

Roger Access Control System

PRxx1 series controllers Functional Description and Programming Guide

Document version: Rev.D

*This document refers to the following products:
PR311SE, PR311SE-BK, PR611, PR621, PR621-CH, PR411DR, PR411DR-BRD*



Contents:

I. General	4
1.1 Introduction	4
1.2 Design and Architecture	4
1.3 Features of PRxx1 series controllers	7
II Functional Description	8
2.1 Available scenarios of operation	8
2.1.1 Standalone System	8
2.1.2 Network System (with CPR32-SE)	9
2.1.3 Network System (without CPR32-SE)	9
2.2 Communication	10
2.2.1 RS485 communication bus	10
2.2.2 Controller address	10
2.2.3 RACS Clock and Data Interface	11
2.2.4 XM-2 - I/O Extension Module	11
2.2.5 Wiegand Interface Readers	12
2.3 Users	12
2.3.1 Standard and Guest Users	12
2.3.2 User Options	13
2.3.3 Groups	14
2.4 Identification Modes	14
2.5 Door Modes	14
2.6 Armed and Disarmed Modes	15
2.6.1 Concept	15
2.6.2 Arming and Disarming	15
2.6.3 Time scheduled arming/disarming	15
2.6.4 Option: Arm/Disarm Schedule	15
2.7 Access Rights	15
2.7.1 Access Signaling	16
2.7.2 Door Lock Control	16
2.7.3 Option: Access Disabled when Controller Armed	16
2.7.4 Option: Door Lock Controlled in Latch Mode (toggle)	17
2.7.5 Option: Auto-relock mode	17
2.7.6 Facility Code	17
2.7.7 Option: Disable PIN under duress	17
2.7.8 Option: Hotel room	17
2.7.9 System Flags	18
2.7.10 Door Alarm	19
2.7.11 Option: Enable Door Alarm signaling on internal buzzer	20
2.7.12 Option: Device temporary blocked after 5 wrong logins	20
2.7.13 Option: Constant activation of Output 1 by card in vicinity of reader	20
2.7.14 Anti-passback (APB)	20
2.7.15 Anti-passback Zones (APB Zones)	21
2.7.16 Alarm Zones	22
2.8 Inputs	23
2.9 Outputs	25
2.10 Function Keys	28
2.11 Function Cards	29
III. Programming	31

3.1 Memory Reset – Setting MASTER identifier and ID address of the controller	31
3.2 User Commands	32
3.3 Installer Programming Mode.....	34
3.4 Acoustic and visible signals.....	41
3.4.1 Visible signals.....	41
3.4.2 Acoustic signals	41

Typing conventions

Functions, options and commands

Examples

Specific names related to RACS system

STATUS, FLAG OR TIMER

Notes

bold letter

italics letters

with first capital letter

capital letters

separated with two lines (upper, lower)
from the standard text

I. GENERAL

1.1 Introduction

This document applies to PRxx1 series standard controllers and includes devices with built-in reader for installation near the door (PR311-SE, PR621, PR612) as well as device without built-in reader for installation inside metal box preferably in some distance from door (PR411DR). The controller PR621-CH is equipped with card holder and functionally is the same as PR621 controller. Therefore in the present document, the name PR621 applies to both versions of the controller. The only difference between PR311-SE-BK and PR311-SE is lack of keypad in the first one. The controller PR411DR is available both in plastic enclosure for installation on DIN 35mm rail (PR411DR) or as electronic module (PR411DR-BRD). The name PR411DR applies to all possible models of this controller.

This document does not apply to older type controllers of following types: PR401, PR301 and PR201.

1.2 Design and Architecture

The PRxx1 series controllers are single-door, two-way access controllers. Each PRxx1 controller can work with two logical access points (readers) called respectively: Terminal ID0 and Terminal ID1. All PRxx1 series controllers except for PR411DR are equipped with built-in reader of EM125kHz standard, which is logically treated as Terminal ID1 and they can operate with one external reader logically treated as Terminal ID0. The PR411DR controller is not equipped with any built-in reader but it can work with two external readers. Generally, the PRxx1 controllers are designed to operate with PRT series readers (from Roger) configured to RACS Clock&Data data protocol, however PR411DR can also work with Wiegand 26-66bit readers as well.

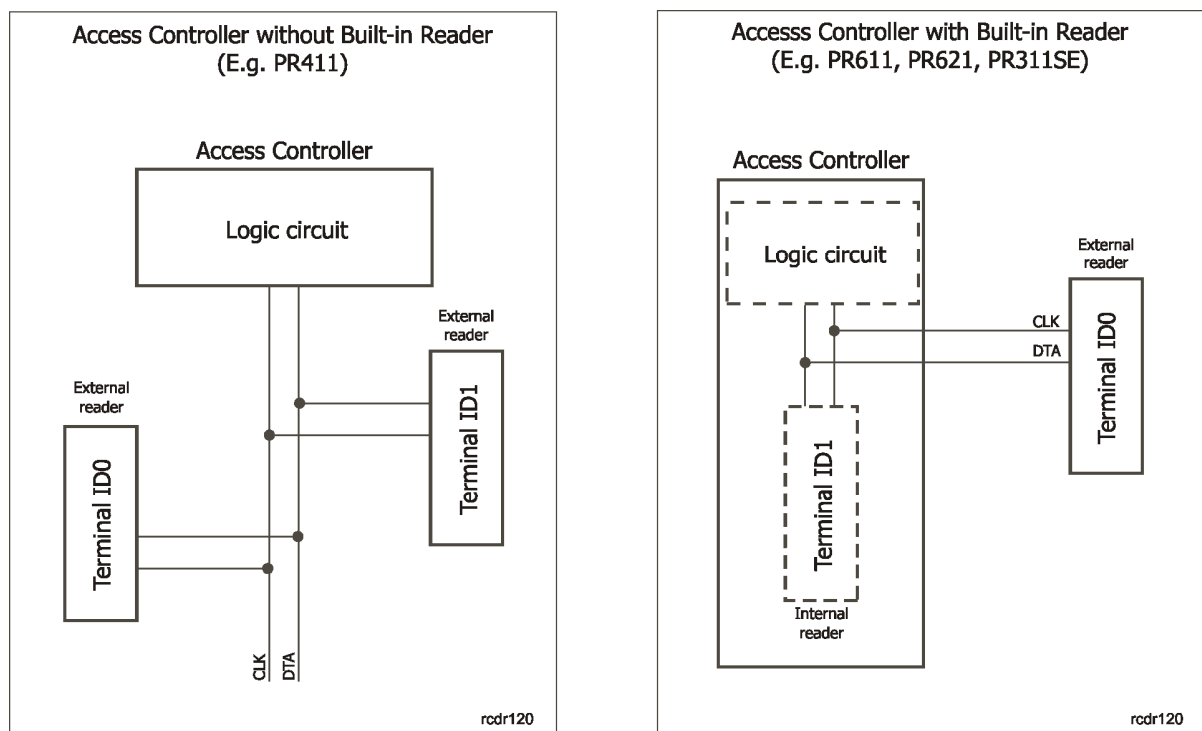


Fig. 1 General architecture of controller and reader(s)

