wejścia komisijnego jest realizowane przez odpowiedni harmonogram czasowy (*Harmonogram trybu wejścia komisijnego*). Gdy na kontrolerze obowiązuje tryb [Karta + PIN] każdy z użytkowników dokonujących identyfikacji jest zobowiązany do dokonania odczytu identyfikatora oraz do wprowadzenia kodu PIN. Zasadniczo tryb wejścia komisijnego jest stosowany do kontroli wejścia do pomieszczeń o szczególnym poziomie ochrony np. sejfy, magazyny, archiwa itp.

Tryby Sterowania Drzwiami (Tryby Drzwi)

Tryb sterowania drzwiami (*Tryb Drzwi*) decyduje o sposobie sterowania zamkiem elektrycznym odpowiedzialnym za otwarcie drzwi. Kontroler udostępnia cztery tryby sterowania drzwiami:

- Tryb [Normalny]
- Tryb [Otwarte]
- Tryb [Warunkowo Otwarte]
- Tryb [Zamknięte]

Nazwa trybu	Zasady otwarcia drzwi
Tryb [Normalny]	W trybie tym drzwi pozostają normalnie w stanie zamknięcia (zamek jest nieaktywny), w następstwie identyfikacji uprawnionego identyfikatora kontroler zwalnia zamek na pewien zdefiniowany wcześniej czas umożliwiając w ten sposób otwarcie drzwi.
Tryb [Otwarte]	W trybie tym zamek elektryczny sterujący otwarciem jest w stanie permanentnego wyzolenia, każdy może otworzyć drzwi bez użycia uprawnionego identyfikatora. Tryb ten znajduje

	zastosowanie tam gdzie istnieje potrzeba otwarcia drzwi na stałe.
Tryb [Warunkowo otwarte]	Początkowo drzwi pozostają w stanie zamknięcia, z chwilą użycia pierwszego uprawnionego identyfikatora zamek zostaje zwolniony i pozostaje w stanie wyzwolenia do momentu zmiany trybu drzwi. Tryb ten zwykle stosuje się na wejściu do biura, sklepu itp., tam gdzie pierwsza osoba przychodząca rano do budynku (pomieszczenia) otwiera drzwi i drzwi pozostają przez pewien czas w stanie otwarcia tak aby kolejne osoby nie posiadające identyfikatorów mogły swobodnie wchodzić do pomieszczenia.
Tryb [Zamknięte]	W czasie trwania tego trybu kontroler całkowicie blokuje możliwość wejścia do pomieszczenia, próba użycia identyfikatora (uprawnionego lub nieuprawnionego) skutkuje odmową przyznania dostępu. Przez cały czas trwania tego trybu zamek sterujący otwarciem drzwi pozostanie w stanie pasywnym (nie wyzwolonym).

Domyślnie kontroler funkcjonuje w trybie *Normalnym* sterowania drzwiami, przejście do innego trybu może odbywać się poprzez manualne wydanie komendy z poziomu programu zarządzającego lub automatycznie według zdefiniowanego harmonogramu czasowego (*Harmonogram trybu drzwi*). Zarówno harmonogram czasowy jak i komenda manualna z PC mogą jednocześnie i w sposób równo uprawniony oddziaływać na aktualny tryb drzwiowy kontrolera. Ustawienie manualne trybu drzwi trwa do momentu najbliższej zmiany trybu drzwi wywołanej przez harmonogram czasowy.

Sterowanie Trybem Rejestracji RCP

Każdy punkt identyfikacji (kontroler z wbudowanym czytnikiem jak również terminal) w systemie RACS posiada swój domyślny tryb rejestracji RCP, tryb ten ustawia się z poziomu oprogramowania zarządzającego systemem KD. Każde przydzielenie dostępu do pomieszczenia jest rejestrowane w pamięci kontrolera wraz z odpowiednim znacznikiem wskazującym na aktualnie załączony tryb rejestracji RCP. PR302LCD dopuszcza dynamiczną zmianę trybu rejestracji RCP, zmianę taką można wykonać poprzez:

- wywołanie odpowiedniej funkcji z klawiatury kontrolera,
- za pomocą przycisku dołączonego do linii wejściowej kontrolera,
- automatycznie według zdefiniowanego harmonogramu czasowego (*Harmonogram trybu RCP*)

W przypadku dwóch pierwszych metod do wyboru jest wariant chwilowej (do momentu odczytu najbliższego identyfikatora) lub trwałej (na czas nieograniczony) zmiany trybu RCP. Istnieje możliwość zadeklarowania kodu, który będzie wymagany gdy zmiana trybu rejestracji będzie dokonywana z klawiatury. Kontroler dopuszcza zdefiniowanie osobnego hasła dla chwilowego wariantu zmiany trybu rejestracji RCP oraz osobnego hasła dla wariantu trwałej zmiany trybu rejestracji.

Uwaga: Nie jest możliwe dynamiczne sterowanie trybem rejestracji dołączonego do kontrolera terminala dostępu.

