

ROGER ACCESS CONTROL SYSTEM

roger[®]
Intelligence for Building



Oferta kontroli dostępu Roger

Grupy urządzeń:

- Elektroniczne zamki szyfrowe
- Czytniki
- Kontrolery
- Centrale
- Interfejsy
- Ekspandery
- Akcesoria



Elektroniczne zamki szyfrowe serii SL2000

Charakterystyka:

- Jedno wyjście przekaźnikowe oraz dwa wyjścia tranzystorowe
- Współpraca z czujnikiem otwarcia drzwi
- Kod Administratora, kod Główny oraz 55 kodów użytkownika
- Możliwość blokady dostępu, gdy zamek w trybie uzbrojenia
- Możliwość podłączenia przycisku wyjścia od środka
- Programowalna długość kodów użytkowników
- Trzy wskaźniki LED oraz głośnik
- Ochrona antysabotażowa (tamper)



SL2000E



SL2000F



SL2000F-VP



Czytniki zbliżeniowe EM 125 kHz – seria PRTxxLT

Charakterystyka:

- Praca wyłącznie w trybie terminalowym
- Obsługa kart EM 125 kHz
- Formaty wyjściowe: Wiegand 26..66 bit, Magstripe, RACS Clock&Data (Roger)
- Praca w warunkach zewnętrznych
- Ochrona antysabotażowa (tamper)



PRT12LT

PRT62LT

PRT66LT

PRT64LT

Czytniki zbliżeniowe EM 125 kHz – seria PRTxxEM

Charakterystyka:

- Praca w trybie terminalowym lub autonomicznym
- Obsługa kart EM 125 kHz
- Formaty wyjściowe: Wiegand 26..66 bit, Magstripe, RACS Clock&Data (Roger)
- Praca w warunkach zewnętrznych
- Wyjście przekaźnikowe oraz dwa wyjścia tranzystorowe
- Dwa wejścia NO/NC
- Możliwość dołączenia ekspandera we/wy typu XM-2DR oraz dodatkowego czytnika serii PRT
- Do 120 zaindeksowanych użytkowników (tryb autonomiczny)
- Bufor 1024 zdarzeń (tryb autonomiczny)
- Programowanie manualne lub z poziomu komputera
- Możliwość pracy jako programator kart EM 125 kHz (przy współpracy z programem RARC)



Czytniki zbliżeniowe 13.56 MHz MIFARE® - seria PRTxxMF

Charakterystyka:

- Praca w trybie terminalowym lub autonomicznym
- Karty 13.56 MHz standardu ISO/IEC 14443A i MIFARE Ultralight, Classic
- Odczyt numerów seryjnych (CSN) oraz programowalnych (PCN) i ich kombinacji
- Formaty wyjściowe: Wiegand 26..66 bit, Magstripe, RACS Clock&Data (Roger)
- Wyjście przekaźnikowe (PRT64MF i PRT66MF) oraz dwa wyjścia tranzystorowe
- Dwa wejścia NO/NC
- Możliwość dołączenia ekspandera we/wy typu XM-2DR oraz dodatkowego czytnika serii PRT
- Do 120 zaindeksowanych użytkowników (tryb autonomiczny)
- Bufor 1024 zdarzeń (tryb autonomiczny)
- Programowanie manualne lub z poziomu komputera
- Możliwość pracy jako programator kart MIFARE (przy współpracy z programem RARC)
- Praca w warunkach zewnętrznych



PRT12MF

PRT62MF

PRT66MF

PRT64MF

Czytnik zbliżeniowy 13.56 MHz MIFARE® DESFire®

Charakterystyka:

- Odczyt kart ISO/IEC 14443A/MIFARE Ultralight, Classic, DESFire EV1, Plus
- Odczyt numerów seryjnych (CSN) oraz programowalnych (PCN) i ich kombinacji
- Zasięg odczytu do 7 cm (dla MIFARE Classic)
- Przeznaczony do zastosowania w systemach kontroli dostępu wymagających wyższego poziomu bezpieczeństwa
- Formaty wyjściowe: RACS CLK/DTA, Wiegand 26..66bit
- Trzy wskaźniki LED
- Wejścia sterujące głośnikiem oraz wskaźnikiem LED
- Głośnik sygnalizacyjny
- Regulacja poziomu głośności oraz poziomu podświetlenia klawiatury
- Detekcja otwarcia obudowy oraz oderwania od podłoża
- Konfiguracja z PC (program RogerVDM)
- Praca w warunkach zewnętrznych



PRT12MF-DES

Czytniki zbliżeniowe 13.56 MHz MIFARE® - QUADRUS

Charakterystyka:

- Praca wyłącznie w trybie terminalowym
- Karty 13.56 MHz standardu ISO/IEC 14443A i MIFARE Ultralight, Classic
- Odczyt numerów seryjnych (CSN) oraz programowalnych (PCN) i ich kombinacji
- Podświetlana klawiatura dotykowa (sensoryczna)
- Formaty wyjściowe: Wiegand 26..66 bit, RACS Clock&Data (Roger)
- Praca w warunkach wewnętrznych
- Ochrona antysabotażowa (tamper)



PRT82MF

PRT84MF

Czytniki administratora systemu KD

Charakterystyka:

- Miniaturowy czytnik podłączany do portu USB komputera
- Zasilanie z portu USB
- Obsługa kart zbliżeniowych
- Zestaw narzędzi SDK umożliwiających integrację czytnika z innym oprogramowaniem

Zastosowanie RUD-2:

- Czytnik administratora systemu RACS 4 do wprowadzania kart EM 125 kHz z poziomu programu PR Master
- Odczyt numerów kart EM 125 kHz z poziomu bezpłatnego programu Roger MiniReader
- Sprzętowy klucz licencyjny dla oprogramowania RCP Master 2



RUD-2

Czytniki administratora systemu KD

Zastosowanie RUD-3/RUD-3-DES:

- Czytnik administratora systemu RACS 4 do wprowadzania kart z poziomu programu PR Master
- Odczyt numerów kart z poziomu bezpłatnego programu Roger MiniReader
- Czytnik/programator do obsługi kart z poziomu programu RogerVDM
- Sprzętowy klucz licencyjny dla oprogramowania RCP Master 2

gdzie:

- **RUD-3** obsługuje karty ISO/IEC 14443A/MIFARE Ultralight, Classic
- **RUD-3-DES** obsługuje karty ISO/IEC 14443A/MIFARE Ultralight, Classic, DESFire EV1



RUD-3
RUD-3-DES

Czytnik linii papilarnych RFT1000

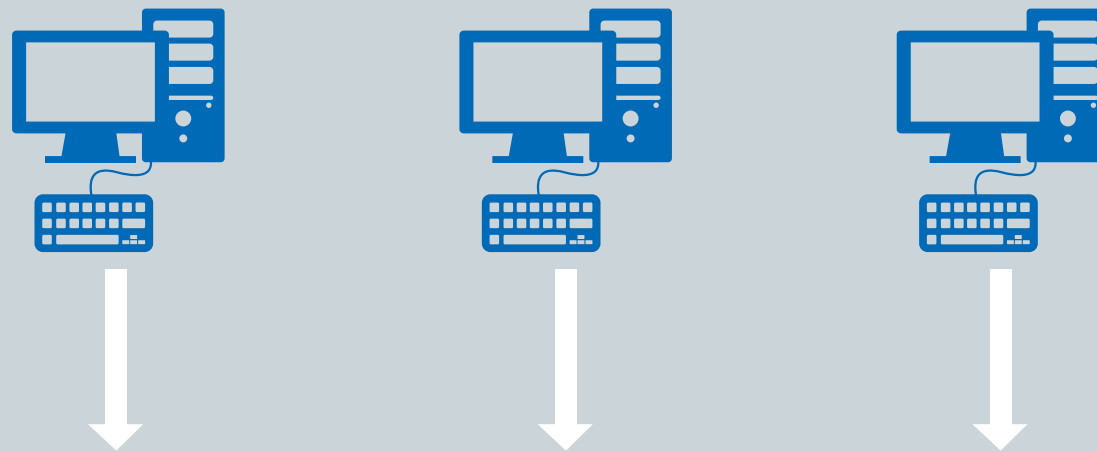
- Optyczny skaner linii papilarnych
- Wbudowany czytnik kart standardu ISO/IEC 14443A MIFARE
- Rozpoznanie w oparciu o dane biometryczne odczytane z karty (tzw. tryb 1:1)
- Rozpoznanie w oparciu o dane biometryczne zapisane w pamięci czytnika (tzw. tryb 1:N)
- Pamięć 1900 wzorów linii papilarnych
- Interfejsy wyjściowe RACS Clock&Data oraz Wiegand
- Program do konfiguracji czytnika i zarządzania użytkownikami (RogerVDM)
- Zarządzanie użytkownikami bezpośrednio z poziomu programu PR Master (system RACS 4)
- Szyfrowany protokół komunikacyjny AES128 CBC
- Konfiguracja przez port RS485 lub Ethernet



RFT1000

Struktura systemu RACS 4

Komputery z programem RACS Remote Monitor



Sieć Komputerowa (LAN lub WAN)

Podsystem nr 1

COM, USB lub Ethernet

Podsystem nr 2

COM, USB lub Ethernet

Do **250** sieci w jednym systemie kontroli dostępu
Do **32** kontrolerów w sieci
Do **1000** kontrolerów w systemie

Podsystem nr 250

COM, USB lub Ethernet



Komputer zarządzający
z programem PR MASTER



Koncepcja systemu RACS 4

RACS 4 to sieciowy system kontroli dostępu obejmujący kontrolery pojedynczego przejścia, czytniki, interfejsy komunikacyjne, moduły rozszerzeń, centrale oraz oprogramowanie zarządzające PR Master.

Funkcjonalność systemu zależy od rodzaju sprzętu użytego w danej instalacji. System RACS 4 może zostać podzielony na osobne gałęzie zwane podsystemami kontroli dostępu, przy czym w obrębie jednego systemu KD można zintegrować do 250 podsystemów. W każdym podsystemie może funkcjonować do 32 kontrolerów dostępu połączonych za pomocą magistrali komunikacyjnej RS485 o maksymalnej długości 1200m.

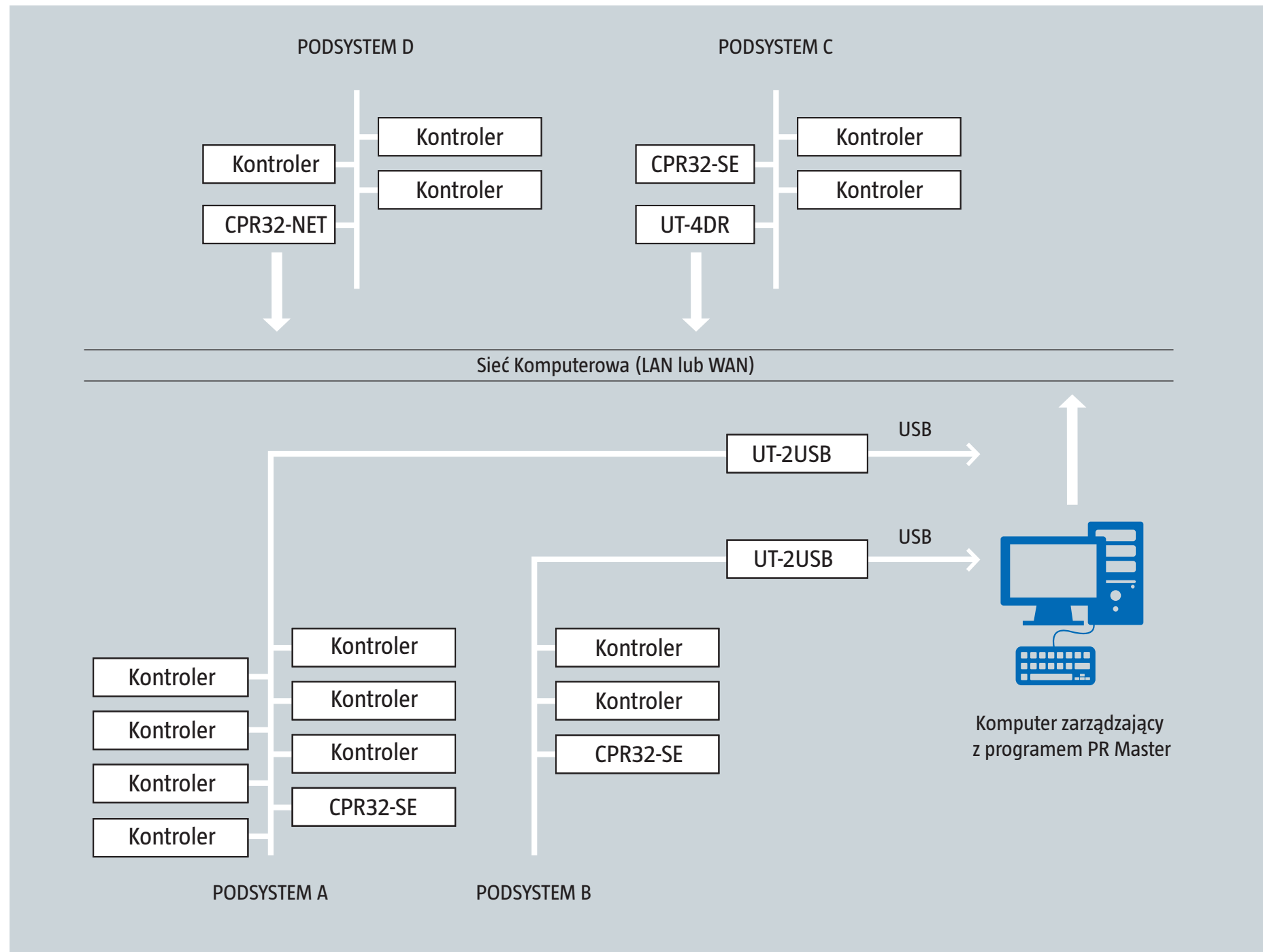


Koncepcja systemu RACS 4

Podstawowe pojęcia występujące w systemie RACS 4:

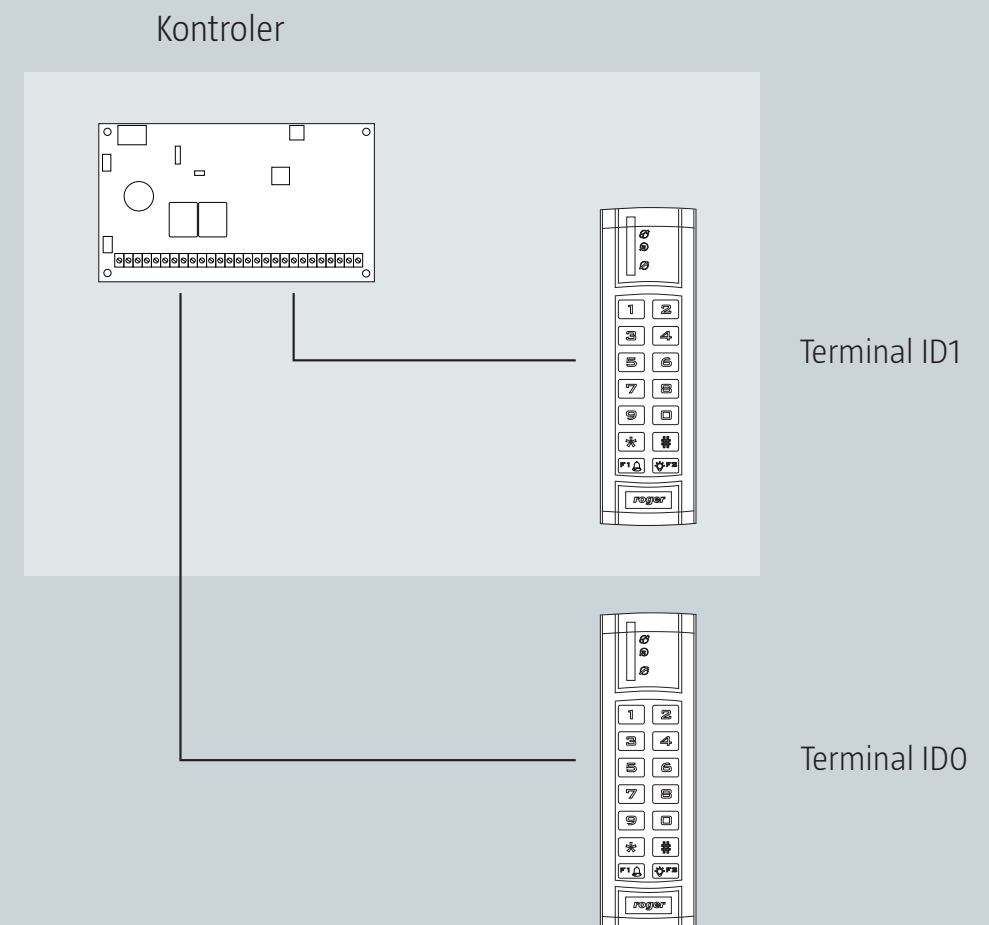
- Podsystem kontroli dostępu to struktura na którą składa się magistrala komunikacyjna RS485, interfejs komunikacyjny, kontrolery dostępu i opcjonalnie centrala serii CPR
- Kanały komunikacyjne kontrolera to układ linii elektrycznych służących do komunikacji pomiędzy urządzeniami
 - Magistrala komunikacyjna zewnętrzna RS485 (dwa przewody A i B)
 - Magistrala komunikacyjna wewnętrzna Clock&Data (dwa przewody CLK i DTA)
- Funkcje lokalne to funkcje realizowane w ramach jednego kontrolera
- Funkcje globalne to funkcje których realizacja wymaga wymiany danych pomiędzy różnymi kontrolerami
 - Strefy Anti-passback
 - Strefy Alarmowe
- Monitorowanie on-line to możliwość obserwacji zdarzeń powstających w systemie w czasie rzeczywistym na ekranie komputera

Przykład systemu RACS 4 z czterema podsystemami



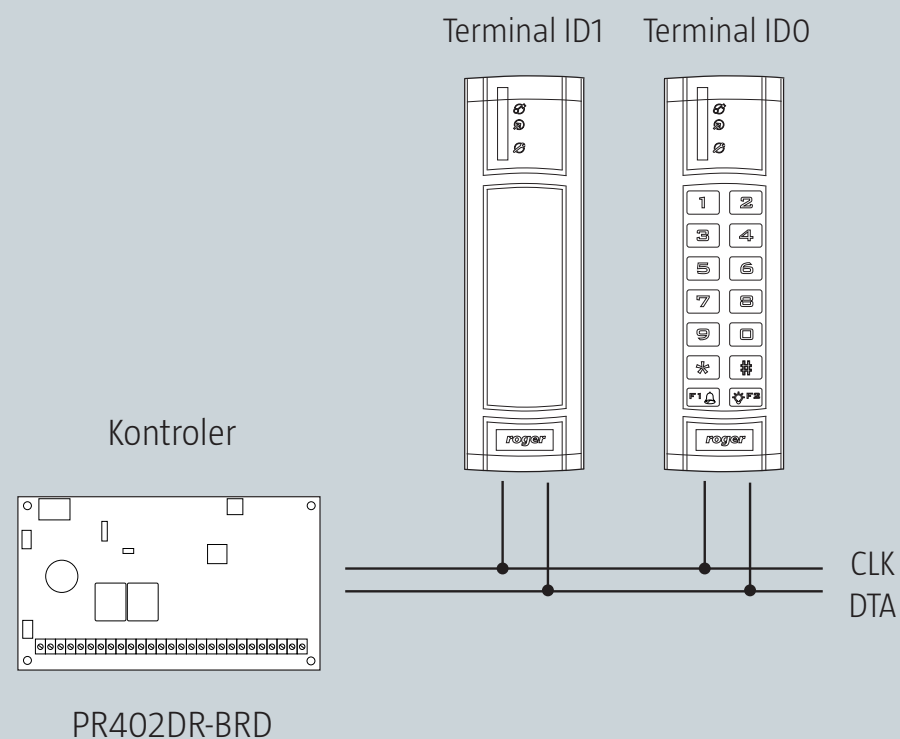
Ogólna koncepcja kontrolera dostępu

- Podział na jednostkę logiczną (kontroler) oraz terminale (czytniki) ID0 i ID1
- Kontroler wymagający podłączenia czytników zewnętrznych (np. PR402DR)
- Kontroler zintegrowany to urządzenie, w którym jednostkę logiczną (kontroler) scalono z terminalem ID1 (np. PR602LCD-DT)