PRxx1 controller can register up to 1000 users plus 8 special ones called Guests. Each user has its own ID number and may have proximity card and/or PIN. Controller firmware can be upgraded on-site by means of RS485 serial interface and what is important the firmware upgrade process does not require unit to be removed from its original place of installation. PRxx1 controllers can operate fully autonomously (Standalone System) or in the Network System with or without CPR32-SE network controller. PRxx1 controllers can be programmed manually or from PC. Manual programming can be performed locally using the device's keypad or from remote keypad located on the external PRT series reader and connected to the programmed controller (the external reader which is used to program controller should be equipped with keypad and configured to RACS Clock&Data mode with ID0 address) – see III. Programming. Later, for some user programming functions a so called Function Cards can be used. Remote programming can be done by means of PR Master software (Roger) installed on PC. The communication with single controller and management of the whole access control system requires a dedicated interface device e.g.:

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

Table 1. List of PRxx1 series controllers							
Controller	PR311SE	PR311SE-BK	PR611	PR621	PR621-CH	PR411DR	PR411DR-BRD
Power supply	12VDC	12VDC	12 VDC	12 VDC	12VDC	12 VDC, 24VDC, 18VAC	12 VDC, 24VDC, 18VAC
Programmable NO/NC inputs	3	3	3	3	3	8	8
Programmable relay outputs	1 x 1,5A/30V	1 x 1,5A/30V	1 x 1,5A/30V	1 x 1,5A/30V	2 x 5A/30V i 230VAC	1 x 1,5A/30V	1 x 1,5A/30V
						1 x 5A/30V and 230VAC	1 x 5A/30V and 230VAC
Programmable transistor outputs 1A/15VDC	2	2	2	2	2	2	2
Built-in EM 125kHz reader	Yes	Yes	Yes	Yes	Yes	No	No
External PRT series readers	1	1	1	1	1	2	2
External Wiegand 26-66bit readers	No	No	No	No	No	2	2
Built-in keypad	Yes	No	Yes	No	No	No	No
Built-in function keys	Yes	No	No	No	No	No	No
Other	Outdoor operation, connecting cable included (45 cm)	Outdoor operation, connecting cable included (45 cm)	Outdoor operation, connecting cable (45 cm) or screw terminals included	Outdoor operation, connecting cable (45 cm) or screw terminals included	Outdoor operation, connecting cable (45 cm) or screw terminals included, card holder	Installation on DIN 35mm rail, built-in 1.2A/12VDC power supply unit, possible connection of backup battery.	Electronic module, built-in 1.2A/12VDC power supply unit, possible connection of backup battery.

1.3 Features of PRxx1 series controllers

Features of standard series PRxx1 controllers:

- Single door, two-way access control
 - Operation in Standalone or Network System
 - Possible connection of PRT series readers (Roger)
 - Possible connection of Magstripe oraz Wiegand readers (only PR411DR)
 - User identification by means of prox. card or PIN
 - Programmable validity time for user prox. card or PIN
 - Limited number of accesses for users
 - Up to 1000 users
 - 250 Access Groups
 - 99 Schedules (*)
 - 128 time periods within single Schedule (*)
 - 4 Holiday Schedules (H1-H4) (*)
 - Automatic winter-summer time change (*)
 - Time and Attendance registration (*)
 - Built-in keypad (PR311SE, PR611)
 - Programmable inputs/outputs
 - Built-in 1.5A/30V relay output
 - Built-in 5A/230V relay output (PR411DR only)
 - Operation with XM-2 I/O module
 - Communication with controllers by RS485 bus
 - Firmware upgrade through RS485 serial port
 - Integration with CCTV systems
 - Management software for Windows XP/Vista/7
 - Outdoor operation (PR311SE, PR311SE-BK, PR611 and PR621)
 - DIN RAIL 35mm enclosure (only PR411DR)
 - Management through LAN/WAN (UT-4 interface required)
 - CE mark
- (*) - features available only in Network Systems (see 2.1.2 Network System (with CPR32-SE))

II FUNCTIONAL DESCRIPTION

2.1 Available scenarios of operation

2.1.1 Standalone System

If PRxx1 controller works autonomously i.e. without CPR32-SE network controller then it does not offer neither time related functions (e.g. timed access rights) nor event log. In this mode, it is possible to assign users to different Access Groups but their right are not time related. Within Standalone system all users have full access rights 24h/7d or have no access depending on settings. This mode enables defining of Access Zones. Controller can be programmed manually or from PC by means of PR MASTER software.

Note: The standalone scenario does not exclude the possibility to connect with controller by means of RS485 interface as well as programming from PC.

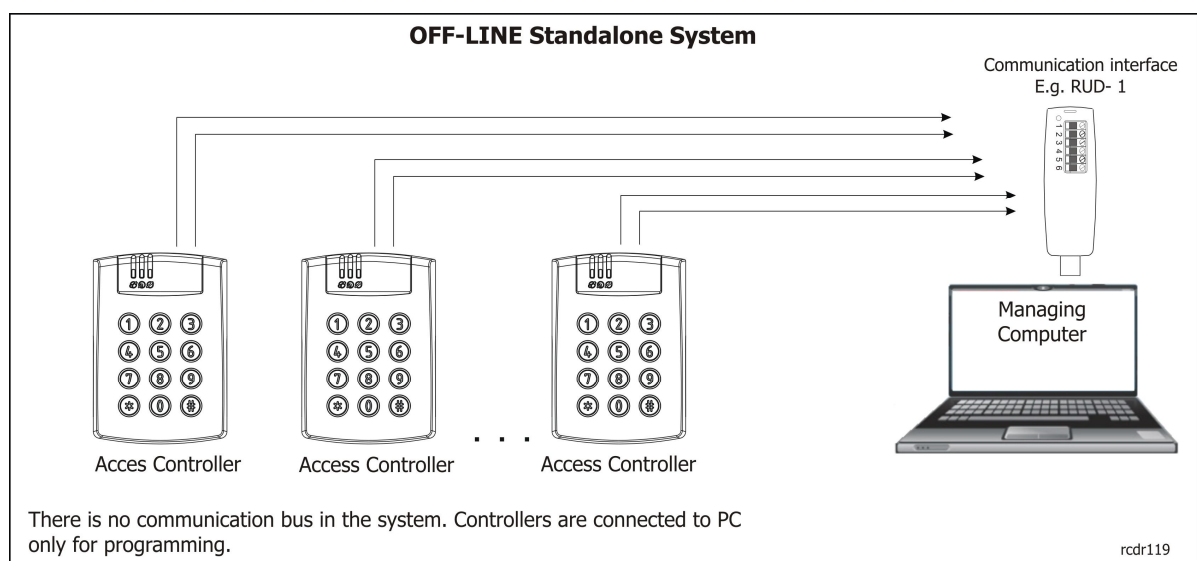


Fig. 2 Standalone System (offline)