Zmiana trybu rejestracji RCP z klawiatury

Dostępne są następujące funkcje umożliwiające z poziomu klawiatury zmianę trybu RCP:

[*1][STU][#]<Hasło>[#]

Funkcja ta umożliwia tymczasową zmianę trybu rejestracji RCP, cyfry [STU] wskazują numer trybu RCP (każdy tryb RCP posiada w bazie danych systemu RACS swój numer identyfikacyjny). Po wydaniu tej komendy kontroler oczekuje na odczyt identyfikatora (pulsuje wskaźnik *SYSTEM*), gdy odczyt ten nastąpi zostanie zarejestrowane zdarzenie przyznania dostępu wraz z wskazanym trybem rejestracji po czym kontroler powraca do wcześniejszego trybu rejestracji. Gdy w przeciągu 8 sekund od momentu wydaniu komendy odczyt identyfikatora nie nastąpi to kontroler samoczynnie powraca do wcześniejszego trybu rejestracji. Jeśli zdefiniowane hasło dla chwilowej zmiany trybu rejestracji, to należy je wprowadzić bezpośrednio po pierwszym znaku [#] inaczej zmiana nie zostanie zaakceptowana. Przy braku zdefiniowanego hasła lub gdy zdefiniowane hasło jest puste kontroler zmienia tryb rejestracji bezpośrednio po pierwszym znaku [#] i nie oczekuje na wprowadzenia hasła.

[*3][STU][#]<Hasło>[#]

Funkcja ta umożliwia stabilną zmianę trybu rejestracji, cyfry [STU] wskazują numer trybu RCP. Po wydaniu tej komendy kontroler zmienia tryb rejestracji i pozostaje w nim do momentu wydania kolejnej komendy zmieniającej tryb rejestracji. Jeśli zostało zdefiniowane hasło dla trwałej zmiany trybu rejestracji to należy je wprowadzić bezpośrednio po pierwszym znaku [#], inaczej zmiana nie zostanie zaakceptowana. Przy braku zdefiniowanego hasła lub gdy zdefiniowane hasło jest puste kontroler zmienia tryb rejestracji bezpośrednio po pierwszym znaku [#] i nie oczekuje na wprowadzenia hasła.

[*1][255][#]

Powrót do normalnego (zdefiniowanego w bazie danych systemu RACS) trybu rejestracji RCP.

[*][#]...[*][#][#]

Wprowadzenie sekwencji [*][#] powoduje przejście kontrolera do kolejnego z dostępnych trybów rejestracji RCP, po przejściu do nowego trybu rejestracji kontroler pozostaje w nim aż do momentu kolejnej zmiany trybu RCP wymuszonej w jeden z dozwolonych sposobów lub spowodowanej funkcjonowaniem harmonogramu trybu RCP. Sekwencja [*][#] może być powtarzana dowolną ilość razy aż do momentu gdy na wyświetlaczu pojawi się pożądaný tryb rejestracji.

Zmiana trybu RCP z linii wejściowej

Zmianę trybu RCP można wykonywać również za pomocą zewnętrznych przycisków dołączonych do linii wejściowych kontrolera. Możliwe są następujące warianty sterowania trybem RCP z linii wejściowych:

[Zmienia tryb RCP – klucz stały]

Każdorazowe wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do kolejnego z dostępnych trybów RCP. Po ustawieniu nowego trybu RCP kontroler pozostaje w nim na czas nieograniczony tzn. do momentu kolejnej zmiany wywołanej poprzez użycie klawiatury urządzenia, odpowiednio zdefiniowanej linii wejściowej lub spowodowanej funkcjonowaniem harmonogramu trybu RCP.

[Zmienia tryb RCP – klucz chwilowy]

Każdorazowe wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do kolejnego z dostępnych trybów RCP. Po ustawieniu nowego trybu RCP kontroler pozostaje w nim do momentu odczytu kolejnego identyfikatora lecz nie dłużej niż 8 sekund.

[Ustawia zadeklarowany tryb RCP – klucz stały]

Każdorazowe wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do wskazanego wcześniej w ustawieniach kontrolera trybu RCP. Po ustawieniu nowego trybu RCP kontroler pozostaje w nim na czas nieograniczony tzn. do momentu kolejnej zmiany wywołanej poprzez użycie klawiatury urządzenia, odpowiednio zdefiniowanej linii wejściowej lub spowodowanej funkcjonowaniem harmonogramu trybu RCP.

[Ustawia zadeklarowany tryb RCP – klucz chwilowy]

Każdorazowe wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do wskazanego wcześniej w ustawieniach kontrolera trybu RCP. Po ustawieniu nowego trybu RCP kontroler pozostaje w nim do momentu odczytu kolejnego identyfikatora lecz nie dłużej niż 8 sekund.

Programowanie kontrolera

Programowanie kontrolera może odbywać się jedynie z poziomu komputera zarządzającego systemem KD lub innego podłączonego do kontrolera za pomocą interfejsu komunikacyjnego UT-2 lub UT-4. Przesyłanie ustawień do kontrolera odbywa się w sposób transakcyjny, oznacza to że w przypadku gdy proces przesyłania nie zakończy się sukcesem (np. nastąpi awaria łącza komunikacyjnego) to na kontrolerze będą obowiązywały stare ustawienia, kontroler przyjmuje nowe ustawienia dopiero wtedy gdy cały proces przesyłania nowej konfiguracji zakończy się sukcesem. Cecha ta ma szczególne ważne znaczenie w przypadku obsługi kontrolerów zlokalizowanych w innych budynkach lub nawet miejscowościach, (np. dołączonych do komputera programującego za pośrednictwem sieci komputerowej TCP/IP lub za pośrednictwem łącza modemowego).

Wyjście Przekaznikowe (Zaciski Door)

Wyjście przekąźnikowe jest przeznaczony do sterowania elementem wykonawczym odpowiedzialnym za sterowanie dostępem (zwora elektromagnetyczna, elektro-zaczep). Wyjście te udostępnia jedną parę styków NO/NC o obciążalności 1.5A /24V DC lub AC. Styki przekąźnika zabezpieczono przed przepięciami elementami typu MOV (warystor tlenkowy) dzięki czemu znacznie wydłużono ich żywotność.

Uwaga: Przekroczenie dopuszczalnych wartości napięcia przełączanego przez przekąźnik może spowodować uszkodzenie elementów zabezpieczających kontakty przekąźnika i tym samym spowodować wadliwe działanie wyjścia.