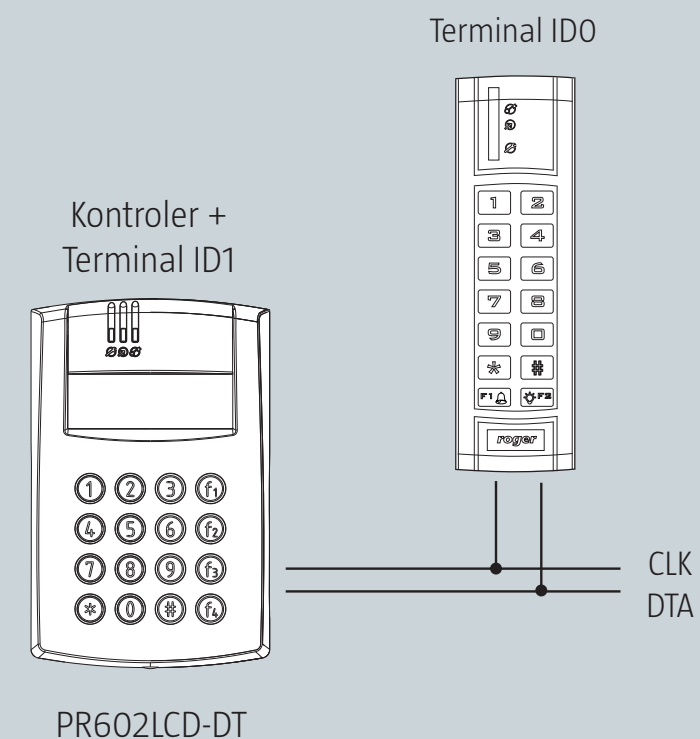


Ogólna koncepcja kontrolera dostępu

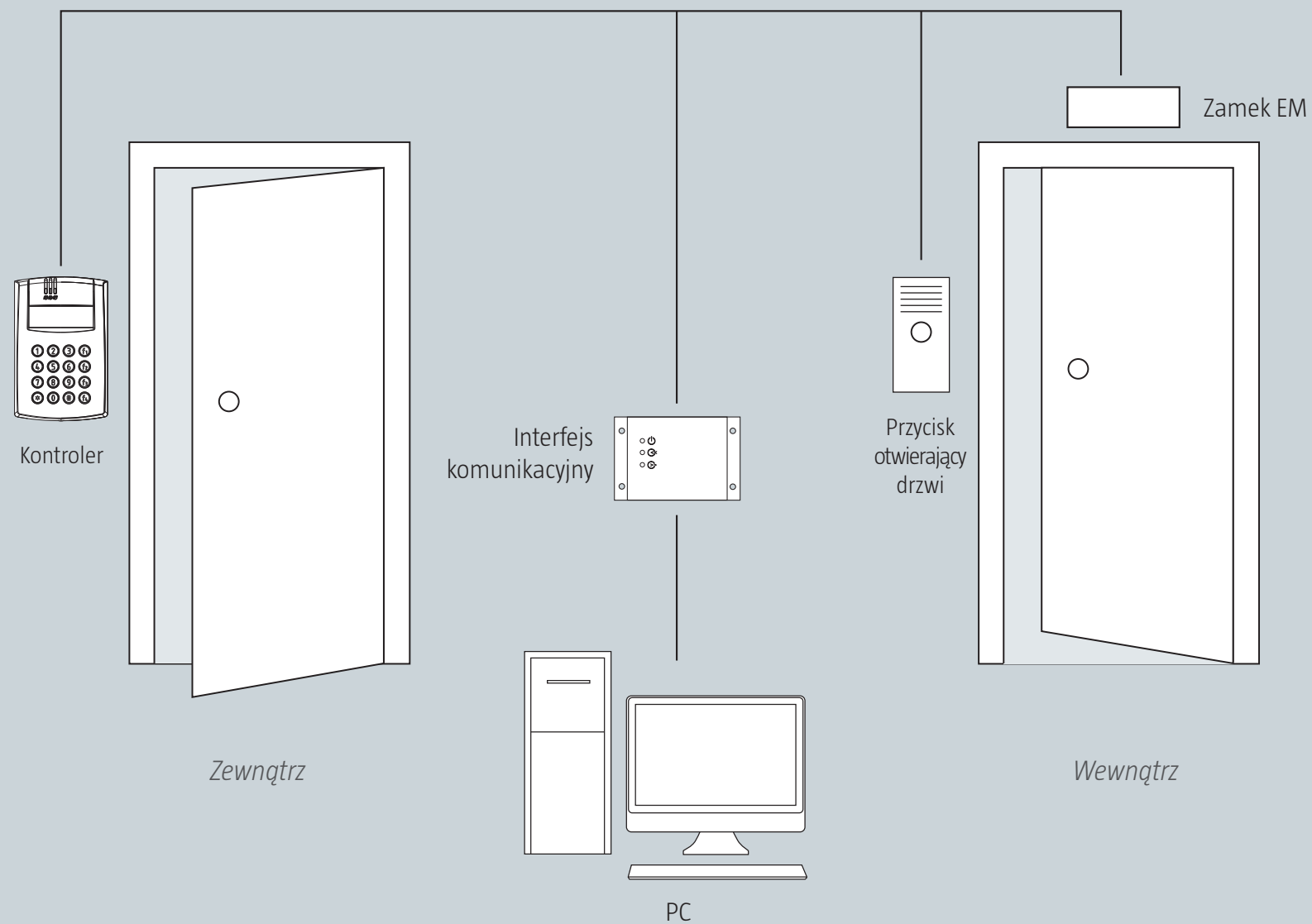
Kontroler bez wbudowanego
czytnika



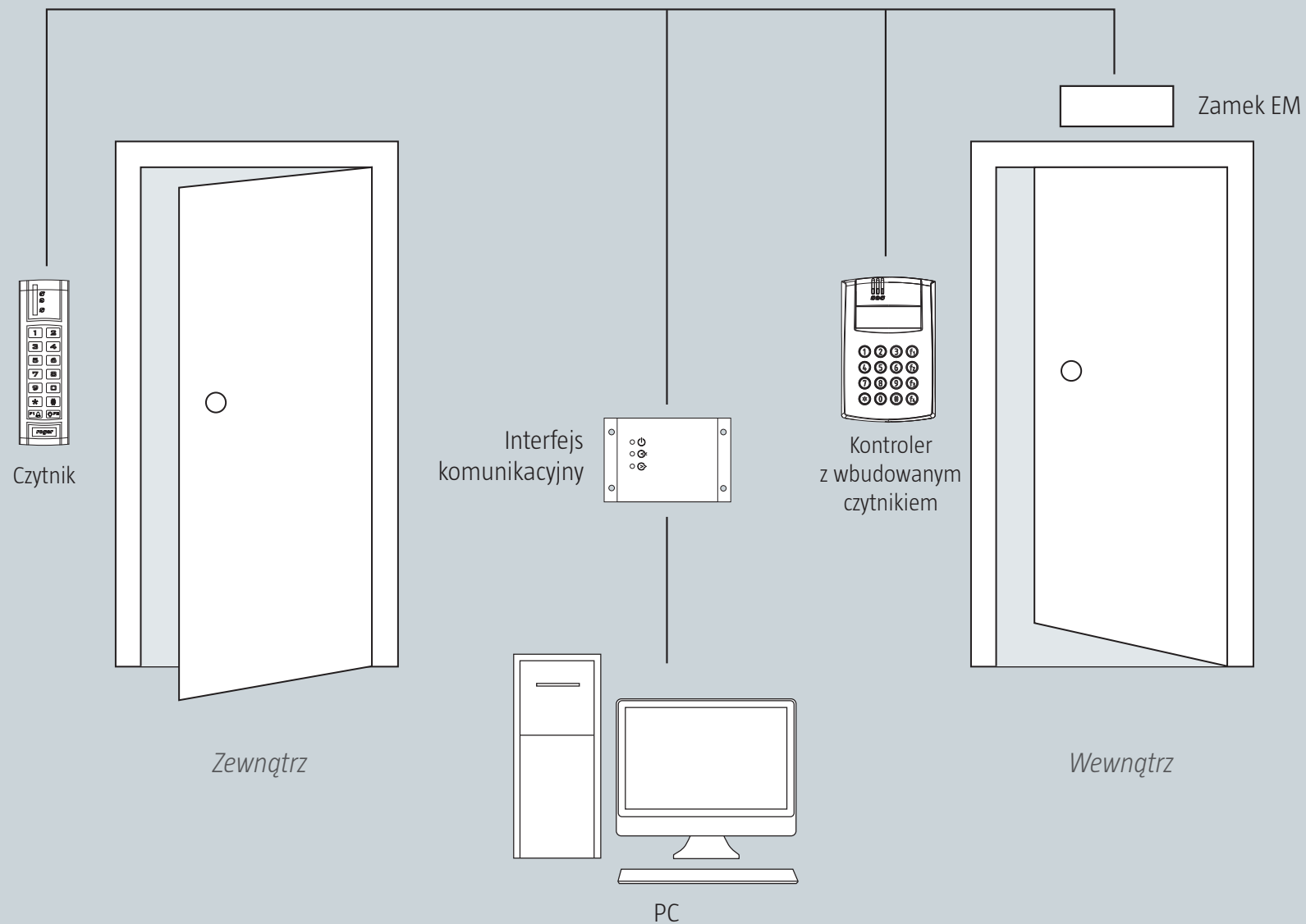
Kontroler zintegrowany
z czytnikiem



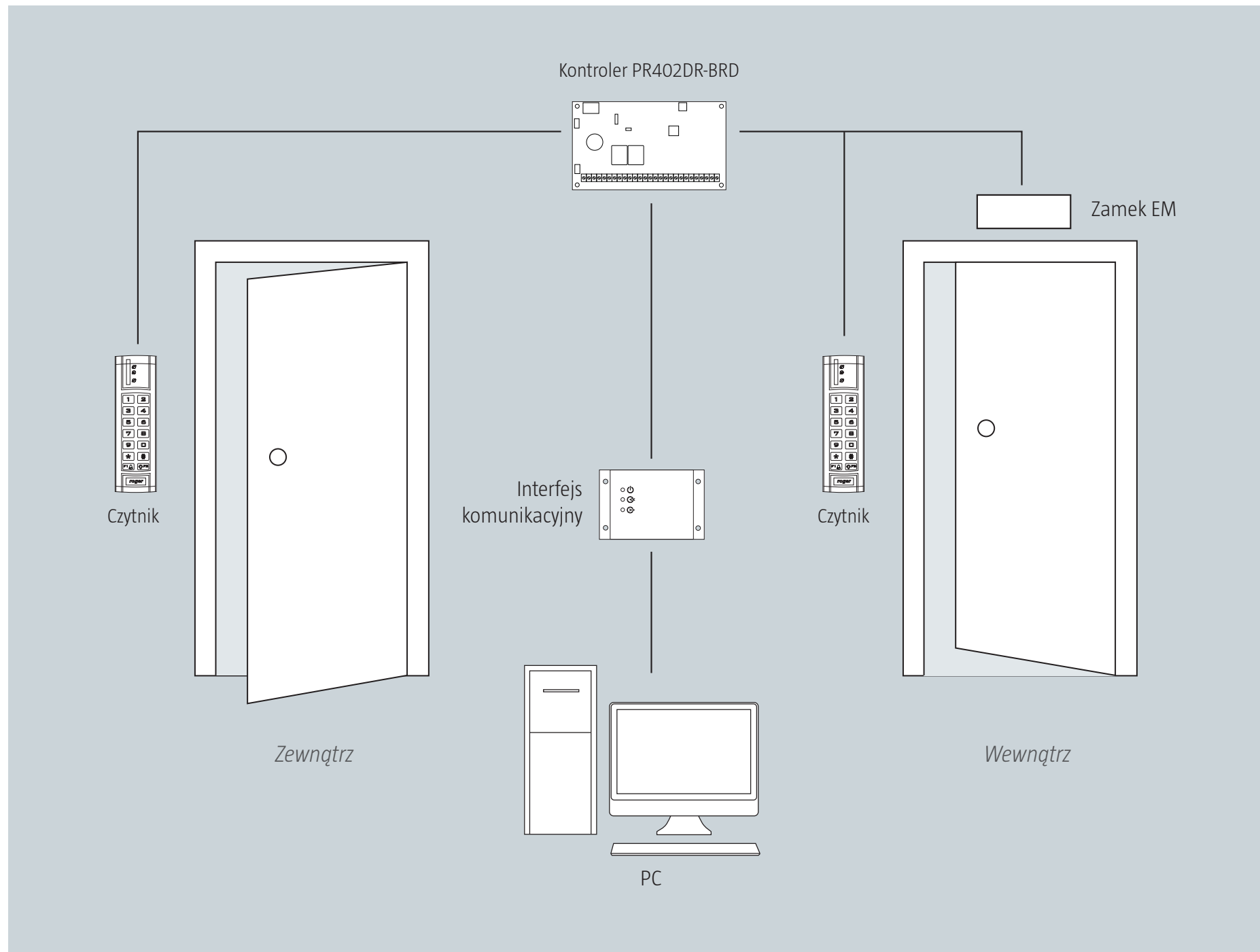
Przejście jednostronne na bazie PR602LCD-DT



Przejście dwustronne na bazie PR602LCD-DT



Przejście dwustronne na bazie PR402DR

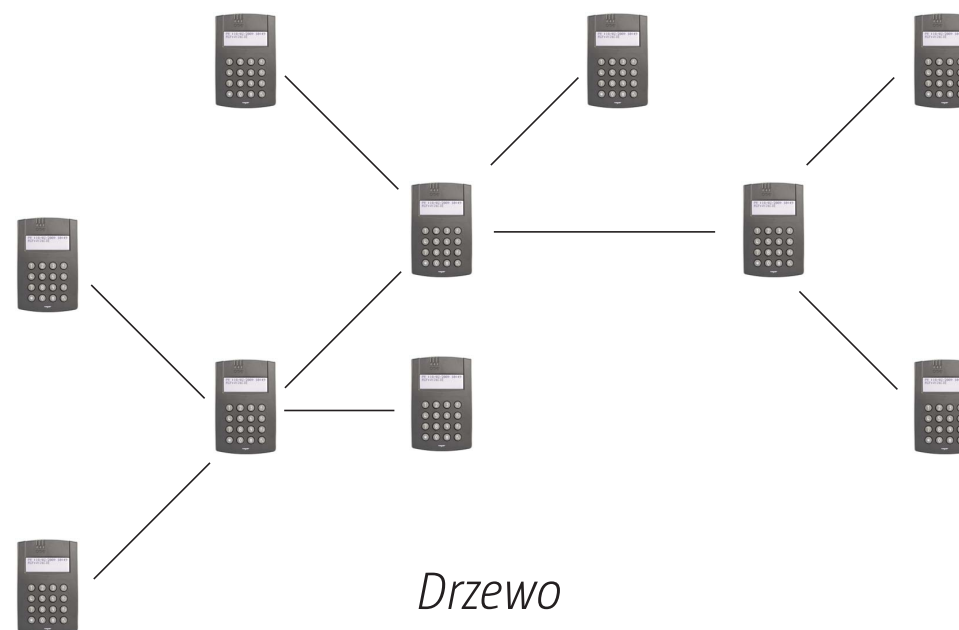


Magistrala komunikacyjna zewnętrzna RS485

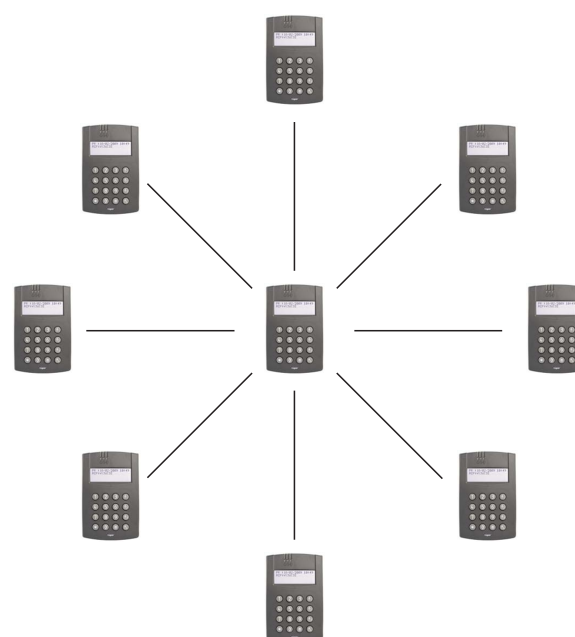
- Każdy kontroler podłączony do magistrali musi posiadać swój niepowtarzalny adres (ID=00-99)
- Adres można nadawać manualnie lub z poziomu oprogramowania
- Do jednej magistrali można dołączyć maksymalnie 32 kontrolery
- Magistralę można wykonać z dowolnego typu kabli sygnałowych niemniej zaleca się stosować skrętkę komputerową bez ekranu
- Kable w ekranie stosować tylko w warunkach silnych zakłócających pól elektromagnetycznych
- Struktura magistrali może być dowolną kombinacją topologii drzewa i gwiazdy
- Wszystkie urządzenia podłączone do tej samej magistrali muszą mieć ten sam potencjał minusa napięcia stałego



Topologie magistrali komunikacyjnej w systemie RACS 4



Drzewo



Gwiazda



*Konfiguracja
zabroniona*

Pętla



Magistrala komunikacyjna wewnętrzna RACS Clock&Data

- Dwie linie komunikacyjne CLK i DTA
- Dowolny typ kabli sygnałowych
- Przeznaczona do komunikacji z zewnętrznymi czytnikami oraz modułami rozszerzeń
- Niepowtarzalny adres (ID=0-15) urządzeń podłączonych do linii CLK i DTA
- Możliwość podłączenia czytników z interfejsem Magstripe lub Wiegand
- Maksymalna gwarantowana odległość pomiędzy kontrolerem a dowolnym urządzeniem podłączonym do magistrali 150m
- Praktyczna długość magistrali do 500m
- Wspólny minus zasilania wszystkich urządzeń podłączonych do magistrali



Urządzenia dołączane do magistrali RACS Clock&Data

- Podstawowy czytnik dostępu (terminal ID0) po stronie wejścia
- Podstawowy czytnik dostępu (terminal ID1) po stronie wyjścia
- Dodatkowy czytnik po stronie wejścia (Tryb Podwójna Identyfikacja - High Security)
- Dodatkowy czytnik po stronie wyjścia (Tryb Podwójna Identyfikacja - High Security)
- Ekspander we/wy XM-2DR (separacja linii we/wy)
- Ekspander we/wy XM-8DR (kontrola dostępu w windzie)

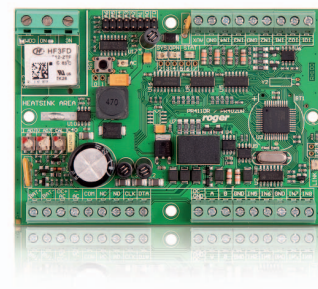
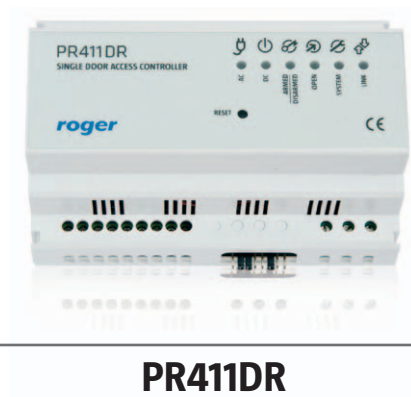


Standardowe kontrolery dostępu serii PRxx1

- Obustronna kontrola jednego przejścia
- Praca autonomiczna lub w systemie sieciowym
- 1000 użytkowników
- Programowanie manualne lub z poziomu komputera (PR Master)
- 250 grup dostępu
- 99 harmonogramów czasowych *
- Rejestracja zdarzeń *
- Szybkie konfigurowanie (ok. 15s)
- Szybka edycja właściwości użytkowników (ok. 5s)

() - funkcje dostępne tylko w systemie sieciowym z centralą serii CPR*

Kontrolery serii PRxx1



PR311SE



PR611



PR611-VP



PR621





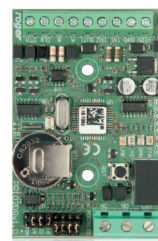
Kontrolery dostępu serii PRxx2

- Obustronna kontrola jednego przejścia
- Praca autonomiczna lub w systemie sieciowym
- 4000 użytkowników
- 250 grup dostępu
- 99 harmonogramów czasowych
- Bufor 32 000 zdarzeń
- Lokalny Anti-passback
- Globalny Anti-passback (wymaga centrali serii CPR)
- Kontrola dostępu w windach
- Szeroki zestaw funkcji zaawansowanych
- Szybka edycja właściwości użytkownika (ok. 5s)
- Pełne programowanie kontrolera wymaga ok. 1 minuty