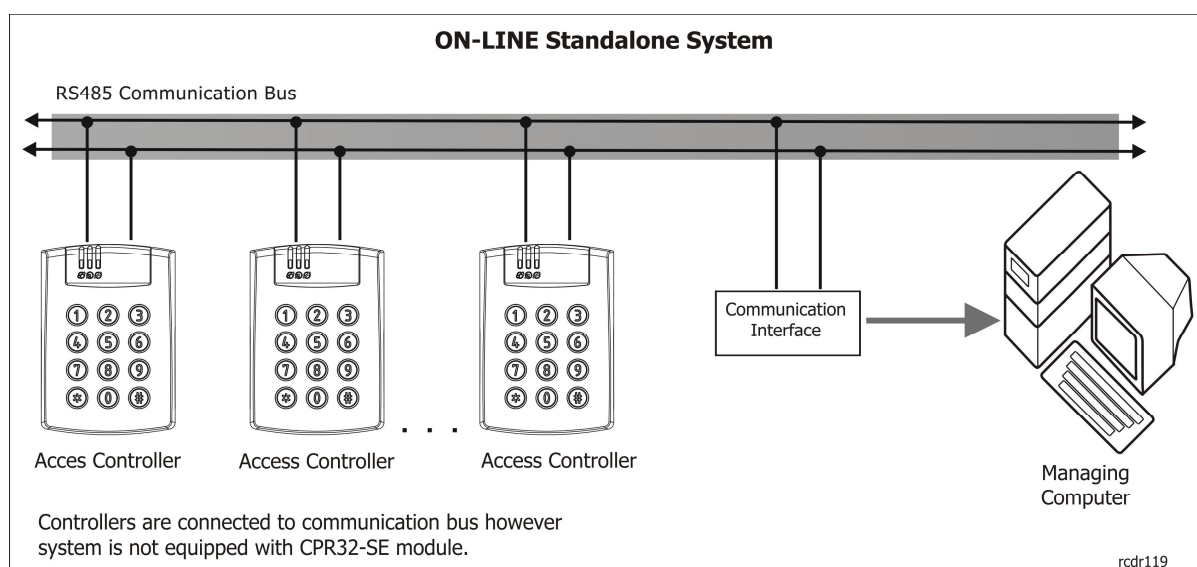


Fig. 3 Standalone system (online)

2.1.2 Network System (with CPR32-SE)

When controllers operate in a system equipped with CPR-32SE unit, users can be divided into 250 different Access Groups and be assigned to Schedules. CPR-32SE also provides event buffer, real time clock and calendar plus global type functionalities like Alarm Zones and Global Anti-passback. Also Access Zones can be specified by administrator. PC is required only for programming and management of such Network System.

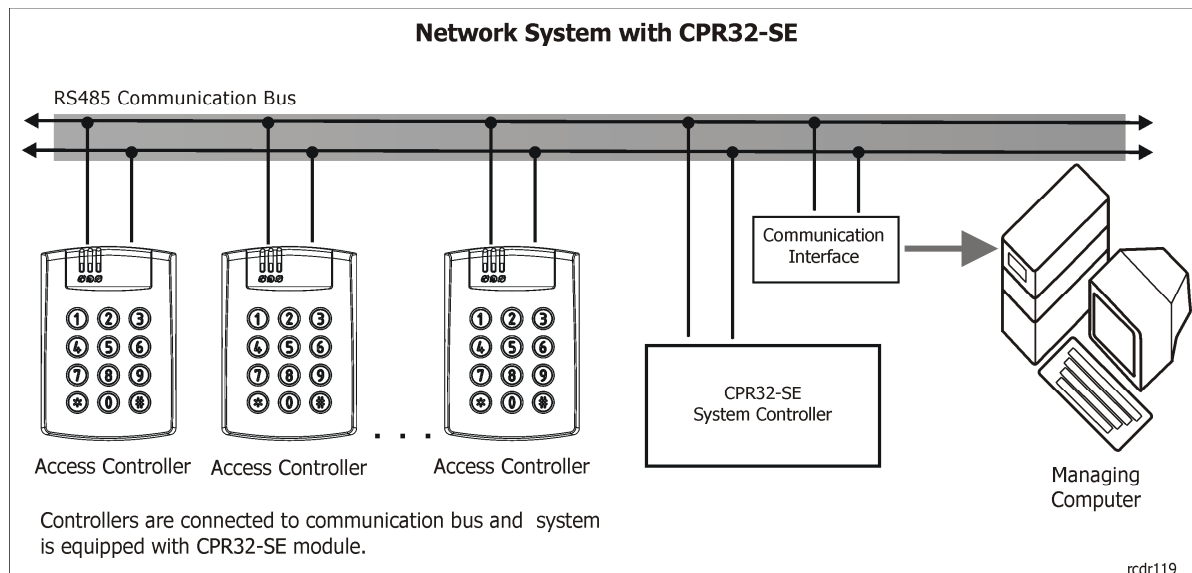


Fig. 4 Network System with CPR32-SE

2.1.3 Network System (without CPR32-SE)

In such configuration, PC and PR Master software in monitoring mode can emulate CPR32-SE network controller. Therefore it is possible to assign users to particular Groups, Schedules and Access Zones as well as define Door Modes and Identification Modes. The same pertains to such global functions as Zone Alarms and APB Zones. Mentioned functionalities are available only if PC is hardwired to communication interface, is always on and PR Master software is in monitoring mode. In case of PC failure or PC turn off, access controllers automatically switch to Autonomous (Standalone) Mode and continue their operation based on the settings available prior to failure/PC disconnection. After recovery of communication with PC, access controllers automatically switch to Network Mode and realize previously suspended functions, including Schedules.

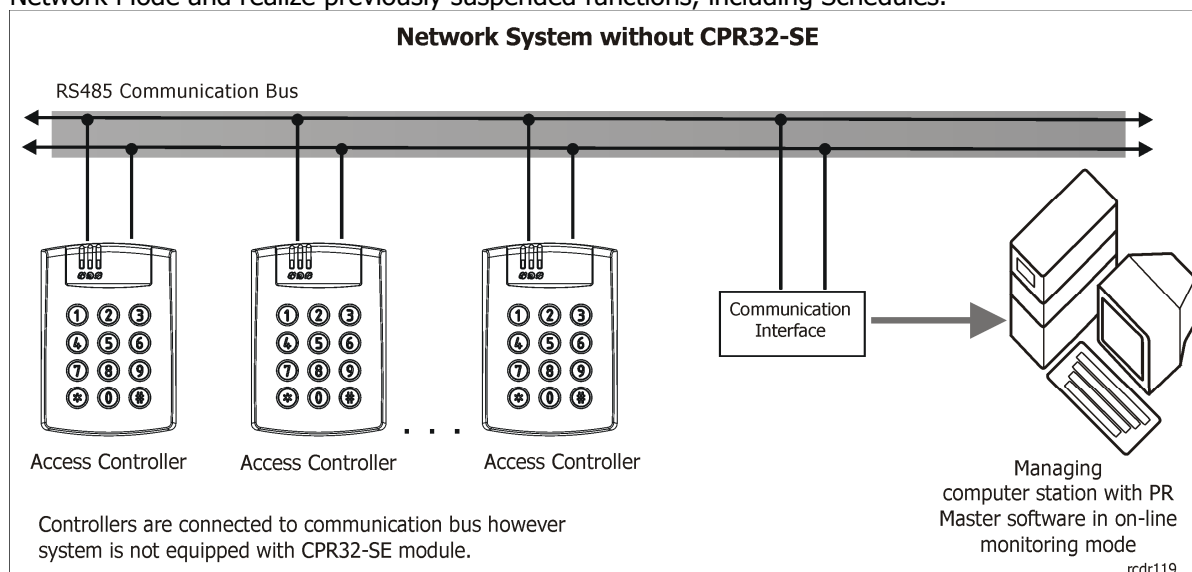


Fig. 5 Network System without CPR32-SE

2.2 Communication

2.2.1 RS485 communication bus

Communication with PRxx1 controllers is based on RS485 interface and devices in RS485 network must have unique address (ID=00-99). A single communication bus may accommodate up to 32 access controllers (complete Network) and one optional CPR32-SE unit. The RACS4 system communication topology of Network is fairly flexible i.e. tree structures as well as star topologies are allowed, however loop topology is forbidden. Regular signal cables can be used and unshielded twisted-pair wire is recommended. Terminating resistors at either end of the communication bus are not required.