Wyjście przekąźnikowe może być załączane na czas zdefiniowany w zakresie od 1 sek. do 99 min. po upływie którego powróci do stanu normalnego lub może być sterowany w sposób Bi-stabilny, tzn. każde wyzwolenie powoduje przejście przekąźnika do stanu przeciwnego (tzn. z stanu normalnego do stanu wyzwolenia lub odwrotnie).

Interfejs Komunikacyjny RS485 (Linie A i B)

Dla celów komunikacji kontroler został wyposażony w interfejs pracujący w standardzie *RS485*. Standard ten zapewnia komunikację na dystansie do 1200 metrów w warunkach zakłóceń przemysłowych. Zbudowanie magistrali komunikacyjnej polega na połączeniu elektrycznym wszystkich zacisków typu A i zacisków typu B znajdujących się na wszystkich kontrolerach zainstalowanych w systemie kontroli dostępu i podłączenie ich do interfejsu komunikacyjnego typu UT-2. Nie jest wymagane zachowanie żadnej sztywno określonej topologii magistrali komunikacyjnej, dopuszczalne są zatem struktury typu gwiazda, drzewo oraz różne kombinacje oby wymienionych topologii. Interfejs komunikacyjny typu UT-2 może być włączony w dowolnym miejscu magistrali.

Uwaga: W przypadku gdy długość magistrali przekracza 1200 metrów, można zastosować interfejs UT-3, który umożliwia przedłużenie magistrali o kolejne 1200 m lub skorzysta z interfejsu UT-4, który umożliwia podłączenie kontrolera lub całego podsystemu złożonego z wielu kontrolerów do sieci komputerowej i za jej pośrednictwem do komputera PC.

Zaleca się aby magistralę komunikacyjną systemu RACS wykonać przy pomocy nie ekranowanego kabla typu skrętka (UTP). Zastosowanie kabli ekranowanych należy ograniczyć do instalacji narażonych na silne zakłócenia przemysłowe. W przypadku gdy w obiekcie, gdzie jest instalowany system KD, istnieje już jakiś rodzaj okablowania to z dużym prawdopodobieństwem można przewidywać, że istniejące okablowanie zapewni zadawalające wyniki jeśli chodzi o pewność transmisji i nie będzie wymagane prowadzenie nowej magistrali komunikacyjnej.

Interfejs Clock&Data

Kontroler umożliwia obsługę dodatkowego terminala identyfikacji (czytnika RFID/PIN) oraz innych modułów rozszerzających (np. ekspander wejść i wyjść, moduł zegarowy, LCD i inne) podłączonych do linii *Clock* i *Data*. Każdy z modułów podłączonych do magistrali *Clock&Data* musi posiadać indywidualny adres (numer ID), który zwykle ustawia się na zworach lub mostkach programujących. Dołączenie dodatkowego terminala identyfikacji umożliwia obustronną kontrolę przejścia lub oddalenie punktu identyfikacji od kontrolera (np. gdy w celu podwyższenia poziomu bezpieczeństwa kontroler powinien być zainstalowany w

miejsu chronionym). Przy obustronnej kontroli przejścia domyślnie przyjmuje się, że terminal zewnętrzny będzie pełnił rolę czytnika wejściowego do pomieszczenia, natomiast kontroler zostanie umieszczony wewnątrz pomieszczenia i będzie traktowany jako terminal wyjściowy z pomieszczenia. Przyprządowanie to jest istotne ze względu na działanie pewnych funkcji systemu, które zajmują się lokalizacją użytkowników w poszczególnych pomieszczeniach lub strefach obiektu oraz ze względu na działania funkcji anti-passback. Zmiana tego przyporządkowania jest możliwa podczas konfiguracji przejścia. Jeśli chodzi o wymogi stawiane okablowaniu linii *Clock&Data* to zasadniczo nie stawia się żadnych ograniczeń na typ kabla z wyjątkiem ograniczenia jego długości do 150m.

Uwaga: Format transmisji *Clock&Data* stosowany w kontrolerach serii PR jest nazywany formatem RACS i nie jest on zgodny z formatami *Clock&Data* stosowanymi przez innych producentów urządzeń kontroli dostępu. W przypadku gdy istnieje potrzeba współpracy kontrolera serii PR z czytnikiem pracującym w standardzie *Wiegand/Magstripe* należy zastosować moduł pośredniczący typu WMC-1.

Linie Wejściowe

Kontroler udostępnia trzy linie wejściowe ogólnego przeznaczenia: IN1, IN2 oraz IN3. Wszystkie te linie mają identyczną strukturę elektryczną i posiadają rezystor 5,6 kΩ połączony z pusem zasilania (gdy brak zewnętrznego sterowania rezystor ten wymusza na wejściu linii potencjał dodatni). Każdą z linii wejściowych można skonfigurować jako linię typu NO lub NC. Wyzwolenie linii typu NO następuje przez zwarcie jej z minusem zasilania. Wejście skonfigurowane jako NC w stanie normalnym musi być zwarte z minusem zasilania, wyzwolenie tego typu linii następuje poprzez odłączenie jej od potencjału minusa. Wyzwolenie linii wejściowej wymaga podania stabilnego stanu elektrycznego przez okres większy niż 500ms, wejście ignoruje stany elektryczne gdy czas ich trwania jest mniejszy niż 200ms. Detekcja sygnałów o czasie trwania pomiędzy 200 i 500ms nie jest gwarantowana. Każde z wejść kontrolera może podlegać działaniu harmonogramu czasowego dzięki czemu można zdefiniować okresy czasu gdy funkcjonowanie wejścia będzie zawieszane.