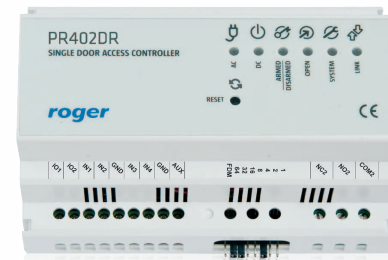
Kontrolery dostępu serii PRxx2



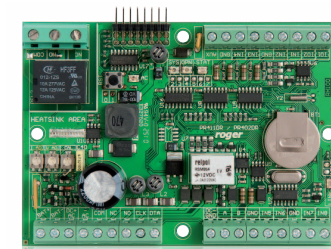
PR102DR



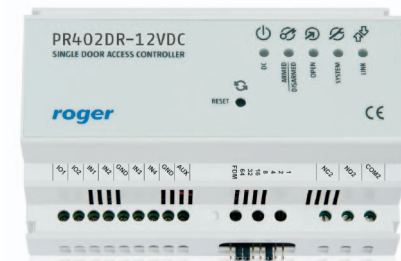
PR102DR-BRD



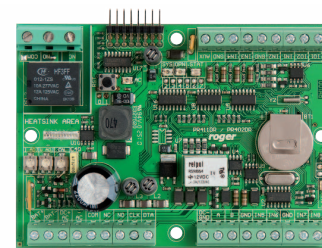
PR402DR



PR402DR-BRD



PR402DR-12VDC



PR402DR-BRD-12VDC

Kontrolery dostępu serii PRxx2



PR612



PR622



PR312EM/PR312MF



PR602LCD-DT-I

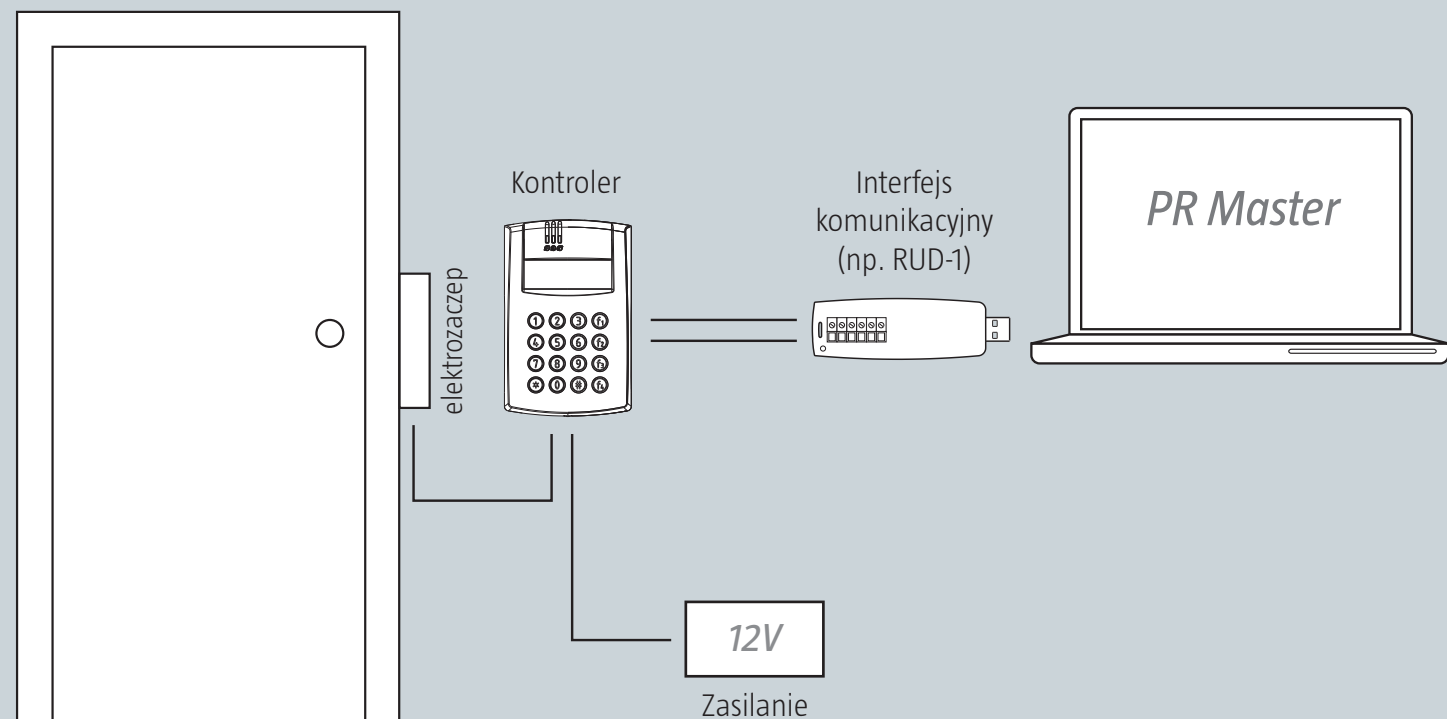


PR602LCD-DT-O



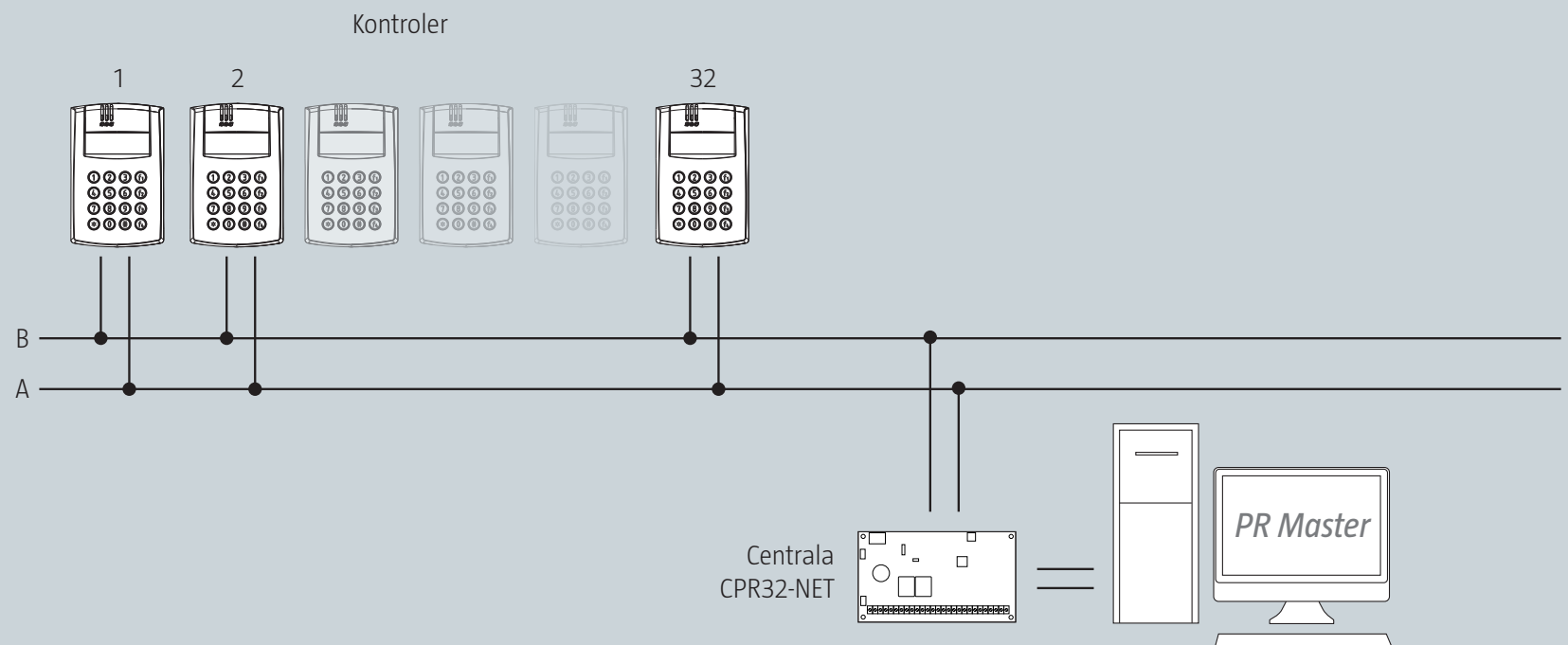
System autonomiczny

- Kontroler działa jako całkowicie niezależne urządzenie
- W systemie brak centrali serii CPR
- Podłączenie kontrolera do komputera wymagane jest wyłącznie na czas programowania i ściągania zdarzeń



System sieciowy

- Kontrolery połączone są ze sobą za pomocą magistrali komunikacyjnej i wymieniają dane z urządzeniem nadrzędnym (centrala serii CPR)
- Podłączenie do komputera wymagane w celu konfiguracji i ściągania zdarzeń



Zestawy kontroli dostępu

Zestaw zawiera:

- Kontroler dostępu: PR402DR lub PR411DR
- Zasilacz transformatorowy PS-10ACDR
- Obudowę metalową z wizjerem, łącznikiem antysabotażowym i szyną DIN 35mm

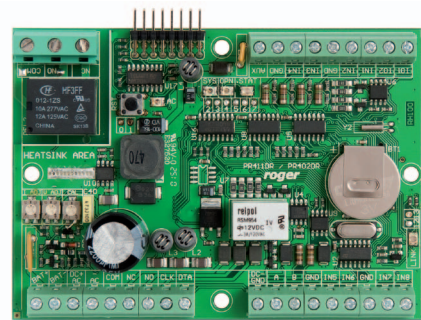


Akumulator widoczny na zdjęciu nie wchodzi w skład zestawu.

PR402DR-SET/PR411DR-SET

Centrala CPR32-SE

- Zbieranie i magazynowanie zdarzeń (bufor 250.000 zdarzeń)
- Synchronizacja zegarów urządzeń funkcjonujących w systemie
- Realizuje funkcje o charakterze globalnym (Strefy Alarmowe, Globalny Antipassback)
- Sterowanie harmonogramami czasowymi w kontrolerach serii PRxx1
- Obsługa akumulatora z kontrolą prądu ładowania oraz monitorowaniem jego stanu



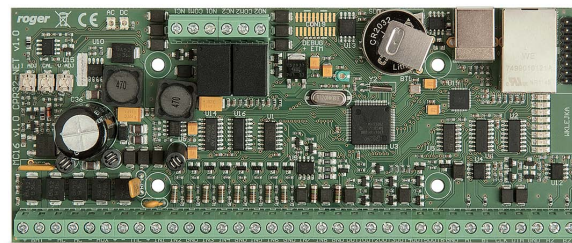
Centrala CPR32-SE



**Moduł centrali z zasilaczem i akumulatorem,
umieszczony w metalowej obudowie**

Centrala CPR32-NET

- Zapewnienie tych samych funkcjonalności co centrala CPR32-SE
- Wbudowany interfejs komunikacyjny Ethernet-RS485
- Obsługa serwerów czasu NTP
- Opcjonalny bufor zdarzeń na dodatkowej karcie pamięci (33 mln zdarzeń)
- Szyfrowany protokół komunikacyjny AES128 CBC
- Integracja programowa na poziomie stref alarmowych z centralami alarmowymi serii Integra (SATEL) w oparciu o płatną licencję do programu PR Master
- Integracja z systemem bezprzewodowych zamków Aperio (Assa Abloy) w oparciu o płatną licencję do programu PR Master
- Zwiększona ilość wejść NO/NC oraz wyjść tranzystorowych w stosunku do CPR32-SE



CPR32-NET



**Moduł centrali z zasilaczem i akumulatorem,
umieszczony w metalowej obudowie**

Interfejsy komunikacyjne



RCI-2
Interfejs USB - RS485



UT-2USB
Interfejs USB - RS485



UT-4
Interfejs RS232/RS485/
RS422 - Ethernet



UT-4DR
Interfejs RS485 - Ethernet

Interfejs komunikacyjny RUD-1

Charakterystyka:

- Przenośny konwerter USB – RS485
- Komunikacja z systemem RACS 4
- Konfiguracja i obsługa kontrolerów dostępu serii PR z poziomu programu PR Master
- Konfiguracja i obsługa czytników serii PRTxxEM i PRTxxMF z poziomu programu RARC
- Aktualizacja oprogramowania firmowego kontrolerów serii PR oraz czytników serii PRTxxEM i PRTxxMF
- Zasilanie programowanego urządzenia z portu USB komputera



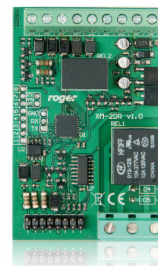
RUD-1

Ekspandery

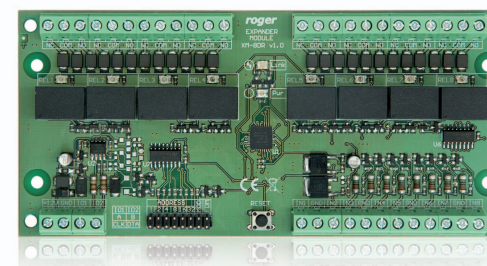
- XM-2DR - ekspander we/wy: 2 wejścia NO/NC, 2 wyjścia przekaźnikowe
- XM-8DR-BRD - ekspander we/wy: 8 wejść NO/NC, 8 wyjść przekaźnikowych, kontrola dostępu w windzie



XM-2DR



XM-2DR-BRD



XM-8DR-BRD

Akcesoria

- ME-1 - obudowa metalowa z transformatorem 40VA, kontaktem antysabotażowym oraz szyną DIN 35 mm
- ME-2-D - obudowa metalowa z zainstalowanymi 3 szynami montażowymi DIN 35mm w zestawie z dozorowanym zasilaczem buforowym 3.5A/13.8VDC oraz dystrybutorem zasilania, kontakt antysabotażowy, miejsce na akumulator 17Ah
- ME-5-S - obudowa metalowa z czterema szynami DIN 35mm i kontaktem antysabotażowym z zasilaczem 11A/13.8VDC oraz dystrybutorem napięcia (zasilacz jest dodany do opakowania celem samodzielnej instalacji w obudowie ME-5)



ME-1



ME-2-D



ME-5-S

Moduły i akumulator nie wchodzą w skład ME-1, ME-2-D.

Kontrolery i akumulator nie wchodzą w skład ME-5-S.

Akcesoria



AX-1
Metalowa
podkładka



AX-9
Karta pamięci



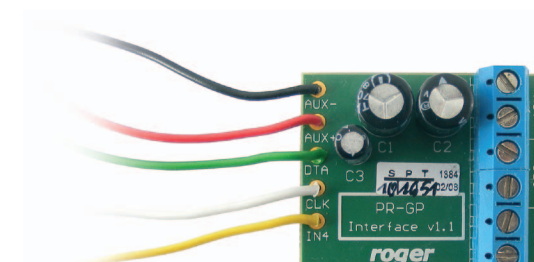
AX-12
Ochronnik
magistrali RS485



ASCD-1
Zegar z wyświetlaczem
matrycowym LED



ML-1
Zamek
mechaniczny



PR-GP-BRD
Moduł
dopasowujący

Sygnalizatory

- Zasilanie 12V DC
- Sygnalizacja akustyczna 110dB/1m
- Sygnalizacja optyczna LED/2Hz
- Możliwość montażu akumulatora 1,2Ah
- Układ czasowy ograniczający czas sygnalizacji



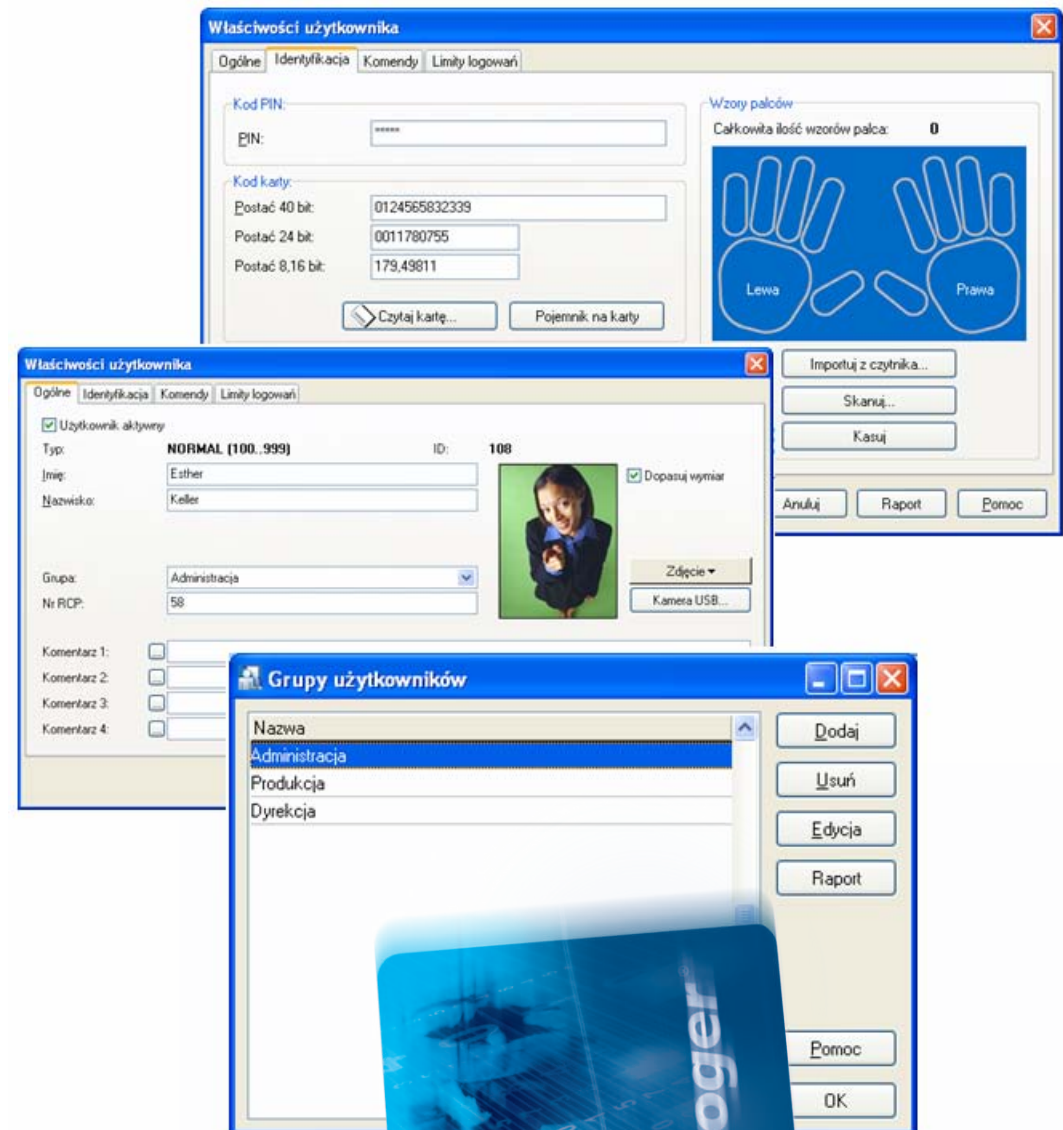
ASP110LC



ASP110S v2.0

Podstawowe pojęcia kontroli dostępu

- Użytkownicy
- Grupy Dostępu
- Strefy Dostępu
- Harmonogramy Czasowe
- Tryby Identyfikacji
- Tryby Drzwi