Maximum cable lengths in the RACS4 system are as follows:

- Between any controller and CPR32-SE: 1200 m
- Between any controller and interface device: 1200 m
- Between CPR32-SE and interface device: 1200 m

Note: All devices connected to RS485 bus must share the same ground potential, and this condition is clearly satisfied if all devices are supplied from the same power supply unit. If more than one power supply unit is used, then negative DC terminals of each power supply unit need to be connected with each other by means of additional wire (could be standard signal wire). If such connection is not feasible for any reasons, negative DC output of each power supply unit should be earthed separately, however, the difference of earth potential across all units cannot exceed +/-2V. DO NOT short circuit positive terminals of power supply.

The structure incorporating RS485 communication bus, access controllers and optional CPR32-SE unit is called an Access Control Network or simply a Network (or Subsystem). Each Network in the RACS4 system must be connected to PC via a separate communication port. It can be the standard COM Port, Virtual COM Port (VCP) or Ethernet port. In case of VCP, users can use interface device (Roger), which emulates COM port, e.g. RUD-1 or UT-2USB. In case of Ethernet port, UT-4DR is recommended.

Each type of PRxx1 controller can manage single door in one-way or two-way mode. Presently, RACS4 permits integration of up to 250 Networks (Subsystems), each including up to 32 controllers. PC with PR Master software communicates with each Network by means of separate communication port, which means that it is possible to integrate Networks connected to PC by means of following interfaces: RS232, USB, Ethernet and Wi-Fi, thus creating one access control system.

Note: All mentioned communication interfaces can be used not only for controller programming but also for the management of entire access control system, depending on applied scenario (see 2.1 Available scenarios of operation). In case of on-site programming, we recommend RUD-1 interface device that provides built-in 12VDC output which can be used to supply programmed device.

2.2.2 Controller address

Each controller connected to RACS4 system communication bus (RS485) must have its own address in range of 00-99. Default address is ID=00 and can be modified either remotely using PR Master software (Roger) or manually (see 3.1 Memory Reset – Setting MASTER identifier and ID address of the controller and 3.3 Installer Programming Mode) or by means of jumpers (only PR411DR). Moreover, it is possible to assign a so called "FixedID" to the controller. This option is particularly useful if there is a risk that someone will accidentally change controller address resulting in disruption of the whole system. The fixed address can be set, changed or cleared only by means of RogerISP software during firmware upgrade procedure.

Besides mentioned methods of addressing, the PR411DR controller offers the option to set address by means of programming jumpers. The whole range of possible address is 0-127. If controller address is set in range of 0-99 then it cannot be changed neither by means of PR Master nor manually. It can be modified only if jumper address is set above 99. For details regarding various address settings refer to the relevant Installation Guide.

Note: The fixed address (FixedID) has always the highest priority – if it is set then it can be modified only using RogerISP software during firmware upgrade procedure.

2.2.3 RACS Clock and Data Interface

Besides the RS485 communication bus, PRxx1 controllers feature also the so-called RACS Clock & Data interface (alternatively called: Internal Bus). This interface is used for communication with external PRT series readers and/or XM-2 I/O extension module. RACS Clock&Data interface incorporates two lines: CLK and DTA. The following devices can be connected to the internal bus:

- Primary access reader (Terminal ID0, address ID=0)
- Secondary access reader (Terminal ID1, address ID=1) (only PR411DR)
- XM-2 input/output extension module (address ID=5)

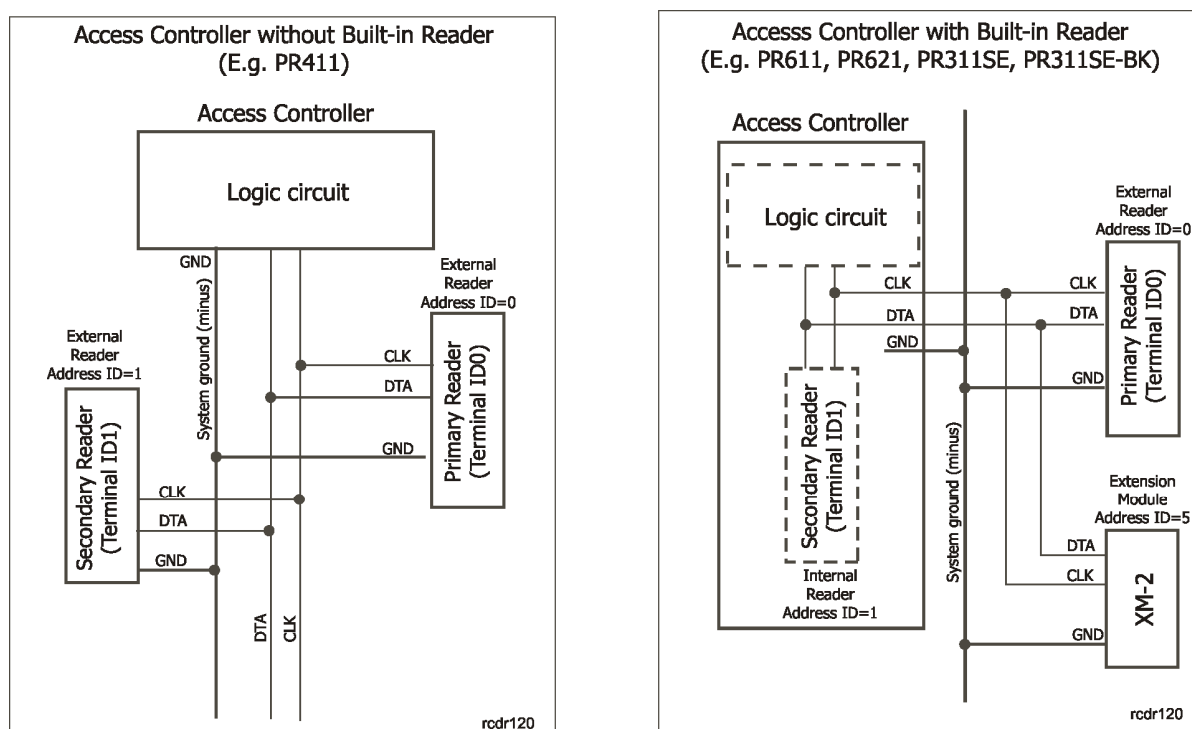


Fig. 6 RACS Clock&Data interface

Note: If there are no devices connected to CLK and DTA lines then it is possible to configure these lines as standard transistor type outputs, capable to sink up to 150mA/15VDC.