Funkcja linii wejściowej	Opis działania
Wejście ignorowane	Załączenie tej funkcji powoduje że linia jest nieobsługiwana (zablokowana). Funkcja ta jest pomocna gdy istnieje potrzeba tymczasowego (np w celach serwisowych) wyłączenia obsługi danej linii bez konieczności odłączania przewodów.
Czujnik otwarcia (DC)	Linia zdefiniowana w ten sposób jest dedykowana do współpracy z czujnikami otwarcia drzwi. Wyzwolenie tej linii jest interpretowane jako otwarcie drzwi, gdy linia jest w stanie normalnym kontroler interpretuje to jak stan domknięcia drzwi.
Przycisk wyjścia (DR)	Linia zdefiniowana w ten sposób jest dedykowana do współpracy z przyciskiem którego aktywacja powoduje zwolnienie zamka sterującego otwarciem drzwi.
Steruje trybem [ZAŁ/WYŁ] - klucz stały	Wyzwolenie linii powoduje przejście kontrolera do stanu ZAŁ, gdy linia jest nie wyzwolona kontroler powraca do stanu WYŁ. Uwaga: Tylko jedna z linii wejściowych może być zdefiniowana do tej funkcji. W przypadku wybrania tej funkcji automatycznemu wyłączeniu ulegają wszystkie inne metody sterowania trybem ZAŁ/WYŁ kontrolera.
Dozór napięcia sieci AC	Wyzwolenie linii powoduje generację zdarzenia [Zanik napięcia sieci AC], powrót linii do stanu normalnego powoduje powstanie zdarzenia [Powrót napięcia sieci AC]. Lina tego typu przeznaczona jest do współpracy z wyjściem zasilacza sygnalizującym obecność/zanik napięcia sieci AC.
Dozór stanu akumulatora	Wyzwolenie linii powoduje generację zdarzenia [Dozór stanu akumulatora - wyzwolenie], powrót linii do stanu normalnego powoduje powstanie zdarzenia [Dozór stanu akumulatora - powrót]. Lina tego typu przeznaczona jest do współpracy z wyjściem zasilacza sygnalizującym stan naładowania akumulatora.
Przycisk przywołania (Bell)	Wyzwolenie linii powoduje generację zdarzenia [Przycisk przywołania - wyzwolenie], powrót linii do stanu normalnego powoduje powstanie zdarzenia [Przycisk przywołania - powrót]. Lina tego typu przeznaczona jest do współpracy z przyciskiem który ma sygnalizować chęć wejścia do pomieszczenia.
Linia antysabotażowa (Tamper)	Wyzwolenie linii powoduje generację zdarzenia [Linia antysabotażowa - wyzwolenie], powrót linii do stanu normalnego powoduje powstanie zdarzenia [Linia antysabotażowa - powrót]. Lina tego typu przeznaczona jest do współpracy z łącznikiem ochrony antysabotażowej obudowy.
Czujnik ruchu	Wyzwolenie linii powoduje generację zdarzenia [Czujnik ruch - wyzwolenie], powrót linii do stanu normalnego powoduje powstanie zdarzenia [Czujnik ruchu - powrót]. Lina tego typu przeznaczona jest do współpracy z czujnikiem ruchu lub innym detektorem systemu antywłamaniowego. Lina tego typu może być automatycznie blokowana gdy kontroler przechodzi do trybu ZAŁ, celowi temu służy opcja [Ignoruj linię Czujnik ruchu w trybie ZAŁ].
Steruje trybem [ZAŁ/WYŁ] - klucz chwilowy	Każde wyzwolenie tej linii powoduje zmianę aktualnego trybu ZAŁ/WYŁ na przeciwny. Zaprogramowanie linii wejściowej do tej funkcji nie blokuje możliwości sterowania trybem ZAŁ/WYŁ innymi metodami (np. identyfikatorem SWITCHER lub z harmonogramu czasowego). Każdemu wyzwoleniu tej linii towarzyszy powstanie zdarzenia [Przejście

	kontrolera do trybu ZAŁ] lub [Przejście kontrolera do trybu WYŁ] w zależności od tego do którego z trybów przeszedł kontroler w następstwie wyzwolenia linii wejściowej.
Blokuje dostęp	Gdy linia tak skonfigurowana przechodzi do stanu wyzwolenia kontroler blokuje dostęp do pomieszczenia bez względu na aktualnie obowiązujące ustawienia praw dostępu, blokada dostępu jest utrzymywana przez cały czas wyzwolenia linii. Wyzwolenie linii jest odnotowywane poprzez zdarzenia [Blokuje dostęp – wyzwolenie] natomiast powrót linii poprzez zdarzenie [Blokuje dostęp – powrót].
Zmienia tryb RCP - klucz stały	Każde wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do kolejnego z wcześniej zdefiniowanych trybów RCP. Zmiana trybu RCP następuje na czas nieokreślony. Zmiana trybu RCP jest odnotowywana odpowiednim zdarzeniem.
Zmienia tryb RCP - klucz chwilowy	Każde wyzwolenie linii tak skonfigurowanej powoduje przejście kontrolera do kolejnego z wcześniej zdefiniowanych trybów RCP. Zmiana trybu RCP następuje na czas odczytu najbliższego identyfikatora lecz nie dłużej niż na 8 sekund. Zmiana trybu RCP jest odnotowywana odpowiednim zdarzeniem.
Ustawia zadeklarowany tryb RCP - klucz stały	Każde wyzwolenie tego typu linii powoduje przejście kontrolera do trybu RCP który został wcześniej dla tej linii określony w ustawieniach kontrolera. Przejście do nowego trybu RCP następuje na czas nieokreślony.
Ustawia zadeklarowany tryb RCP - klucz chwilowy	Każde wyzwolenie tego typu linii powoduje przejście kontrolera do trybu RCP który został wcześniej dla tej linii określony w ustawieniach kontrolera. Przejście do nowego trybu RCP następuje na do momentu odczytu najbliższego identyfikatora lecz nie dłużej niż na 8 sekund.
Zeruje rejestr APB	Każde wyzwolenie tej linii powoduje wyzerowanie rejestru funkcji <i>anti-passback</i> . Po wyzerowaniu rejestru APB każdy z użytkowników może użyć swojego identyfikatora zarówno na wejściu jak i na wyjściu z pomieszczenia.