Typy użytkowników

Typy użytkowników

<i>Nazwa</i>	<i>Numer ID</i>	<i>Opis</i>
MASTER	ID=000	Uprawnienie do otwierania drzwi oraz przezbrajania. Zdefiniowanie użytkownika MASTER umożliwia wstępne przetestowanie kontrolera.
SWITCHER Full	ID=001-049	Uprawnienie do otwierania drzwi oraz do przezbrajania kontrolera. Przebrojenie kontrolera wymaga dwukrotnego użycia identyfikatora SWITCHER natomiast przyznanie dostępu następuje z chwilą pierwszego użycia tego identyfikatora
SWITCHER Limited	ID=050-99	Uprawnienie tylko do przezbrajania kontrolera, przebrojenie następuje w następstwie jednokrotnego użycia identyfikatora
NORMAL	ID=100-3999	Uprawnienie tylko do otwierania drzwi. Użytkownicy typu NORMAL o numerze ID większym niż 1000 mogą posiadać dodatkowo atrybut Local SWITCHER, który uprawnia ich również do przezbrajania kontrolera



Grupy Dostępu

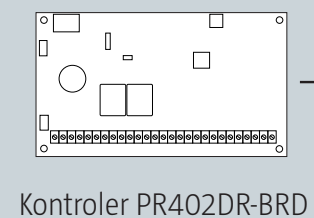
- Użytkownicy kontrolera mogą posiadać status Bez Grupy, Grupy bez Dostępu lub przynależeć do jednej ze zdefiniowanych przez administratora w systemie Grup Dostępu
- Przynależność do danej Grupy Dostępu determinuje prawa dostępu użytkownika w ramach danego systemu KD
- Wszyscy użytkownicy należący do tej samej Grupy Dostępu mają te same uprawnienia dostępu
- W szczególnym przypadku Grupa Dostępu może się składać tylko z jednego użytkownika
- Członkowie Grupy Dostępu uzyskują dostęp do określonych obszarów zwanych Strefami Dostępu zgodnie z indywidualnie zdefiniowanymi Harmonogramami Czasowymi
- Użytkownicy posiadający status Bez Grupy posiadają dostęp do wszystkich Stref Dostępu bez żadnych ograniczeń czasowych (nie obowiązują ich Harmonogramy Czasowe)
- Domyślnie, każdy nowo dodany użytkownik systemu RACS 4 ma status Bez Grupy



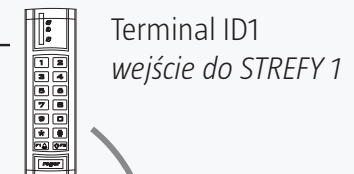
Strefy Dostępu

- Strefa Dostępu to grupa punktów identyfikacji (czytników) które kontrolują wejście do pewnego obszaru w ramach systemu Kontroli Dostępu
- Pojęcie Strefy Dostępu ma na celu uproszczenie sposobu definiowania praw dostępu
- Definiowanie praw dostępu przeprowadza się nie dla pojedynczego punktu identyfikacji (pojedynczych drzwi) lecz dla grupy urządzeń, które tworzą Strefę Dostępu
- W szczególnym przypadku każdy punkt identyfikacji (każde pomieszczenie) może stanowić osobną Strefę Dostępu

Przykład organizacji kontroli dostępu



STREFA 2



STREFA 1

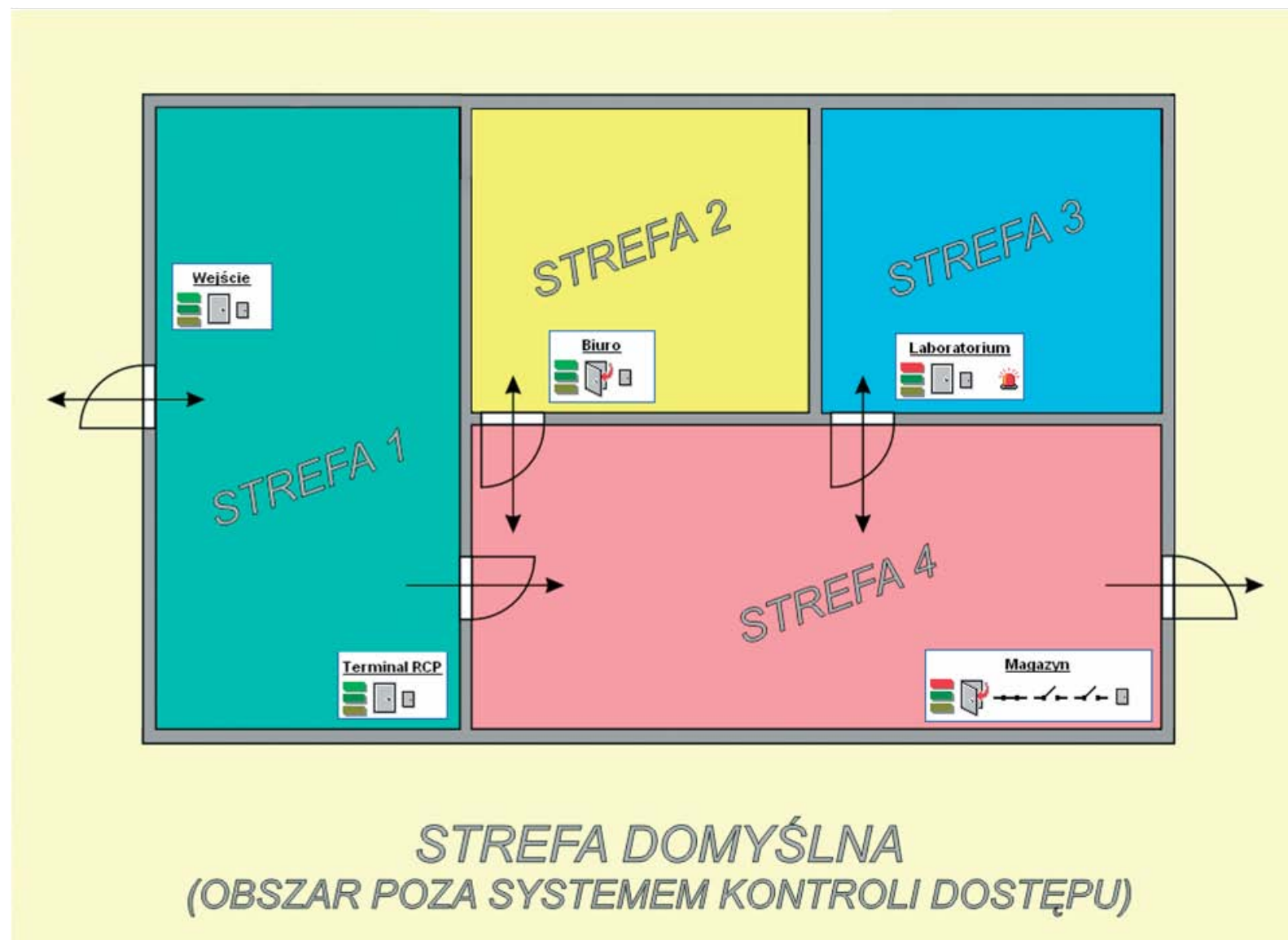
Terminal ID0
wejście do STREFY 2

**STREFA
PUBLIC**

Terminal ID0
wejście do STREFY 1

Kontroler
z wbudowany
Terminalem ID1
wejście do STREFY
PUBLIC

Strefy Dostępu





Harmonogramy Czasowe

- Harmonogramy Czasowe to kalendarze obejmujące swoim zakresem 7 dni tygodnia (Pon. - Niedz.) plus 4 dni świąteczne (H1-H4)
- Ustawienia świąteczne to dni, w których przestają obowiązywać zwykłe ustawienia harmonogramów czasowych zdefiniowanych w ramach dni tygodnia, a w miejsce nich kontroler stosuje pewne reguły zastępcze
- Każdy harmonogram może posiadać do 128 przedziałów czasowych od ... do ... zdefiniowanych z dokładnością do 1 minuty
- W systemie RACS 4 rozróżnia się następujące typy harmonogramów czasowych:
 - Harmonogramy Ogólnego Przeznaczenia
 - Harmonogramy Trybu RCP
 - Harmonogramy Trybu Drzwi
 - Harmonogramy Zerowania APB
 - Harmonogramy Trybu Identyfikacji

Tryby Identyfikacji

to metoda jaką kontroler stosuje w celu identyfikacji użytkownika

Tryby Identyfikacji

<i>Nazwa trybu</i>	<i>Opis</i>
Karta lub PIN	Kontroler wymaga odczytu karty lub podania kodu PIN
Karta i PIN	Kontroler wymaga odczytu karty i podania kodu PIN, kolejność nie gra roli
Tylko karta	Kontroler wymaga tylko karty nie akceptuje kodów PIN
Tylko PIN	Kontroler wymaga tylko kodu PIN nie akceptuje karty



Tryby Drzwi

to sposób sterowania elementem wykonawczym odpowiedzialnym za blokowanie/odblokowywanie drzwi

Tryby Drzwi

<i>Nazwa trybu</i>	<i>Opis</i>
Normalny	Normalnie drzwi są zablokowane, zwolnienie drzwi następuje tylko na czas przyznania dostępu
Odblokowane	Drzwi są odblokowane na stałe, wejście może się odbywać bez użycia identyfikatorów
Warunkowo Odblokowane	Początkowo drzwi są w trybie Normalnym, z chwilą przyznania dostępu pierwszej osobie drzwi przechodzą do trybu Odblokowane
Zablokowane	Drzwi są permanentnie zablokowane niezależnie od tego czy użytkownik który próbuje wejść jest uprawniony do wejścia czy nie

A vertical strip on the left side of the slide shows a blurred image of people walking, likely in a transit or public area, with a blue geometric pattern overlaid.

Funkcje specjalne

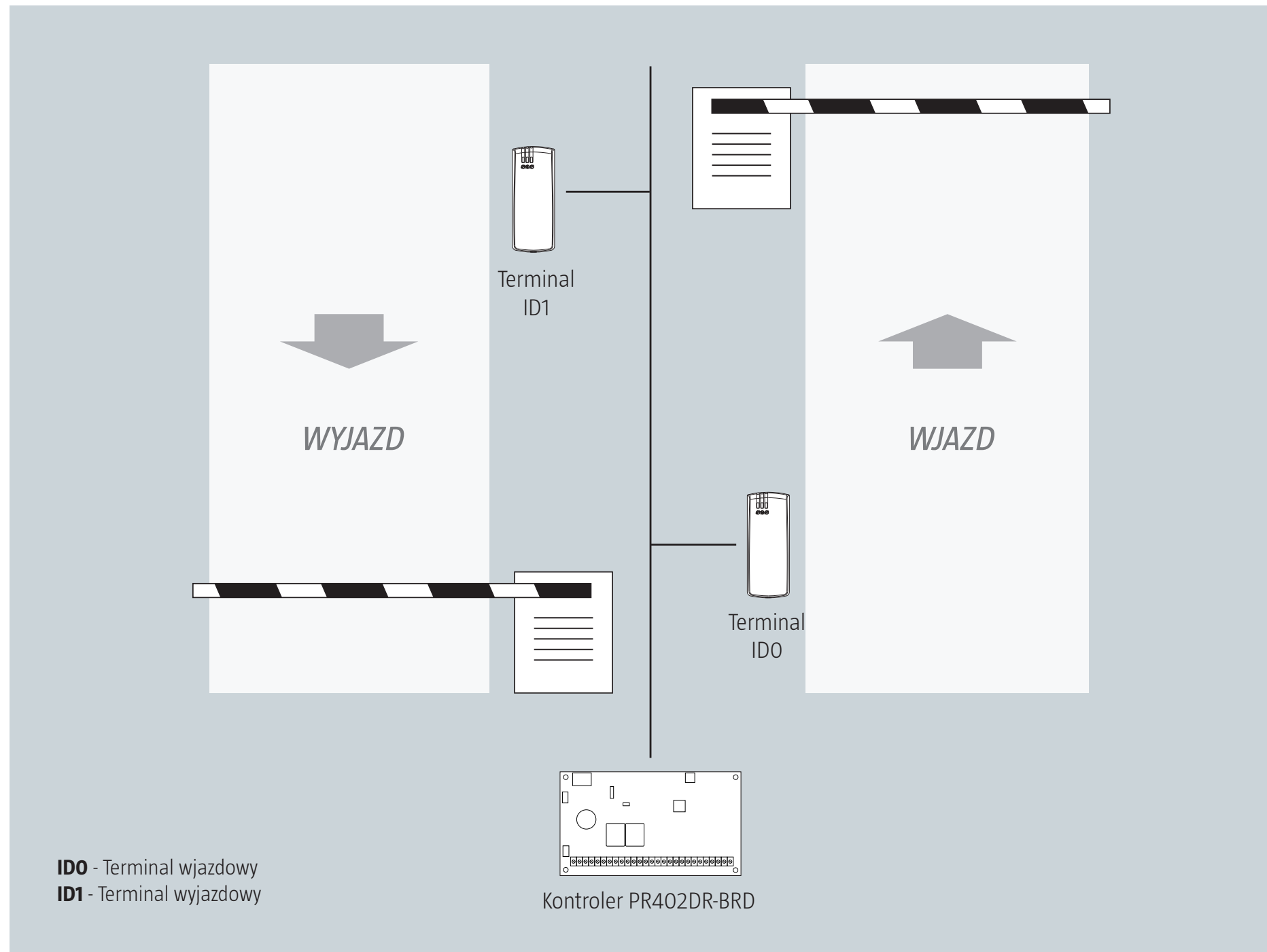
- Anti-passback Lokalny
- Anti-passback Globalny
- Limit osób w pomieszczeniu
- Limit użytkowników w Strefie APB
- Limit logowań
- Wejście Warunkowe
- Wejście Komisyjne
- Tryb High Security
- Kod Obiektu (Facility Code)
- Klawisze funkcyjne
- Warunek dodatkowy