For CLK/DTA lines any type of signal cable can be used. There is no need to use either twisted or shielded cables. The maximum cable length between controller and external reader and/or XM-2 extension module is limited to 150m. Similarly as in case of RS485 bus, all devices connected to CLK/DTA line should have common negative terminals. Such condition is usually satisfied because devices connected to CLK/DTA line are usually directly supplied from controller. Otherwise negative terminal of each reader must be connected to respective controller GND or COM terminal.

2.2.4 XM-2 - I/O Extension Module

The PRxx1 series controller can operate with single XM-2 I/O extension module. This module offers two NO/NC inputs and two relay outputs. Both inputs and outputs of XM-2 can be programmed in the same way as internal inputs/outputs of the controller. The XM-2 can be used to extend number of available inputs and outputs and/or separate relay output connected to door strike. Such separation of relay output might be required in case of PR302 and PR602LCD controllers as they

are installed near the door and can suffer from intrusion. The XM-2 module connected to controller must be configured to address ID=5. Digital communication between controller and XM-2 module is performed by means of RACS Clock&Data bus. For more information on XM-2 module refer to Installation Guide, which is available at www.roger.pl.

2.2.5 Wiegand Interface Readers

Only PR411DR can work with Wiegand interface readers. The controller uses separate input lines in order to connect with such readers, as presented in figure 6 below.

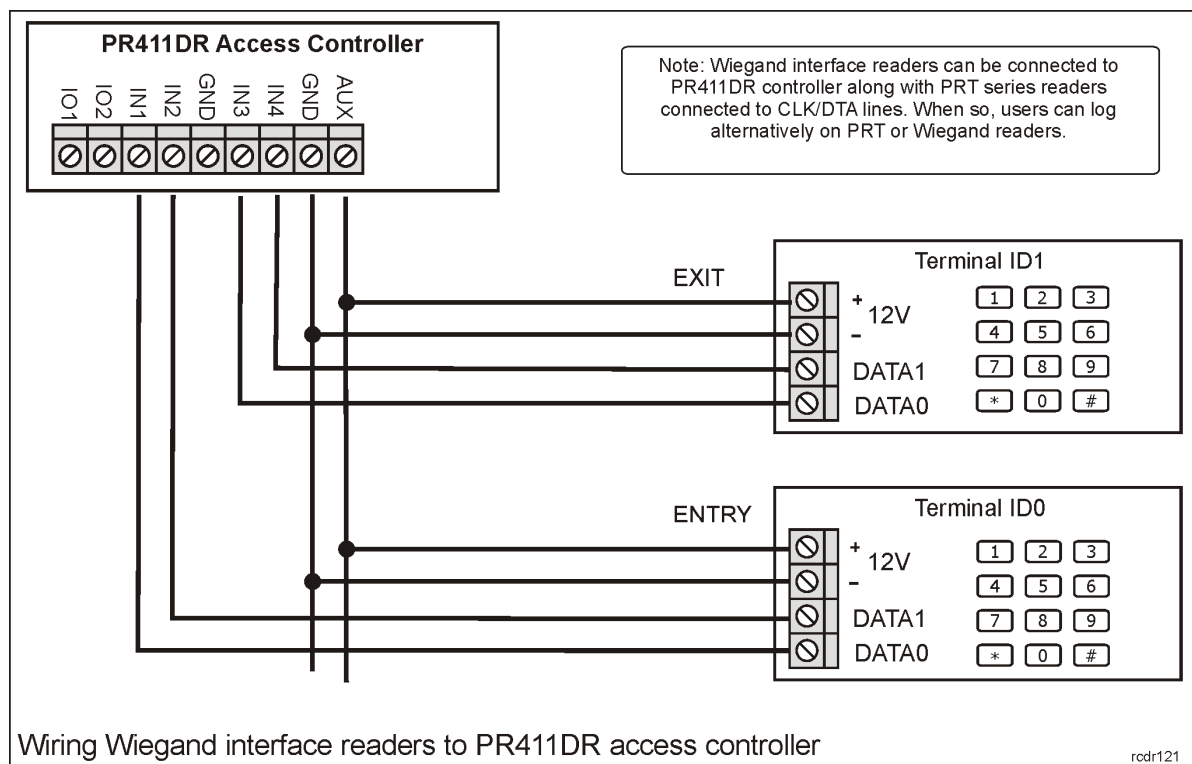


Fig. 7 Wiring for Wiegand interface readers

In general, Wiegand readers can be connected to PR411DR controller along with PRT series readers. If so, users can login either on Wiegand or PRT reader.

2.3 Users

2.3.1 Standard and Guest Users

Each user programmed in the controller might have card and/or PIN (3-6 digits followed by #), also he/she can be granted with 8 special User Options. All types of users are specified in table 2.

Table 2. User types		
User type	ID	Description
MASTER	000	MASTER has the highest privileges in the system and is allowed for both door access and arming/disarming of the controller. The MASTER has always fixed Op.1 = No and all other options Op.2-Op.8 = Yes (see table 3)
SWITCHER Full	ID=001-049	SWITCHER Full is allowed for both normal access and arming/disarming of the controller. Double use of identifier is

		required for arming/disarming and single use of identifier gives door access.
SWITCHER Limited	ID=050-099	SWITCHER Limited is allowed solely for arming/disarming of the controller and is not allowed for door access. Single use of identifier is required for arming/disarming.
NORMAL	ID=100..999	NORMAL is allowed solely for door access and by default is not allowed to arm/disarm controller.
GUEST	ID=4000-4007	GUEST is defined individually in each controller in the system. GUEST might be authorized for door access and for arming/disarming.

Standard users (ID=000-999) are recorded in all controllers of the access control system and Guest users (ID=4000-4007) are programmed individually on each controller. These users are programmed and managed by means of special programming procedures. Optionally, for management of Guest users there is a special programmer's interface (API) which allows system integrators to create special software dedicated to manage this kind of users. Every Guest user may have card and/or PIN and can be granted with one or more special User Options as any other standard user of the system. If the controller works in Network Access Control System (see 2.1.2 Network System) then Guest users can be assigned to the Access Group – as a result their access rights will be under control of Schedule.

2.3.2 User Options

Eight special options (called Op.1 - Op.8) can be assigned to every individual user within particular controller including Standard Users, Guest users and Facility Code cardholders as well. The options define additional rights related to programming and management of particular controller.

Table 3: User options		
Option	Name	Function
Op.1	Access completely disabled	When option is active, the user do not have access rights at particular controller regardless of other settings.
Op.2	Enabled for authorization of F1 key at Terminal ID0	When option is active, the user will be allowed to use F1 key at terminal ID0 (if such authorization is required at all (see 2.10 Function Keys)
Op.3	Enabled for authorization of F2 key at Terminal ID0	When option is active, the user will be allowed to use F2 key at terminal ID0 (if such authorization is required at all (see 2.10 Function Keys)
Op.4	Enabled for authorization of F1 key at Terminal ID1	When option is active, the user will be allowed to use F1 key at terminal ID1 (if such authorization is required at all (see 2.10 Function Keys)
Op.5	Enabled for authorization of F2 key at Terminal ID1	When option is active, the user will be allowed to use F2 key at terminal ID1 (if such authorization is required at all (see 2.10 Function Keys)
Op.6	Enabled for authorization of User Commands	When option is active, the user will be allowed to apply User Commands (see 3.2 User Commands)
Op.7	Enabled for arming/disarming	When option is active, the user will be allowed to arm/disarm particular controller.
Op.8	Enabled for authorization of Function Cards	When option is active, the user will be allowed to use Function Cards (see 2.11 Function Cards)

2.3.3 Groups

Users of RACS4 access control system can be divided into Groups or may belong to special (default) group called: No Group or No Access Group. All users assigned to a particular user Group share the same (identical) access rights. You can also define Group for single user. Members of particular Group are granted access to particular areas in accordance with defined Schedules. Users belonging to No Group are given unlimited 24h/7d access to all Access Zones, while users assigned to No Access Group cannot open any door.