Linie Wyjściowe IO1 i IO2

Obydwie linie wyjściowe składają się z tranzystora typu NMOS i są w stanie przełączać prąd stały o wartości 1A. W stanie normalnym linia wyjściowa tego typu znajduje się w stanie wysokiej impedancji, gdy następuje wyzwolenie, tranzystor wyjściowy przechodzi do stanu niskiej impedancji w wyniku czego na wyjściu linii pojawia się potencjał minusa zasilania. Obydwie linie można skonfigurować do kilku predefiniowanych funkcji jak również można skojarzyć z harmonogramem czasowym, który umożliwi czasowe blokowanie ich działania. Każda z linii jest zabezpieczona przed przeciążeniem prądowym oraz przed przepięciami, które mogą pojawiać się w trakcie sterowania obciążeniem indukcyjnym (np. cewką przekaźnika wykonawczego).

Uwaga: Linie IO1 i IO2 nie można używać do przełączania prądu zmiennego, maksymalny prąd przełączany przez te linie wynosi 1A a dołączony potencjał 16V względem minusa zasilania.

Funkcja linii wyjściowej	Opis działania
Wyjście alarmowe	Wyjście jest aktywowane w momencie powstania w kontrolerze jednego z dozwolonych alarmów. Zasadniczo możliwa jest sygnalizacja trzech sytuacji alarmowych: PREALAR, DRZWI OTWARTE oraz WEJŚCIE SIŁOWE. Każdy z tych alarmów jest sygnalizowany w odmienny sposób.
Wyjście sterowane z PC	Wyjście jest aktywowane/dezaktywowane poprzez wydanie zdalnej komendy z poziomu komputera zarządzającego systemem kontroli dostępu.
Sygnalizuje tryb ZAŁ.	Wyjście jest aktywowane gdy kontroler znajduje się w trybie ZAŁ.
Sygnalizuje przyznanie dostępu	Wyjście jest każdorazowo aktywowane w następstwie przyznania dostępu przez kontroler, wyjście pozostaje wywołone przez czas otwarcia drzwi, lecz nie dłużej niż określa to parametr [Czas aktywacji zamka]. Wyjście to nie jest aktywowane gdy przyznanie dostępu nastąpiło w wyniku użycia przycisku wyjścia (DR).
Sygnalizuje otwarcie drzwi	Wyjście przechodzi do stanu aktywnego w wyniku rozpoznania otwarcia drzwi i pozostaje aktywne tak długo jak drzwi pozostają otwarte.
Sygnalizuje odmowę dostępu	Wyjście jest każdorazowo aktywowane w następstwie odmowy dostępu przez kontroler.
Sterowane wyłącznie przez harmonogram	Wyjście jest aktywowane/dezaktywowane według harmonogramu czasowego wcześniej zdefiniowanego w ustawieniach programu zarządzającego systemem KD.
Sterowane przez harmonogram + z PC	Wyjście jest aktywowane/dezaktywowane według harmonogramu czasowego wcześniej zdefiniowanego w ustawieniach programu zarządzającego systemem KD oraz może być sterowane poprzez wydanie interaktywnej komendy z poziomu PC.
Sygnalizuje identyfikację na terminalu ID=0	Wyjście jest aktywowane gdy przyznanie dostępu nastąpiło na terminalu o adresie ID=0, wyjście pozostaje w stanie aktywnym do momentu aż nastąpi identyfikacja na terminalu o adresie ID=1. Wyjście tego typu służy zwykle do realizacji sterowania bramkami typu „Tripod” lub podobnymi gdzie istnieje konieczność sterowania ruchem „lewo”/”prawo” lub „wejście/wyjście”.

Ochrona Antysabotażowa

W celu zabezpieczenia kontrolera przed ingerencją osób postronnych do jego wnętrza kontroler wyposażono w łącznik ochrony antysabotażowej. W stanie normalnym łącznik tej jest w stanie zwarcia, otwarcie obudowy urządzenia powoduje przejście łącznika do stanu otwarcia. Styki łącznika ochrony antysabotażowej można połączyć w szeregu z łącznikami *TAMPER* innych urządzeń i podłączyć do odpowiedniego wejścia centrali CPR lub centrali systemu alarmowego. Istnieje również możliwość podłączenia łącznika antysabotażowego bezpośrednio do linii wejściowej kontrolera skonfigurowanej jako [Wejście antysabotażowe *TAMPER*]. W tym drugim przypadku wywołanie i powrót łącznika antysabotażowego będą rejestrowane w historii zdarzeń systemu oraz na konsoli operatora systemu *RACS*.