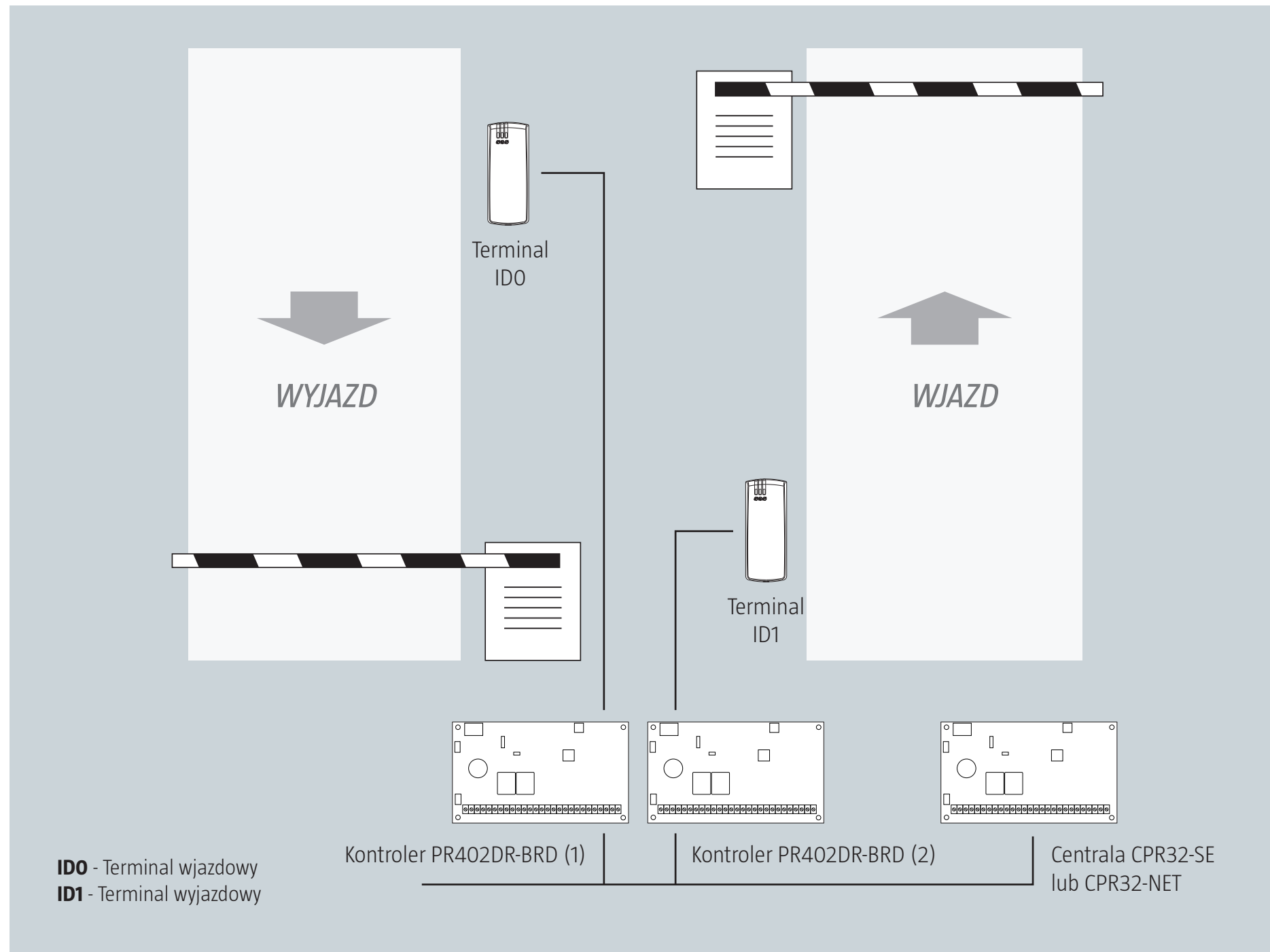
Pojęcie funkcji Anti-passback (APB)

- Funkcja Anti-passback obliguje użytkownika do logowania się naprzemiennie raz na wejściu raz na wyjściu z pomieszczenia lub strefy
- Ze względu na to czy funkcja APB odnosi się do pojedynczego przejścia czy też obszaru złożonego z wielu przejść rozróżnia się:
 - APB Lokalny
 - APB Globalny
- Ze względu na sposób reakcji kontrolera na naruszanie zasad APB rozróżnia się:
 - APB Twardy
 - APB Miękki
- Wyróżnia się również tzw. True APB wymagający zastosowania czujnika otwarcia drzwi do dodatkowego monitorowania faktycznej lokalizacji użytkownika w ramach APB
- Istnieje możliwość skonfigurowania przejścia wewnętrznego w strefie APB
- Funkcja APB umożliwia kontrolę ilości osób przebywających w pomieszczeniu (APB Lokalny) i Strefie APB (APB Globalny)

APB Lokalny – przykład zastosowania



APB Globalny – przykład zastosowania





Limity logowań

- Dostęp do pomieszczenia może być udzielany danemu użytkownikowi określoną ilość razy aż do wyczerpania limitu logowań
- Ze względu na sposób obsługi wyróżniamy:
 - nieodnawialny limit logowań
 - odnawialny limit logowań
- Odnawialny limit logowań jest definiowany dla określonych powtarzalnych przedziałów czasowych w okresie dobowym



Wejście Warunkowe

- Prawo wejścia do pomieszczenia posiadają nie tylko osoby uprawnione ale również wszystkie inne pod warunkiem, że jest już ktoś w pomieszczeniu
- Wymaga załączenia funkcji Anti-passbacku Lokalnego
- Sterowanie za pośrednictwem harmonogramu czasowego
- Może podlegać warunkowi dodatkowemu

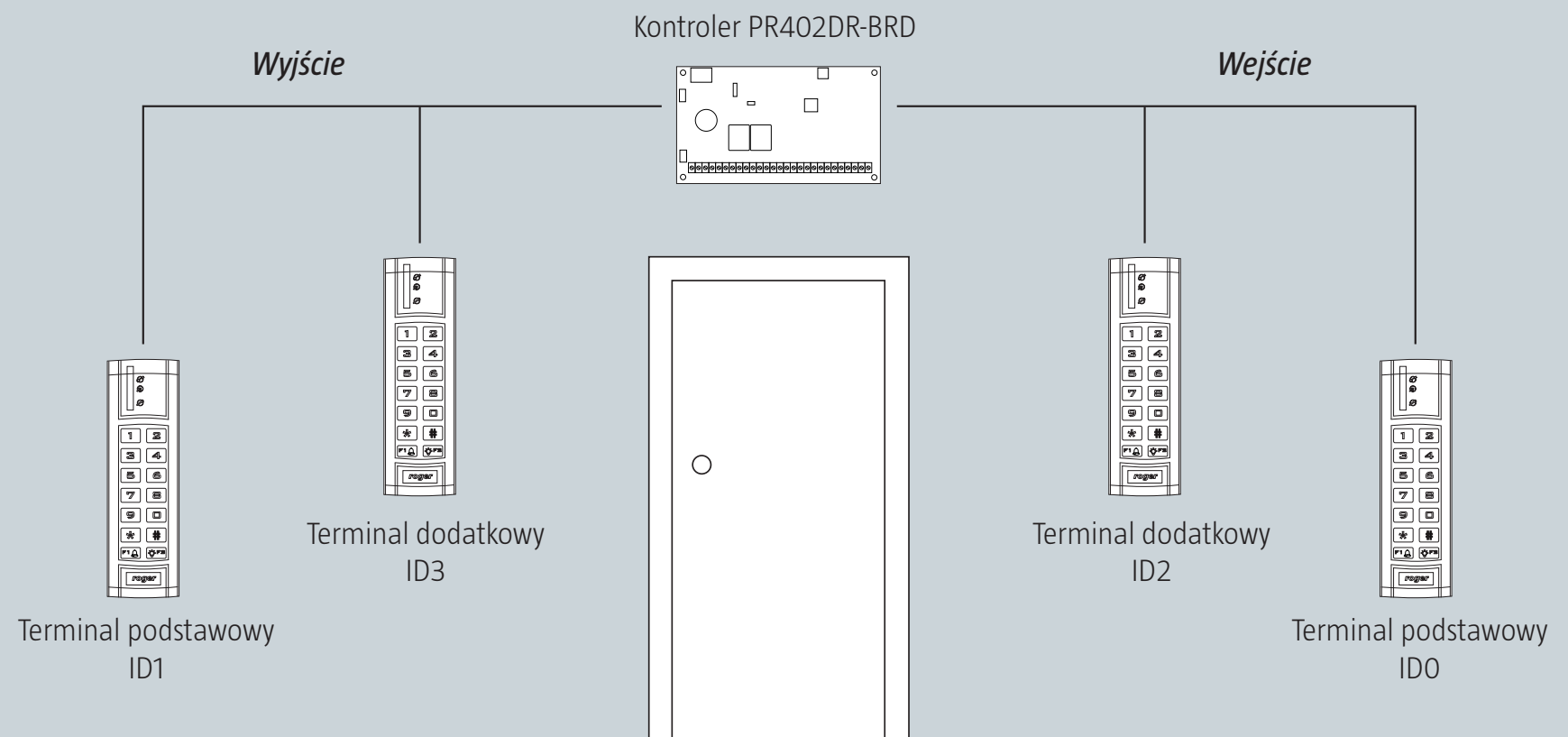
A blurred, vertical image on the left side of the slide showing a group of people walking, possibly in a public space or transit. The image is out of focus, with colors like blue, black, and white visible.

Wejście Komisyjne

- Dostęp do pomieszczenia może być przyznany dopiero wtedy, gdy dwóch użytkowników, jeden po drugim dokona poprawnej identyfikacji
- Drugi użytkownik może zalogować się po tej samej stronie przejścia co użytkownik pierwszy lub po stronie drugiej
- Załączenie trybu Wejścia Komisijnego odnosi się do obydwu stron przejścia, nie można załączyć tego trybu indywidualnie dla każdej ze stron
- Działanie trybu Wejście Komisyjne może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu

Tryb High Security (dwuetapowa identyfikacja)

- W pierwszym kroku użytkownik musi dokonać identyfikacji na terminalu podstawowym a następnie (w drugim kroku) na terminalu dodatkowym zainstalowanym po tej samej stronie przejścia co czytnik podstawowy
- Tryb High Security definiuje się dla każdej strony przejścia osobno
- Działanie trybu High Security może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu





Kod Obiektu (Facility Code)

- Kod Obiektu to część kodu karty która wskazuje na przynależność danej karty do pewnej (wybranej) grupy kart
- Karty posiadające ten sam Kod Obiektu mają identyczny fragment kodu na pozycjach od 16 do 24 bitu
- Załączenie opcji Kod Obiektu powoduje, że kontroler przyznaje dostęp wszystkim kartom które mają ten sam Kod Obiektu
- Działanie funkcji Kod Obiektu może podlegać harmonogramowi czasowemu oraz warunkowi dodatkowemu
- Kod Obiektu znajduje praktyczne zastosowanie w obsłudze dostępu do parkingów, akademików itd. czyli tam gdzie chcemy udostępnić dostęp konkretnej grupie bez potrzeby identyfikacji poszczególnych osób

Klawisze funkcyjne

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



Kontroler z czterema klawiszami funkcyjnymi PR602LCD-DT

Warunek dodatkowy

- Warunek dodatkowy wskazuje na dodatkową okoliczność lub stan który musi wystąpić aby dana funkcja/opcja dla której dany warunek jest przypisany mogła zostać zrealizowana
- Warunek dodatkowy można zdefiniować dla wielu funkcji i opcji kontrolera jak również dla linii wejściowych i wyjściowych

Wejście Warunkowe

Harmonogram:

Zawsze

Warunek dodatkowy:

[128]: Zezwól gdy kontroler jest rozbrojony

[128]: Zezwól gdy kontroler jest rozbrojony

[129]: Zezwól gdy kontroler jest uzbrojony

[130]: Zezwól gdy wejście IN1 jest wyzwolone

[131]: Blokuj gdy wejście IN1 jest wyzwolone

[132]: Zezwól gdy wejście IN2 jest wyzwolone

[133]: Blokuj gdy wejście IN2 jest wyzwolone

[134]: Zezwól gdy wejście IN3 jest wyzwolone

Lista warunków dodatkowych

A vertical strip on the left side of the slide shows a blurred image of people walking, likely in a public space, with a blue geometric pattern overlaid.