2.4 Identification Modes

Following Identification Modes are available for the purpose of user identification:

Table 4: Identification modes	
Mode	Description
Card or PIN	Controller requires card or PIN
Card and PIN	Controller requires card and PIN
Card Only	Controller requires card only, PINs are not accepted
PIN Only	Controller requires PIN only, cards are not accepted

Identification Modes are set for both sides of door. Unless modified by administrator, the controller applies default Identification Mode (i.e. Card or PIN). Identification modes apply to all users at particular controller/reader and they can be set or changed by:

- Schedule (only Network System)
- Function keys
- Input lines

2.5 Door Modes

Door Modes determine rules for locking/unlocking of access controlled doors. Following Door Modes are available in RACS4 system:

Table 5: Door Modes	
Mode	Description
Normal	Normally the door is locked and opened only for the time of granted access.
Unlocked	The door is unlocked permanently. No identification is required to enter or exit.
Conditionally unlocked	Initially, the door is in the Normal Mode. As soon as the first user is granted an access, the controller switches to the Unlocked mode.
Locked	The door is locked permanently for all users regardless of their access rights.

Default mode is always the Normal Mode. Door Modes can be set or changed by:

- Schedule (only Network Systems, see 2.1.2 Network System (with CPR32-SE))
- Function keys
- Input lines

2.6 Armed and Disarmed Modes

2.6.1 Concept

PRxx1 series controllers feature 2 arming modes: Armed and Disarmed. The current mode is indicated on the controller's LED STATUS . Red color indicates Armed mode, whereas the green one indicates Disarmed mode. Following methods can be used to set or change the modes:

- Manually by means of identifier (access card or PIN)
- Schedule (only in network systems, see 2.1.2 Network System)
- Input lines
- Function keys
- Alarm Zones logic (only in network systems, see 2.1.2 Network System)
- Remotely by PR Master software (PC)

2.6.2 Arming and Disarming

The controller can be armed/disarmed by following user types: MASTER, SWITCHER Full or SWITCHER Limited (see 2.3.1 Standard and Guest Users). In case of MASTER and SWITCHER Full users the procedure of arming/disarming is as follows:

- Use card and/or PIN (depending on current Identification Mode – see 2.4 Identification Modes)
- Upon a successful authorization, the controller might grant access and release the door lock (depends on general access rights and some other options)
- Wait till the LED SYSTEM  starts blinking
- While LED is blinking, use card/PIN once more (card or PIN regardless of current Identification Mode)

In case of SWITCHER Limited just use card and/or PIN once. SWITCHER Limited is only authorized to arm/disarm, thus access shall not be granted.

2.6.3 Time scheduled arming/disarming

A controller's arming mode can be altered automatically via Schedule. There are two possible two scenarios. If controller belongs to Alarm Zone it will be armed/disarmed automatically as the given Alarm Zone changes its arming mode however it is not important what caused the given Alarm Zone to change Arming Mode (Schedule, user activity or any other logic). If a controller is not assigned to any Alarm Zone, it may be assigned any Schedule which will control its arming mode. Assigning the controller the so-called NEVER Schedule forces it to remain always in the armed mode. On the contrary, applying the ALWAYS Schedule makes the controller operate continuously in the disarmed mode.

An Arming/Disarming Schedule by itself is a standard schedule (a so-called General Purpose Schedule - GPS). The GPS schedule is composed of time periods From/To used for specifying when controller will automatically switch to disarmed mode. While outside the specified time periods, a controller will automatically return to the armed mode. Automatic switching back to the armed mode may be disabled if the input line **[13]: Arming disabled** is triggered or a door is opened (**Input line [01]: Door contact** indicates that the door is not closed).

2.6.4 Option: Arm/Disarm Schedule

Whenever this option is activated, the current armed/disarmed mode on a controller changes automatically according to the specified Schedule. The Schedule can be defined exclusively for the Alarm Zone the controller is assigned to or it could be any schedule if the controller is not assigned to any Alarm Zone. If the option is deactivated then arming/disarming based on Schedules is switched off.

2.7 Access Rights

Defining access rights in a RACS4 type system consists in determining a user access to particular Access Zones as well as defining Schedules. Shortly, access control process definition is as follows

- Assigning users to Groups
- Defining Access Zones (assigning terminals to particular Access Zone)
- Defining Schedules
- Linking user Groups to Access Zones and Schedules. In that stage administrator specifies Schedules (hours, days) for users gaining access to particular Access Zones
- Configuring other access control mechanisms (e.g. Door Modes, Inputs, Function Keys, APB Zones and more)

Access granting procedure by a controller is as follows:

- User authentication (login)
- Group identification the user belongs to
- Determining access rights for a given Group to the given Access Zone
- Verifying other access control mechanisms
- Process of granting access by controller is as follows
- User authentication (login)
- Identification of the Group, the user belongs to
- Determining access rights of identified Group to particular Access Zone
- Verifying other access control mechanisms
- Decision on granting the access
- Door lock is released

Note: In RACS4 system, administrator defines who, where and when is granted the access. New user can be assigned to No Access Group and cannot open any door or to No Group and then he is given unlimited 24h/7d access to all Access Zones.

2.7.1 Access Signaling

Whenever a controller grants the access, it activates the LED OPEN , and it remains lit as long as the door lock is released.

2.7.2 Door Lock Control

Typically, there are four methods for the actuator's control:

- applying voltage for the actuator (e.g. door strike)
- removing voltage from the actuator (e.g. magnetic lock)
- applying electric pulse (e.g. barriers)
- triggering servo motor (e.g. motor lock)

Door lock can be controller using the following outputs: **[97]: Entry door lock, [98]: Exit door lock, [99]: Door lock.**

A controller activates the output **[99]** after access granted event on either side of the controlled door (Terminal ID0 or Terminal ID1). **[97]** and **[98]** outputs are activated depending on which side of door the access was granted. In general, **[97]** and **[98]** outputs are used for the rotary gate control where it is important to determine the direction of gate rotation.

As soon as user is granted the access, door is unlocked for the time period determined by the following parameter: Door Unlock Time which may vary from 1 to 99 seconds. As an option, the door lock control can be accomplished using the latch mode (Door Unlock Time=00). In such case, the door is unlocked till another access grant event occurs.

2.7.3 Option: Access Disabled when Controller Armed

As long as the option is activated, a controller may grant access to a room only when it remains in disarmed mode. If armed, user access is denied to all users regardless of their access rights to that room/access controlled area. The purpose of this option is to enable users, who can arm/disarm to deny/grant access for the other users. This option overrides scheduled settings.