Sygnalizacja Optyczna

Dla celów komunikacji z użytkownikiem, kontroler posiada trzy wskaźniki LED opisane jako *ZAŁ/WYŁ*, *OTWARTE*, *SYSTEM* oraz sygnalizator akustyczny (*BZZZER*). Wskaźnik *ZAŁ/WYŁ* jest wskaźnikiem dwukolorowym, gdy świeci na zielono oznacza to, że kontroler jest w trybie *ZAŁ* (*ZAŁACZONE*), gdy wskaźnik ten świeci na czerwono to kontroler znajduje się w trybie *WYŁ* (*WYŁĄCZONE*). Wskaźnik *OTWARTE* jest koloru zielonego, gdy świeci na stałe sygnalizuje, że kontroler przydzielił dostęp (aktywował wyjście przekąźnikowe), gdy wskaźnik ten pulsuje wskazuje to, że kontroler oczekuje na wprowadzenie identyfikatora *MASTER* (np. w celu wejścia do trybu programowania). Wskaźnik *SYSTEM* jest koloru bursztynowego, wskaźnik ten jest załączany krótkotwale, każdorazowo po wprowadzeniu PIN kodu lub po odczytanie karty, gdy wskaźnik *SYSTEM* pulsuje oznacza to że kontroler oczekuje na wprowadzenie identyfikatora *SWITCHER* lub *MASTER* celem zmiany aktualnie aktywnego stanu *ZAŁ/WYŁ*. Gdy wszystkie wskaźniki LED są zapalone i towarzyszy temu cyklicznie powtarzany sygnał dźwiękowy oznacza to, że uszkodzeniu uległa zawartość pamięci i kontroler wymaga ponownego zaprogramowania. W trakcie przesyłania ustawień do kontrolera wskaźniki *ZAŁ/WYŁ* oraz *OTWARTE* sygnalizują przepływ danych pomiędzy kontrolerem a komputerem PC i są zapalane synchronicznie w takt przychodzących/wychodzących pakietów danych.

Uwaga: Gdy w następstwie wprowadzenia identyfikatora (karty lub kodu) kontroler wygeneruje jeden krótki sygnał akustyczny poczym pojawi się jeden sygnał długi to oznacza to, że wprowadzony identyfikator nie jest zarejestrowany w pamięci kontrolera (jest obcy), gdy jednak w miejsce sygnału długiego wygeneruje dwa zwykłe tony akustyczne to oznacza że identyfikator jest zarejestrowany w kontrolerze lecz w danej chwili nie posiada prawa dostępu.

Sygnaly Akustyczne

Kontroler generuje następujące sygnaly akustyczne:

Brzmienie sygnału	Znaczenie sygnału
Jeden krótki sygnał (1 x <i>BEEP</i>)	Odczyt karty lub naciśnięcie klawisza.
Dwa krótkie sygnały (2 x <i>BEEP</i>)	Sygnał OK, kontroler oczekuje na dalszą część komendy (funkcji).
Dwa krótkie sygnały (3 x <i>BEEP</i>)	Sygnał OK, polecenie (funkcja) wykonana prawidłowo.
Jeden długi sygnał (1 x <i>LONG BEEP</i>)	Nieznana karta lub niezany PIN kod.
Dwa krótkie sygnały (2 x <i>LONG BEEP</i>)	Karta/PIN poprawny lecz w danej chwili brak uprawnień do wejścia.
Sygnał długi powtarzany cyklicznie (<i>LONG BEEP</i>)	Uszkodzenie danych w pamięci, wymagany jest Reset Pamięci.

Aktualizacja Oprogramowania Firmowego - Fleszowanie Kontrolera

Aktualizacja oprogramowania sterującego urządzeniem polega na przesłaniu nowej wersji programu (*firmware*) do pamięci kontrolera. Operacja ta jest zwykle wykonywana gdy producent urządzenia udostępni nowe, ulepszone i wzbogacone oprogramowanie sterujące wybranym urządzeniem. Zasadniczo operację fleszowania urządzenia można wykonać bezpośrednio w systemie w którym ono pracuje bez konieczności jego demontażu, można również je zdemontować i podłączyć do innego komputera, niemniej w obydwu wymienionych przypadkach przesłanie oprogramowania wymaga zastosowania interfejsu UT-2 oraz programu ładującego *RogerISP*.

Uwaga: Każdorazowo przed aktualizacją oprogramowania w kontrolerze należy upewnić się czy oprogramowanie zarządzające systemem KD (pakiet *RACS*) umożliwia obsługę urządzeń z nowszym oprogramowaniem firmowym i ewentualnie zainstalować nowszą wersję pakietu *RACS*.

Reset Pamięci Ustawień

RESET pamięci ustawień kasuje wszystkie dotychczasowe ustawienia kontrolera i nadaje im ustawienia fabryczne, dodatkowo umożliwia zaprogramowanie nowego identyfikatora *MASTER* oraz nowego adresu ID kontrolera. W celu dokonania RESETU pamięci należy wykonać następujące kroki:

- otworzyć obudowę urządzenia,
- nacisnąć przycisk *Memory Reset* i trzymać go aż do momentu gdy zacznie pulsować wskaźnik *OTWARTE*,
- wprowadzić sekwencję: [**Kod**] + [**#**] + [**Karta**] + [**ID**] + [**#**]

Gdzie:

[**Kod**] to nowy PIN kod *MASTER*,

[**Karta**] to nowa karta *MASTER* oraz

[**ID**] to nowy numer identyfikacyjny (adres) kontrolera, numer *ID* powinien zawierać się w zakresie od 00 do 99.

Po tym ostatnim kroku kontroler dokona skasowania starych ustawień i zapisze w pamięci ustawienia nowo wprowadzone, (czynności ta może trwać ok. 5 sekund) poczym kontroler przejdzie do zwykłego trybu pracy.

Instalacja Kontrolera

Kontroler powinien być zainstalowany na pionowym fragmencie konstrukcji, zwykle w pobliżu drzwi, wszystkie połączenia elektryczne powinny być dokonane przy wyłączonym napięciu zasilania.