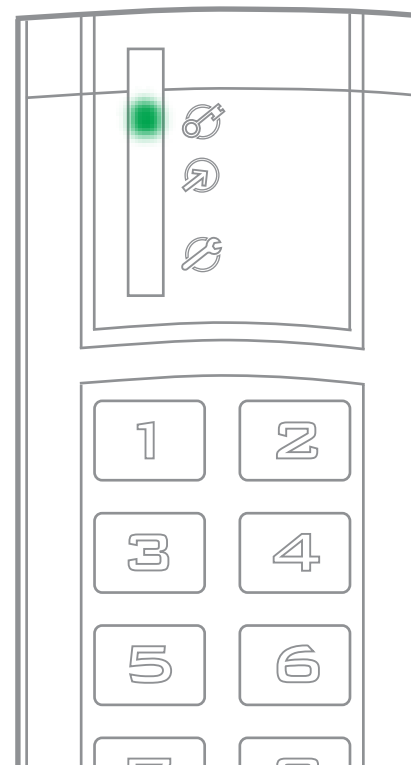
Linie alarmowe

- **Linie wejściowe**
 - Tamper
 - WŁAMANIE
- **Linie wyjściowe**
 - Tamper
 - WŁAMANIE
 - Drzwi Otwarte
 - Wejście Siłowe
 - Prealarm
 - Alarm Drzwi

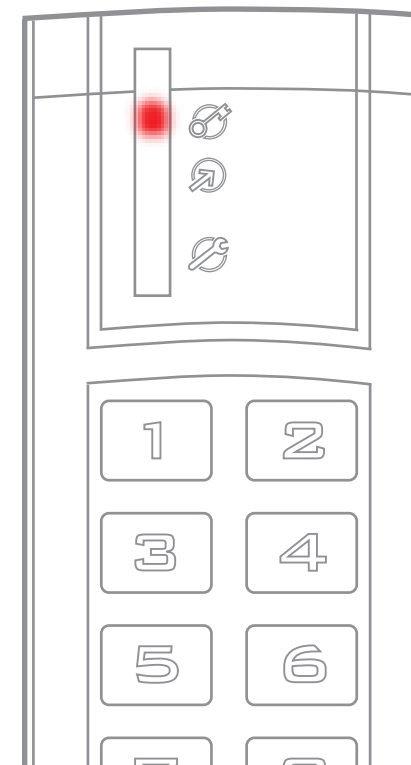
Koncepcja stanów Uzbrojony/Rozbrojony

- Tryby Uzbrojenia
 - Uzbrojony
 - Rozbrojony
- Sterowanie trybem uzbrojenia
 - Manualnie przy pomocy identyfikatorów
 - Automatycznie z poziomu harmonogramu czasowego
 - Z linii wejściowej
 - Z klawisza funkcyjnego
 - Poleceniem (komendą) z klawiatury
 - Zdalnie z poziomu centrali serii CPR
 - Zdalnie z komputera zarządzającego

Kontroler
rozbrojony



Kontroler
uzbrojony



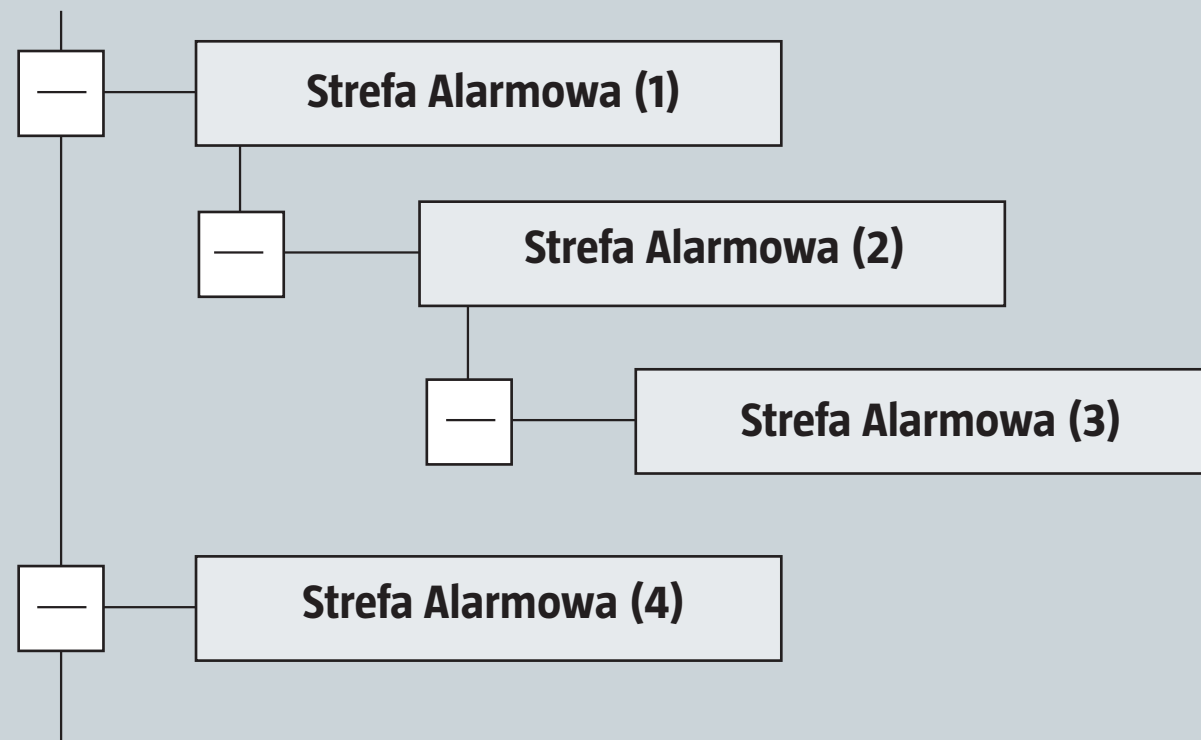


Reguły funkcjonowania i zastosowanie Trybów Uzbrojenia

- Rozbrojenie kontrolera w żadnym wypadku nie jest tożsame z anulowaniem kontroli dostępu na danym przejściu gdyż nadal dostęp jest udzielany jedynie użytkownikom z nadanymi prawami dostępu
- W przypadku ustawień domyślnych, w ramach bieżącego funkcjonowania systemu RACS 4 nie ma znaczenia czy kontroler jest uzbrojony czy rozbrojony
- Aktywowanie Trybów Uzbrojenia dla danego kontrolera skutkuje tym, że kontroler uzbrojony wymaga w pierwszej kolejności rozbrojenia by w następnym kroku uprawnieni użytkownicy mogli uzyskać dostęp
- Stan uzbrojenia może być sygnalizowany na wyjściach kontrolera, więc może służyć on do kontrolowania urządzeń zewnętrznych
- Tryby uzbrojenia mogą być wykorzystane do wprowadzenie dodatkowego poziomu zabezpieczeń poprzez nadawanie użytkownikom praw dostępu oraz praw do przezbierania
- Możliwość zastosowania Trybów Uzbrojenia w integracjach z systemami alarmowymi

Strefy Alarmowe

- Strefa Alarmowa to grupa kontrolerów współbieżnie zmieniających swój aktualny stan uzbrojenia
- Funkcja współbieżnego przezbierania dostępna jest tylko w systemach wyposażonych w centralę serii CPR
- Strefy Alarmowe mogą być niezależne od siebie lub tworzyć pewną zhierarchizowaną strukturę



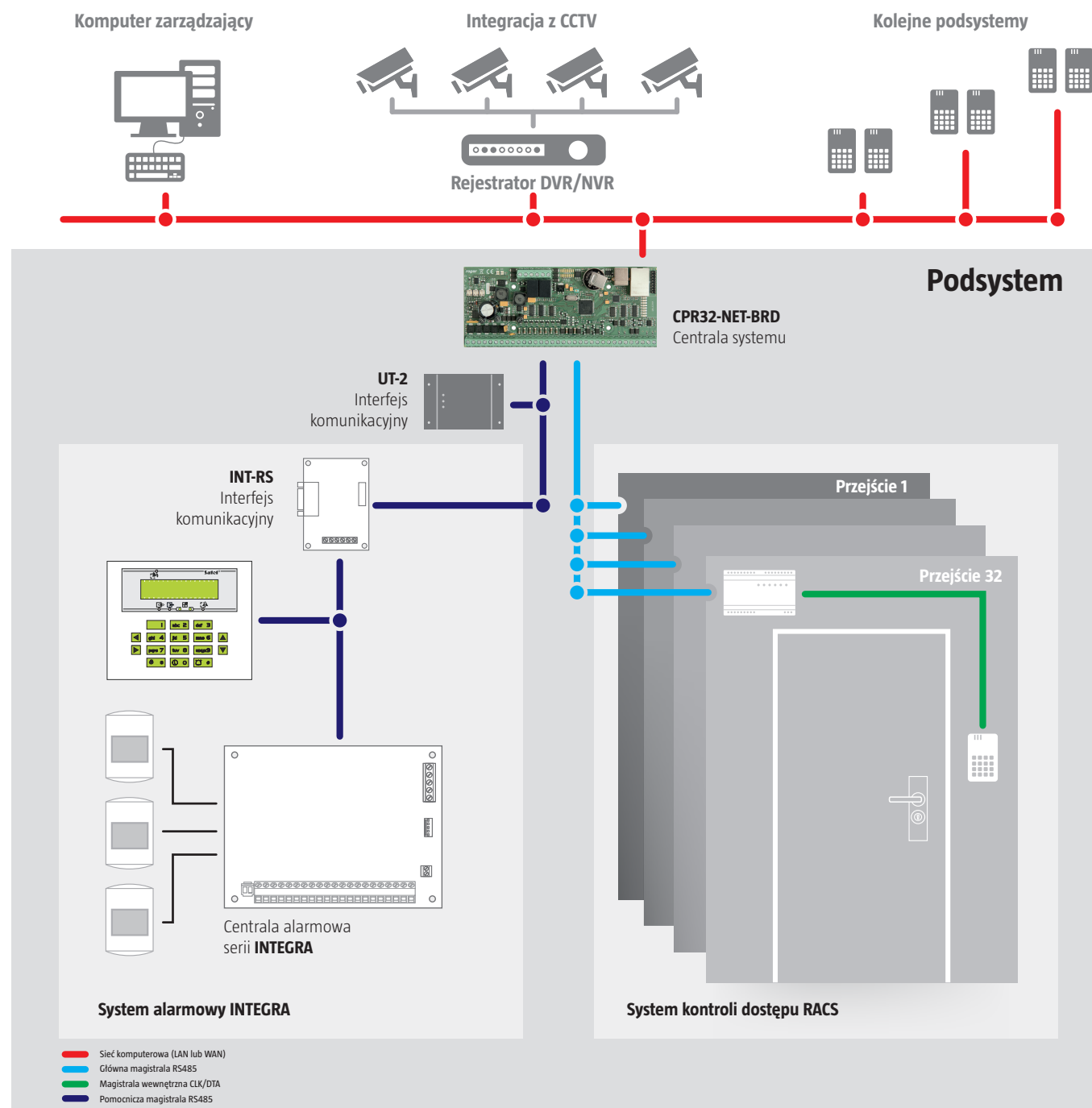
Przykład hierarchii stref alarmowych



Integracja systemu RACS 4 z systemami alarmowymi

- Ogólna integracja systemu RACS 4 z centralami alarmowymi różnych producentów polegająca na połączeniu wejść i wyjść kontrolerów z wejściami i wyjściami centrali alarmowej
- Programowa integracja systemu RACS 4 z **centralami alarmowymi serii INTEGRA (SATEL) na bazie centrali CPR32-NET** przy następujących założeniach:
 - ilość central serii INTEGRA w danej instalacji nie może być większa niż ilość central CPR32-NET
 - pojedyncza centrala CPR32-NET może obsłużyć do 32 stref alarmowych centrali INTEGRA i jest to jednocześnie maksymalna ilość stref integrowanych w całym systemie KD
 - do komunikacji pomiędzy centralami CPR32-NET i INTEGRA konieczne jest zastosowanie takich interfejsów jak UT-2 (ROGER) oraz INT-RS (SATEL)

Integracja systemu RACS 4 z systemami alarmowymi

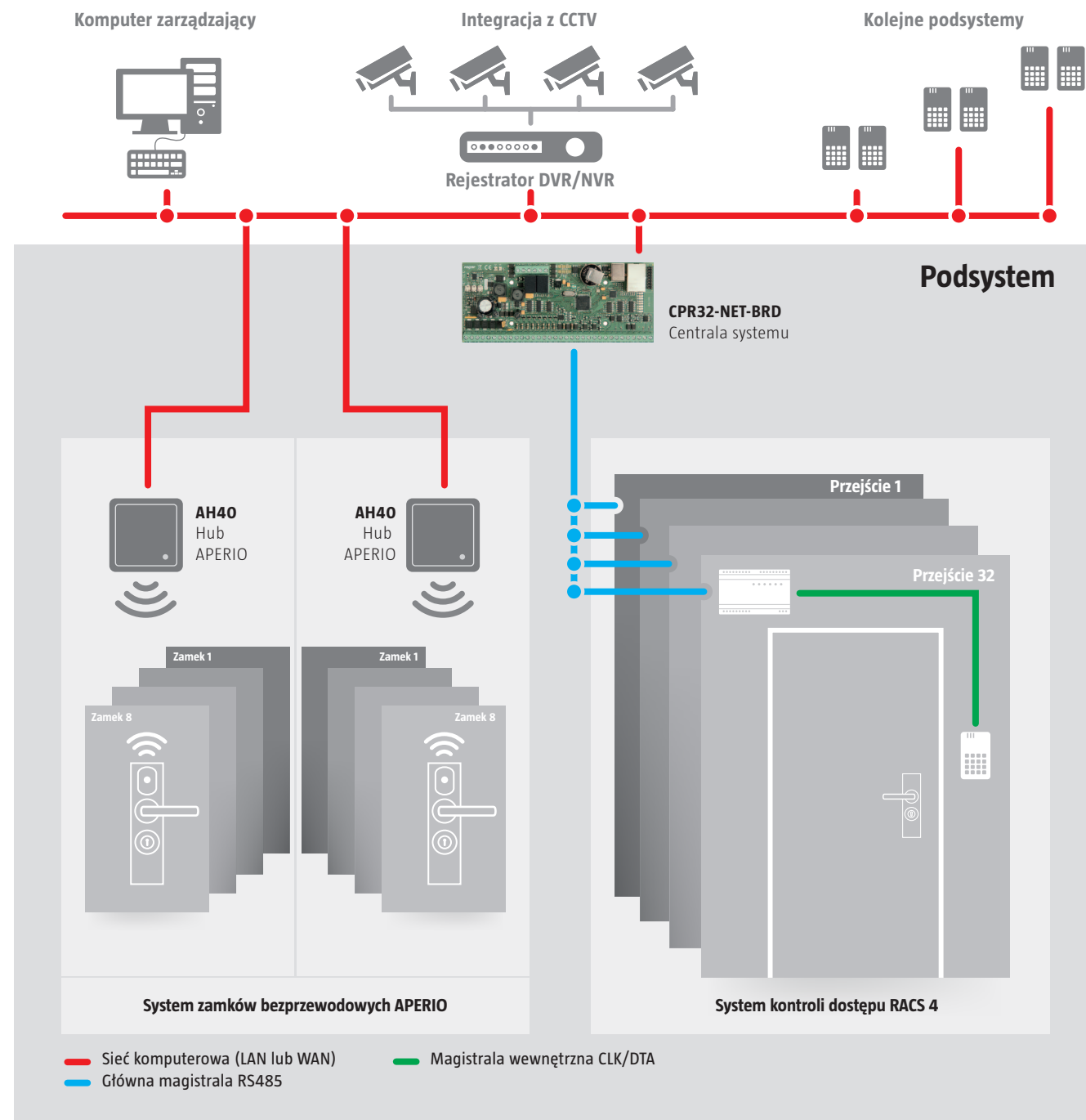


A blurred, vertical image on the left side of the slide showing a crowd of people walking, possibly at a transit station or event. The image is out of focus, with colors like blue, black, and white visible.