2.7.4 Option: Door Lock Controlled in Latch Mode (toggle)

When activated, every access granting event switches the door lock into the opposite state (locked or unlocked). The door lock remains in that state till access is granted again. If the option is not checked then door lock is activated only for the time period determined by the following parameter: Door Unlock Time. Once the specified time interval elapses, the output returns automatically to the previous state.

2.7.5 Option: Auto-relock mode

The Auto-relock function can be used effectively only if a controller is connected to door opening detector (door contact). This function allows for advanced door lock control. Normally, when Auto-relock function is disabled controller unlocks door for the entire Door Unlock Time. With Auto-relock option active, this can be changed depending on one of two possible selections:

- Deactivate a door lock upon door opening detection
- Activate door lock upon door closing detection.

In first case controller will de-energize door lock as soon as it recognizes that door has been opened. In second case controller will re-energize door lock as soon as it recognizes that door is closed. This first scenario is usually used for door locks which unblock door upon energizing (e.g. door strike). While, second is used for door locks which unblock doors upon de-energizing (e.g. magnetic lock).

2.7.6 Facility Code

Facility Code (also called: Site Code) is a part of the whole proximity card code which is located between 16th and 24th bit and is intended to characterize some group of cards customized and produced for individual order.

Example: If the card has following code (presented in binary form):

0001000000000000111011100010001010110111

the underline digits 11101110 are treated as Facility Code.

Proximity cards and key fobs provided by Roger have card code printed in two forms: full card code in decimal system e.g. 68735083191 and reduced code which is generated from the first 24 bits of the full card code. This reduced code is presented as three decimal digits (from range 000-255) separated by comma from remaining 5 digits e.g. 238,08887. As a result the first 3 decimal digits before comma correspond to card Facility Code.

When Facility Code option is active, controller grants the access to all users with the same Facility Code. Thanks to this feature controller can be used to grant access to larger number of cardholders whose cards comply to a given Facility Code.

Also, the group of cards with particular Facility Code can be assigned to specific User Groups, thus all users with the same Facility Code will have the same access rights. Moreover, special options can be assigned to Facility (see 2.3.2 User Options).

2.7.7 Option: Disable PIN under duress

By default, the option 'Disable PIN under duress' is inactive. When the option is inactive, controller will assume that entry of the PIN code which differs by 1 from the valid PIN is under duress. In such case door shall be unlocked and FORCED ENTRY state shall be signaled.

Example: The correct PIN is [4569][#]. Codes [4568][#] or [4560][#] are treated as entry attempt under duress.

Note: To ensure correct operation of duress option, all PINs in the system need to differ by more than one. The PR Master software verifies that condition and informs of any exceptions to that rule. The option can also be switched off and then the system will allow for arbitrary PIN assignments.

2.7.8 Option: Hotel room

If the option is activated then manual programming of the User Commands (see 3.2 User Commands) and Function Cards (see 2.11 Function Cards) is disabled.

2.7.9 System Flags

System Fags or simply Flags are logic states in a controller's memory corresponding to certain conditions/events related to controller. Some of the flags are predefined for particular purposes (LIGHT, TAMPER, INTRUDER), whereas other are fairly universal and can be used for arbitrary user-defined purposes (AUX1, AUX2).

Initially, every flag is switched off. Flags can only be switched on upon certain system events/conditions. Flag returns to previous states autonomously after a preset time interval elapsed or after specific event took place forcing the flag to return to deactivated state.

Flag activation time is determined by a relevant timer. Some of the flag timers can be set into a bi-state type mode (latch mode) – in this mode flag state changes permanently till occurrence of particular event.

Table 6: System flags		
Flag	Flag activation	Flag deactivation
AUX1	Function Cards: [FP12]: Set AUX1 [FP14]: Toggle AUX1 Inputs: [71]: Set AUX [73]: Toggle AUX1 Function keys: [71]: Set AUX1 [73]: Toggle AUX1	Function Cards: [FP13]: Clear AUX1 [FP14]: Toggle AUX1 Inputs: [72]: Clear AUX1 [73]: Toggle AUX1 Function keys: [72]: Clear AUX1 [73]: Toggle AUX1 Flag is also switched off after elapsed time of respective Timer
AUX2	Function Cards: [FP20]: Set AUX2 [FP22]: Toggle AUX2 Inputs: [74]: Set AUX2 [76]: Toggle AUX2 Function Keys: [74]: Set AUX2 [76] Toggle AUX2	Function Cards: [FP21]: Clear AUX2 [FP22]: Toggle AUX2 Inputs: [75]:Clear AUX2 [76]: Toggle AUX2 Function Keys: [75]: Clear AUX2 [76]: Toggle AUX2 Flag is also switched off after elapsed time of respective Timer
LIGHT	Function Cards: [FP15]: Set LIGHT [FP17]: Toggle LIGTH Inputs: [68]: Set LIGHT	Function Cards: [FP16]: Clear LIGHT [FP17]: Toggle LIGHT Inputs: [69]: Clear LIGHT

	[70]: Toggle LIGHT Function Keys: [78]: Set LIGHT [70]: Toggle LIGHT	[70]: Toggle LIGHT Function Keys: [69]: Clear LIGHT [70]: Toggle LIGHT Flag is also switched off after elapsed time of respective Timer
TAMPER	Input: [08]: Tamper	Controller disarming Flag is also switched off after elapsed time of respective Timer
INTRUDER	Inputs: [09]: Intruder [08]: Tamper Function Key: [09]: Intruder	Controller disarming Flag is also switched off after elapsed time of respective Timer
DURESS	Entering of PIN under duress (see Facility Code (also called: Site Code) is a part of the whole proximity card code which is located between 16th and 24th bit and is intended to characterize some group of cards customized and produced for individual order. <i>Example: If the card has following code (presented in binary form):</i> <i>0001000000000000<u>11101110</u>0010001010110111</i> <i>the underline digits 11101110 are treated as Facility Code.</i> Proximity cards and key fobs provided by Roger have card code printed in two forms: full card code in decimal system e.g. 68735083191 and reduced code which is generated from the first 24 bits of the full card code. This reduced code is presented as three decimal digits (from range 000-255) separated by comma from remaining 5 digits e.g. 238,08887. As a result the first 3 decimal digits before comma correspond to card Facility Code. When Facility Code option is active, controller grants the access to all users with the same Facility Code. Thanks to this feature controller can be used to grant access to larger number of cardholders whose cards comply to a given Facility Code. Also, the group of cards with particular Facility Code can be assigned to specific User Groups, thus all users with the same Facility Code will have the same access rights. Moreover, special options can be assigned to Facility (see 2.3.2 User Options).	Flag is switched off after elapsed time of respective Timer

	2.7.7 Option: Disable PIN under duress)	
TROUBLE	Inputs: [05]: AC lost [06]: Low battery Loss of connection with XM-2 I/O extension module	Controller disarming Flag is also switched off after elapsed time of respective Timer
ENTRY DELAY	Input: [15] Intruder - delayed	Controller disarming Flag is also switched off after elapsed time of respective Timer
EXIT DELAY	Controller arming	Controller disarming Flag is also switched off after elapsed time of respective Timer
CARD PRESENT – SWITCH OFF DELAY	Removal of proximity card (any or authorized) from card holder of PR621-CH controller	Flag is switched off after elapsed time of respective Timer

2.7.10 Door Alarm

The PRxx1 controllers have been designed to detect and indicate a so called Door Alarm which consists of three states:

- PREALARM
- DOOR AJAR
- FORCED ENTRY

Door Alarm can be signaled at dedicated output lines and internal buzzer (option). Each alarm is signaled on separate output or alternatively the same output can be configured to signal two or even three mentioned above states. For Door Alarm signaling PRxx1 series controller uses different signal modulation in output line and/or buzzer, depending on alarm type (see table below). If more than one alarm is triggered, the unit indicates the alarm with the highest priority.