- w przypadku konieczności zainstalowania kontrolera na podłożu metalowym należy pomiędzy czytnikiem a podłożem umieścić niemetaliczną przekładkę (np. płytę gipsową) o grubości min. 10mm,
- minusy wszystkich zasilaczy powinny być na wspólnym potencjalnie, można to uzyskać łącząc je wspólnym przewodem wyrównującym potencjały lub je indywidualnie uziemiać,
- zaleca się uziemienie minusa zasilania systemu,
- ze względu na relatywnie małą moc promieniowania elektromagnetycznego czynniki nie powinien zakłócać pracy innych urządzeń, niemniej inne urządzenia generując zakłócenia mogą utrudniać odczyt kart, dotyczy to w szczególności urządzeń radiowych oraz lampowych monitorów komputerowych,
- zaleca się aby minimalna odległość pomiędzy czytnikami zbliżeniowymi nie była mniejsza niż 0.5 m,
- w przypadku gdy w miejscu docelowej instalacji obserwuje się pogorszenie parametrów czytnika w zakresie odczytu kart (zredukowany zasięg lub fałszywe odczyty) należy rozważyć zmianę lokalizacji czytnika,
- PR302LCD jest przystosowany do pracy wewnątrz budynków, instalacja czytnika na zewnątrz budynków jest niedopuszczalna.