Integracja systemu RACS 4 z zamkami bezprzewodowymi

- Integracja z zamkami bezprzewodowymi stanowi uzupełnienie systemu RACS 4 o terminale z komunikacją bezprzewodową
- Integracja wymaga zastosowania centrali CPR32-NET
- Pojedyncza centrala CPR32-NET jest w stanie obsłużyć do 16 zamków systemu APERIO (ASSA ABLOY)

Integracja systemu RACS 4 z zamkami bezprzewodowymi systemu APERIO (ASSA ABLOY)





Integracja PR Master z CCTV

- Integracja z rejestratorami DVR/NVR oraz kamerami IP (z kartami pamięci) takich producentów jak Dahua (BCS) i HIK Vision
- Możliwość odtwarzania obrazów wideo dla wybranych zdarzeń w ramach oprogramowania PR Master
- Możliwość podglądu obrazu z kamer w czasie rzeczywistym w ramach oprogramowania PR Master



Oprogramowanie



PR Master

Oprogramowanie do zarządzania systemem RACS 4



RARC

Program do konfiguracji czytników serii PRTxxMF i PRTxxEM



RCP Master

Oprogramowanie do analizy oraz tworzenia raportów czasu pracy



Roger VDM

Program narzędziowy do niskopoziomowej konfiguracji różnych urządzeń z oferty Roger



Patrol Master

Program do obsługi systemu rejestracji pracy wartowników Patrol II LCD



Roger ISP

Program do aktualizacji oprogramowania firmowego



Roger Mobile Key

Aplikacja mobilna do identyfikacji użytkownika



Roger MiniReader

Program do obsługi czytników zbliżeniowych USB

Charakterystyka programu PR Master



- Obsługa kontrolerów serii PR
- Monitorowanie zdarzeń w czasie rzeczywistym
- Wysyłanie interaktywnych komend do systemu
- Przeglądanie historii zdarzeń z możliwością jej filtracji
- Rejestracja i eksport zdarzeń do oprogramowania RCP
- Graficzna wizualizacja pracy systemu (mapa obiektu)
- Automatyczny i konfigurowalny system tworzenia kopii zapasowych
- Przyznawanie różnych poziomów uprawnień operatorom aplikacji
- Eksport/Import ustawień z/do pliku zewnętrznego w formacie XML

Rejestracja Czasu Pracy w systemie RACS 4



- **Podstawowa** – z poziomu programu PR Master
 - Definiowanie Obszarów Obecności poprzez wskazanie punktów (Terminali) wejściowych i wyjściowych do/z obszaru
 - Możliwość korekty i wstawiania brakujących zdarzeń
 - Tworzenie raportów czasu przebywania użytkownika w obszarze (raport dzienny bądź dla dowolnego zakresu, raporty indywidualne bądź zbiorcze dla całej grupy)

Obszary Obecności

Obszary Obecności:

Nazwa	Komentarz
Produkcja	

Dodaj Edycja Usuń

Punkty identyfikacji:

Punkty wejściowe do Obszaru Obecności:

Nazwa
PR302/145.7/0001/0C19_T1
PR402/145.7/0012/1C23_T1
PR602LCDv2.03.1517/0018/2C29_T1

Dodaj Usuń

Punkty wyjściowe z Obszaru Obecności:

Nazwa
PR402/145.3/0022/3C2F_T1
PR302/145.7/0001/0C19_T0

Dodaj Usuń

OK Pomoc

System RACS 4 w zastosowaniach hotelowych

- Urządzenia przeznaczone do zastosowań hotelowych: kontroler PR821-CH z wbudowanym czytnikiem kart EM 125 kHz/MIFARE oraz z kieszenią na kartę, czytnik HRT82MF i panel klawiszy funkcyjnych HRT82FK
- Kontroler PR821-CH posiada wbudowaną logikę automatyki hotelowej, kontroli dostępu oraz alarmową
- Szybkie meldowanie gości za pomocą oprogramowania PR Master
- Możliwość wykorzystania urządzeń hotelowych w systemach innych producentów w oparciu o API programu PR Master



PR821-CH



HRT82MF



HRT82FK

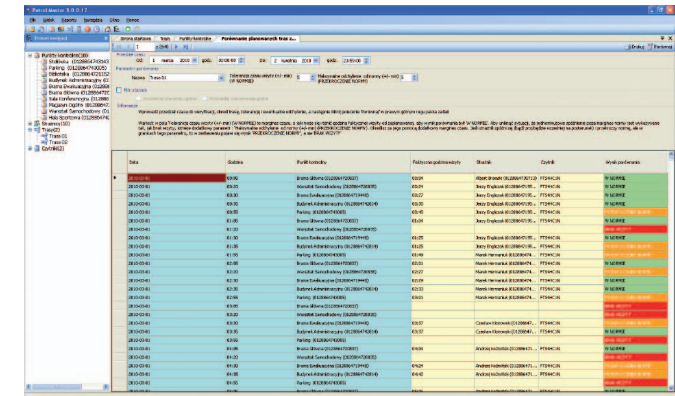
Urządzenia automatyki hotelowej do integracji

- Urządzenia hotelowe do integracji: kontrolery serii HRC, urządzenia peryferyjne serii HRT takie jak kieszeń na kartę, czytnik korytarzowy, panel sterowania klimatyzacją i panele klawiszy funkcyjnych oraz ekspandery serii XM
- Kontrolery HRC umożliwiają realizację funkcji kontroli dostępu, hotelowych, automatyki hotelowej i sygnalizacji włamania
- Oferta obejmuje jedynie urządzenia i protokół komunikacyjny a przygotowanie oprogramowania zarządzającego jest po stronie integratora
- Gotowe oprogramowanie zarządzające aktualnie oferuje firma GiP (<http://gip.com.pl>)



Rejestracja Pracy Wartowników – Patrol II LCD

- Rejestracja pracy wartowników
- Nieulotna pamięć 32 000 zdarzeń
- Odtwarzanie zdarzeń archiwalnych
- Komunikacja poprzez port USB
- Wysoka odporność mechaniczna
- Obsługa za pomocą jednego przycisku
- Do 8000 odczytów na jednym zestawie baterii
- Zasilanie: 2 baterie LR6 (AA)
- Darmowe oprogramowanie pod Windows
- Zabezpieczenia antysabotażowe



Data	Godzina	Wykrywanie	Przebieg	Stwierdzenie	Stwierdzenie	Wykrywanie
2010-01-01	00:00	Wykrywanie (0000000000)	0000	Wykrywanie (0000000000)	0000	Wykrywanie
2010-01-01	00:01	Wykrywanie (0000000000)	0001	Wykrywanie (0000000000)	0001	Wykrywanie
2010-01-01	00:02	Wykrywanie (0000000000)	0002	Wykrywanie (0000000000)	0002	Wykrywanie
2010-01-01	00:03	Wykrywanie (0000000000)	0003	Wykrywanie (0000000000)	0003	Wykrywanie
2010-01-01	00:04	Wykrywanie (0000000000)	0004	Wykrywanie (0000000000)	0004	Wykrywanie
2010-01-01	00:05	Wykrywanie (0000000000)	0005	Wykrywanie (0000000000)	0005	Wykrywanie
2010-01-01	00:06	Wykrywanie (0000000000)	0006	Wykrywanie (0000000000)	0006	Wykrywanie
2010-01-01	00:07	Wykrywanie (0000000000)	0007	Wykrywanie (0000000000)	0007	Wykrywanie
2010-01-01	00:08	Wykrywanie (0000000000)	0008	Wykrywanie (0000000000)	0008	Wykrywanie
2010-01-01	00:09	Wykrywanie (0000000000)	0009	Wykrywanie (0000000000)	0009	Wykrywanie
2010-01-01	00:10	Wykrywanie (0000000000)	0010	Wykrywanie (0000000000)	0010	Wykrywanie
2010-01-01	00:11	Wykrywanie (0000000000)	0011	Wykrywanie (0000000000)	0011	Wykrywanie
2010-01-01	00:12	Wykrywanie (0000000000)	0012	Wykrywanie (0000000000)	0012	Wykrywanie
2010-01-01	00:13	Wykrywanie (0000000000)	0013	Wykrywanie (0000000000)	0013	Wykrywanie
2010-01-01	00:14	Wykrywanie (0000000000)	0014	Wykrywanie (0000000000)	0014	Wykrywanie
2010-01-01	00:15	Wykrywanie (0000000000)	0015	Wykrywanie (0000000000)	0015	Wykrywanie
2010-01-01	00:16	Wykrywanie (0000000000)	0016	Wykrywanie (0000000000)	0016	Wykrywanie
2010-01-01	00:17	Wykrywanie (0000000000)	0017	Wykrywanie (0000000000)	0017	Wykrywanie
2010-01-01	00:18	Wykrywanie (0000000000)	0018	Wykrywanie (0000000000)	0018	Wykrywanie
2010-01-01	00:19	Wykrywanie (0000000000)	0019	Wykrywanie (0000000000)	0019	Wykrywanie
2010-01-01	00:20	Wykrywanie (0000000000)	0020	Wykrywanie (0000000000)	0020	Wykrywanie
2010-01-01	00:21	Wykrywanie (0000000000)	0021	Wykrywanie (0000000000)	0021	Wykrywanie
2010-01-01	00:22	Wykrywanie (0000000000)	0022	Wykrywanie (0000000000)	0022	Wykrywanie
2010-01-01	00:23	Wykrywanie (0000000000)	0023	Wykrywanie (0000000000)	0023	Wykrywanie
2010-01-01	00:24	Wykrywanie (0000000000)	0024	Wykrywanie (0000000000)	0024	Wykrywanie
2010-01-01	00:25	Wykrywanie (0000000000)	0025	Wykrywanie (0000000000)	0025	Wykrywanie
2010-01-01	00:26	Wykrywanie (0000000000)	0026	Wykrywanie (0000000000)	0026	Wykrywanie
2010-01-01	00:27	Wykrywanie (0000000000)	0027	Wykrywanie (0000000000)	0027	Wykrywanie
2010-01-01	00:28	Wykrywanie (0000000000)	0028	Wykrywanie (0000000000)	0028	Wykrywanie
2010-01-01	00:29	Wykrywanie (0000000000)	0029	Wykrywanie (0000000000)	0029	Wykrywanie
2010-01-01	00:30	Wykrywanie (0000000000)	0030	Wykrywanie (0000000000)	0030	Wykrywanie
2010-01-01	00:31	Wykrywanie (0000000000)	0031	Wykrywanie (0000000000)	0031	Wykrywanie
2010-01-01	00:32	Wykrywanie (0000000000)	0032	Wykrywanie (0000000000)	0032	Wykrywanie
2010-01-01	00:33	Wykrywanie (0000000000)	0033	Wykrywanie (0000000000)	0033	Wykrywanie
2010-01-01	00:34	Wykrywanie (0000000000)	0034	Wykrywanie (0000000000)	0034	Wykrywanie
2010-01-01	00:35	Wykrywanie (0000000000)	0035	Wykrywanie (0000000000)	0035	Wykrywanie
2010-01-01	00:36	Wykrywanie (0000000000)	0036	Wykrywanie (0000000000)	0036	Wykrywanie
2010-01-01	00:37	Wykrywanie (0000000000)	0037	Wykrywanie (0000000000)	0037	Wykrywanie
2010-01-01	00:38	Wykrywanie (0000000000)	0038	Wykrywanie (0000000000)	0038	Wykrywanie
2010-01-01	00:39	Wykrywanie (0000000000)	0039	Wykrywanie (0000000000)	0039	Wykrywanie
2010-01-01	00:40	Wykrywanie (0000000000)	0040	Wykrywanie (0000000000)	0040	Wykrywanie
2010-01-01	00:41	Wykrywanie (0000000000)	0041	Wykrywanie (0000000000)	0041	Wykrywanie
2010-01-01	00:42	Wykrywanie (0000000000)	0042	Wykrywanie (0000000000)	0042	Wykrywanie
2010-01-01	00:43	Wykrywanie (0000000000)	0043	Wykrywanie (0000000000)	0043	Wykrywanie
2010-01-01	00:44	Wykrywanie (0000000000)	0044	Wykrywanie (0000000000)	0044	Wykrywanie
2010-01-01	00:45	Wykrywanie (0000000000)	0045	Wykrywanie (0000000000)	0045	Wykrywanie
2010-01-01	00:46	Wykrywanie (0000000000)	0046	Wykrywanie (0000000000)	0046	Wykrywanie
2010-01-01	00:47	Wykrywanie (0000000000)	0047	Wykrywanie (0000000000)	0047	Wykrywanie
2010-01-01	00:48	Wykrywanie (0000000000)	0048	Wykrywanie (0000000000)	0048	Wykrywanie
2010-01-01	00:49	Wykrywanie (0000000000)	0049	Wykrywanie (0000000000)	0049	Wykrywanie
2010-01-01	00:50	Wykrywanie (0000000000)	0050	Wykrywanie (0000000000)	0050	Wykrywanie
2010-01-01	00:51	Wykrywanie (0000000000)	0051	Wykrywanie (0000000000)	0051	Wykrywanie
2010-01-01	00:52	Wykrywanie (0000000000)	0052	Wykrywanie (0000000000)	0052	Wykrywanie
2010-01-01	00:53	Wykrywanie (0000000000)	0053	Wykrywanie (0000000000)	0053	Wykrywanie
2010-01-01	00:54	Wykrywanie (0000000000)	0054	Wykrywanie (0000000000)	0054	Wykrywanie
2010-01-01	00:55	Wykrywanie (0000000000)	0055	Wykrywanie (0000000000)	0055	Wykrywanie
2010-01-01	00:56	Wykrywanie (0000000000)	0056	Wykrywanie (0000000000)	0056	Wykrywanie
2010-01-01	00:57	Wykrywanie (0000000000)	0057	Wykrywanie (0000000000)	0057	Wykrywanie
2010-01-01	00:58	Wykrywanie (0000000000)	0058	Wykrywanie (0000000000)	0058	Wykrywanie
2010-01-01	00:59	Wykrywanie (0000000000)	0059	Wykrywanie (0000000000)	0059	Wykrywanie
2010-01-01	01:00	Wykrywanie (0000000000)	0060	Wykrywanie (0000000000)	0060	Wykrywanie

Patrol Master 3



Patrol II LCD



PK-2



PK-3



Dziękujemy za uwagę

Zastrzeżenia:

Niniejszy dokument nie stanowi dokumentacji technicznej produktu i ma jedynie charakter poglądowy. Producent zastrzega sobie prawo zmian w charakterystyce produktu bez konieczności uprzedniego powiadamiania. Podane w dokumencie dane prezentują możliwości funkcjonalne urządzenia, których dostępność jest uzależniona od jego wersji, konfiguracji oraz dodatkowego wyposażenia.

© 2016 ROGER sp. z o.o. sp. k. All rights reserved. Niniejszy dokument podlega Warunkom Użytkowania w wersji bieżącej, opublikowanej w serwisie internetowym www.roger.pl

roger[®]

ROGER sp. z o.o. sp. k.
82-400 Sztum
Gościszewo 59
Polska

T. +48 55 272 0132
F. +48 55 272 0133
E. roger@roger.pl
www.roger.pl