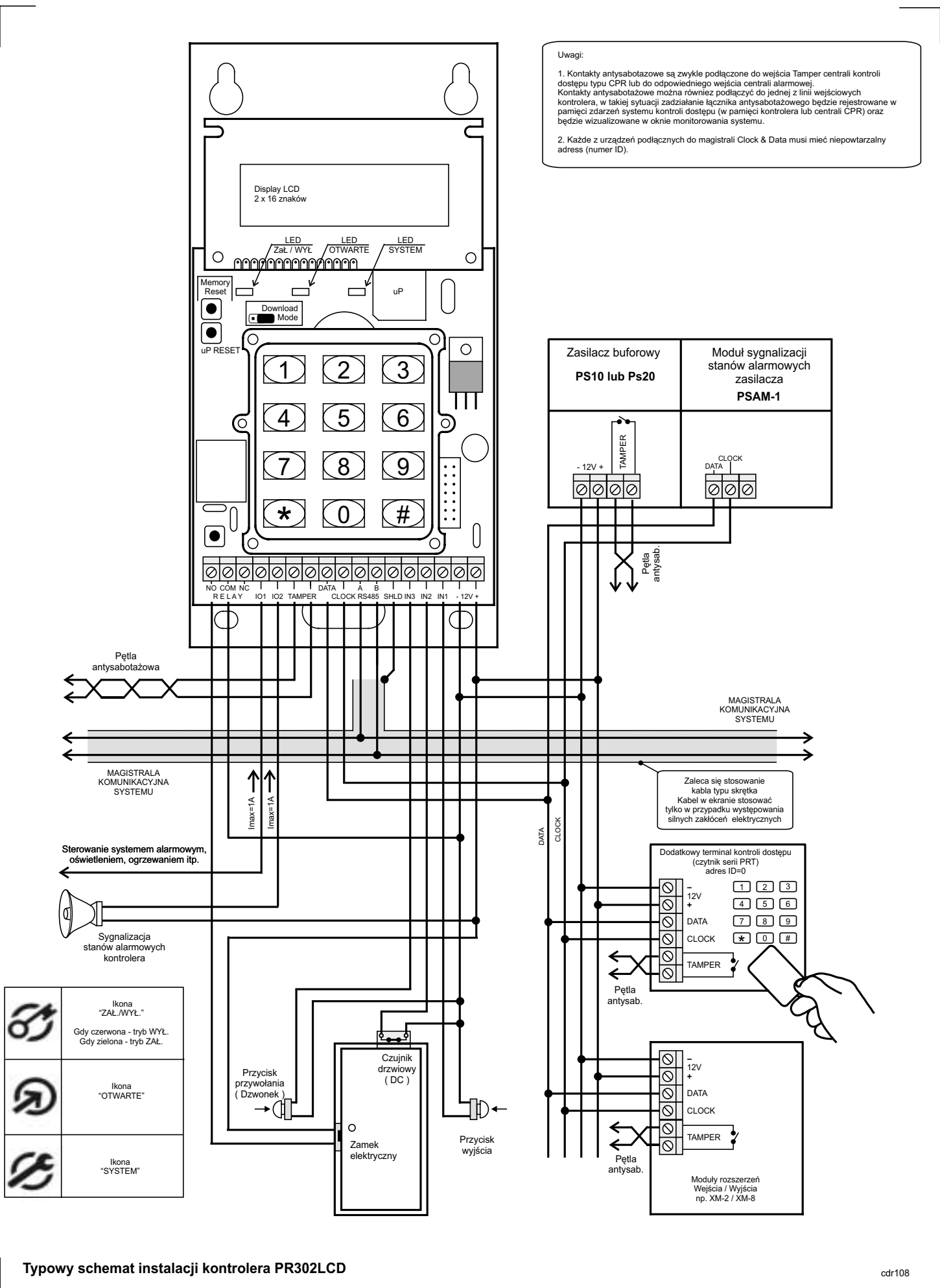
Zasilanie Kontrolera

PR302LCD powinien być zasilany z źródła napięcia stałego z zakresu od 10.0 to 16.0 VDC wyposażonego w baterię rezerwową. Znamionowy pobór prądu kontrolera wynosi 120 mA i może wzrosnąć do wartości 170 mA gdy załączony jest przełącznik wyjściowy. Przy projektowaniu zasilania szczególną uwagę należy zwrócić aby maksymalny spadek napięcia pomiędzy zasilaczem a kontrolerem nie przekroczył wartości 1.0V w chwilach największego poboru prądu. Prawidłowe zasilanie urządzeń ma krytyczny wpływ na pracę systemu kontroli dostępu. Dużym zagrożeniem dla funkcjonowania kontrolera jest zasilanie zamka elektrycznego (zwory lub zaczepu) z tego samego źródła co kontroler, zdarza się, że z powodu braku precyzyjnie przeprowadzonego bilansu prądów i spadków napięć w przewodach zasilających dochodzi do powstawania chwilowych zapadów napięcia, które wykraczają poniżej dopuszczalnego zakresu napięcia zasilania akceptowanego przez kontroler. Jeśli jednak podjęto decyzję aby zasilac elementy wykonawcze z tego samego źródła co urządzenia elektroniczne, należy do zasilania elementów wykonawczych zastosować osobne pary przewodów zasilających. Ze względu na to, że większość systemów kontroli dostępu jest rozproszona na obszarze dziesiątek lub setek metrów (odległość liczona po kablu), zachodzi konieczność stosowania zasilania rozproszonego. W takim przypadku zaleca się grupowanie urządzeń w strefy i zasilanie ich z osobnych zasilaczy zainstalowanych możliwie blisko grupy zasilanych urządzeń. Gdy w systemie zastosowano więcej niż jeden zasilacz należy minusy zasilaczy połączyć dodatkowym przewodem wyrównującym potencjały, nie wolno jednak łączyć ze sobą plusów zasilania gdyż może to doprowadzić do zakłócenia procesu ładowania akumulatorów. Zaleca się stosowanie zasilaczy typu PS20N wyposażonych w funkcje sygnalizacji stanów alarmowych (Brak napięcia sieci oraz Niższy stan baterii). Z praktyki instalatorskiej wynika że zastosowanie jednego zasilacza tego typu zapewni z zapasem poprawne funkcjonowanie 4 przejść kontrolowanych dwustronnie. Do zasilania kontrolerów i terminali można użyć zarówno zasilaczy liniowych jak i impulsowych. W przypadku zastosowania zasilaczy impulsowych niskiej jakości (o dużym poziomie tętnień) może dojść do efektu ubocznego w postaci redukcji zasięgu czytania kart.

Oznaczenie wersji	
PR302LCD	Kontroler dostępu z metalową klawiaturą oraz wyświetlaczem LCD.

Dane techniczne	
Napięcie zasilania	10...16 VDC
Pobór prądu:	ok. 120mA
Ochrona antysabotażowa	Styki NO, obciążalność 50mA
Zasięg czytania kart	Do 7 cm dla karty ISO (zależy od jakości karty)
Karty zbliżeniowe	Standard UNIQUE, modulacja ASK, 125kHz (kompatybilne z EM4001/2)
Zakres temperatur otoczenia	0...+55° C.
Długość magistrali <i>Clock/Data</i> liczona po kablu	150 m (500 ft)
Odległość pomiędzy dowolnym kontrolerem a komputerem nadzorującym lub centralą CPR liczona po kablu	1200 m (4000 ft)
Wilgotność względna	10 to 95% (bez kondensacji)
Stopień ochrony przed wnikaniem:	IP30 (tylko do użytku wewnętrznego, brak zabezpieczenia przed wilgocią i deszczem)
Wymiary (mm):	97 X 176 X 29
Waga (gramy):	~740G

Opis zacisków podłączeniowych	
Nazwa zacisku	Funkcja
+ 12V -	Plus/minus zasilania
IN1	Linia wejściowa IN1
IN2	Linia wejściowa IN2
IN3	Linia wejściowa IN2
SHLD	Ekran magistrali RS485
A	Zacisk "A" magistrali RS485
B	Zacisk "B" magistrali RS485
CLK	Interfejs <i>Clock & Data</i> , linia <i>Clock</i>
DATA	Interfejs <i>Clock & Data</i> , linia <i>Data</i>
TAMP	Zaciski łącznika ochrony antysabotażowej, w stanie zamknięcia obudowy kontakty zwarte.
IO2	Tranzystorowa linia wyjściowa IO2
IO1	Tranzystorowa linia wyjściowa IO1
NC	Wyjście <i>Door</i> , styk "Normalnie zwarty" wyjścia przekaźnikowego
COM	Wyjście <i>Door</i> , styk "Wspólny" wyjścia przekaźnikowego
NO	Wyjście <i>Door</i> , styk "Normalnie otwarty" wyjścia przekaźnikowego



Uwagi:

1. Kontakty antysabotażowe są zwykle podłączone do wejścia Tamper centrali kontroli dostępu typu CPR lub do odpowiedniego wejścia centrali alarmowej. Kontakty antysabotażowe można również podłączyć do jednej z linii wejściowych kontrolera, w takiej sytuacji zadziałanie łącznika antysabotażowego będzie rejestrowane w pamięci zdarzeń systemu kontroli dostępu (w pamięci kontrolera lub centrali CPR) oraz będzie wizualizowane w oknie monitorowania systemu.
2. Każde z urządzeń podłączonych do magistrali Clock & Data musi mieć niepowtarzalny adres (numer ID).

Zaleca się stosowanie kabla typu skrętka. Kabel w ekranie stosować tylko w przypadku występowania silnych zakłóceń elektrycznych.

	Ikona "ZAŁ./WYŁ." Gdy czerwona - tryb WYŁ. Gdy zielona - tryb ZAŁ.
	Ikona "OTWARTE"
	Ikona "SYSTEM"

Typowy schemat instalacji kontrolera PR302LCD