Table 7: Door Alarms			
Alarm Type	Description	Priority	Signaling method
PREALARM	Started after five consecutive entries of unknown identifier (card/PIN) within five minutes.	Low	Single pulses repeated periodically every 2 s.
DOOR AJAR	Started when a door is not closed within a preset time interval i.e. Door Open Timeout.	Medium	Two pulses repeated periodically every 2 s.
FORCED ENTRY	Started upon detection of unauthorized door opening or PIN under duress input (see Facility Code (also called: Site Code) is a part of the whole proximity card code which is located between 16 th and 24 th bit and is intended to characterize some group of cards customized and produced for individual order. <i>Example: If the card has following code</i>	High	Single 1 sec. pulses repeated periodically every 1 second.

	<i>(presented in binary form):</i> <i>0001000000000000<u>11101110</u>0010001010110111</i> <i>the underline digits 11101110 are treated as Facility Code.</i> Proximity cards and key fobs provided by Roger have card code printed in two forms: full card code in decimal system e.g. 68735083191 and reduced code which is generated from the first 24 bits of the full card code. This reduced code is presented as three decimal digits (from range 000-255) separated by comma from remaining 5 digits e.g. 238,08887. As a result the first 3 decimal digits before comma correspond to card Facility Code. When Facility Code option is active, controller grants the access to all users with the same Facility Code. Thanks to this feature controller can be used to grant access to larger number of cardholders whose cards comply to a given Facility Code. Also, the group of cards with particular Facility Code can be assigned to specific User Groups, thus all users with the same Facility Code will have the same access rights. Moreover, special options can be assigned to Facility (see 2.3.2 User Options).		
	2.7.7 Option: Disable PIN under duress).		

2.7.11 Option: Enable Door Alarm signaling on internal buzzer

When the option is active, any of following alarm states: PREALARM, DOOR AJAR and FORCED ENTRY is signaled by internal buzzer.

PREALARM is started after five consecutive entries of incorrect identifier (card/PIN) within five minutes. PREALARM can be signaled at following outputs: **[01]: Prealarm, [03]: Prealarm + Door Ajar, [05]: Prealarm + Forced Entry or [07] Prealarm + Door Ajar + Forced Entry.**

The option is not available in PR411DR as it does not contain buzzer.

2.7.12 Option: Device temporary blocked after 5 wrong logins

When the option is active and PREALARM is started then entering of cards and/or PINs at that controller is blocked for 5 minutes.

2.7.13 Option: Constant activation of Output 1 by card in vicinity of reader

When the option is checked then Output 1 (REL1) is active (associated door is opened) as long as authorized proximity card is in vicinity of the controller with built in reader. If the card is removed then the Output 1 is released with delay specified by Door Unlock Time.

2.7.14 Anti-passback (APB)

When anti-passback function is active then user can log either on entry or exit reader however every next time he must login on opposite side of the given door. Following types of anti-passbacks are available:

- Soft anti-passback (Soft APB)
- Hard anti-passback (Hard APB)

When Soft APB is selected controller grants access despite of violation of APB rule but such violation is reported in the system. When Hard APB is selected then violation of APB rule will cause rejection of access at that controller for particular user (two long acoustic signals) and such event will be reported within system.

Option: True APB

When option True APB is active controller assumes that user entered/left only if door opening is detected. If access is granted but the door opening is not detected then anti-passback status remains unchanged. True APB requires installation of door contact to monitor actual door opening.

APB Reset Time

Two times per day, APB Register can be cleared and set to default values. In such case all users logged at particular controller acquire Not logged status. This functionality is available only for Network Systems (see 2.1.2 Network System (with CPR32-SE)).

Note: Once the APB Register is cleared all users have Not logged status and initially they can login either at entry or exit side of the door. After that they must log alternately.

2.7.15 Anti-passback Zones (APB Zones)

An APB Zone is a selected access controlled area with multiple access points (readers). APB Zones incorporate a list of entry readers as well as exit readers. A PRxx1 controller is capable of monitoring only one 2-way passage. Therefore, it needs to be located at a border between 2 APB Zones, where one reader connected to controller monitors the entry to particular APB zone and the other one, monitors the exit from that zone. It is not allowed for readers connected to the same controller to control one entrance to one APB Zone.

Note: A PRxx1 controller located at the APB Zone border is not required to feature two readers. APB zone entrance and exit can be controlled by two access controllers, respectively.

Every RACS4 access control system incorporates predefined Public APB Zone. The public zone is defined as an area surrounding the access system. Assuming an access control system to be located in a building, every user leaving it enters the public zone and vice versa.

Note: In RACS4 system, controllers defining particular APB zone must be incorporated in one Network. APB Zone cannot be defined by means of controllers from various access Networks.

APB Register

The APB Register is located in controller memory and it keeps information about the latest logging of each user (ID0 or ID1 terminal). Following records are assigned in APB Register to all users:

Table 8: APB Status	
Type	Description
Logged on Terminal ID0	Recently, user logged at Terminal ID0
Logged on Terminal ID1	Recently, user logged at Terminal ID0
Logged OFF	The location of last login is missing. In such a case user can log either on Terminal ID0 or Terminal ID1 of passage or APB Zone.
Disabled	Access to the APB Zone for user with Disabled status shall be denied at every terminal until the status is changed.

APB Reset

The APB Reset clears APB Register and sets Logged OFF Status (see Table 8) for all users. Once the reset procedure is completed, the users may attempt to log either at Terminal ID0 or Terminal ID1. Obviously after that alternate logging at door entry or exit is required.

APB Reset is conducted automatically on system start-up (power on), but APB Reset procedure can also be accomplished in accordance with following means:

- Input line **[60]: APB Register reset**
- Function key **[60]: APB Register reset**
- Remotely from managing PC (PR Master software)
- Automatically from Schedule (only Network Systems, see 2.1.2 Network System (with CPR32-SE))

Hierarchy of APB Zones

APB Zone Hierarchy reflects relationships between various APB Zones within one particular access Network. In access control systems with activated global ABP, users are allowed to re-locate only within neighboring APB Zones. Neighboring APB Zones are zones with adjacent passages. As a result, the access control system permits users to move from one APB Zone to another one through the neighboring/adjacent zones only. The APB Hierarchy can be switched on/off by means of PR Master software. With the APB Hierarchy switched off, users are allowed to leave their APB Zone and enter another one. In such case, APB Zones are not required to be adjacent to each other.

Note:

1. The term passage refers to a controller located at a border of two ABP Zones.
 2. Neighboring APB Zones are zones with passage.
 3. The Hierarchy of APB Zones is determined automatically by assignment of readers to particular ABP Zones in a system. The Hierarchy can be modified only by modification of reader assignment structure, i.e., by assigning readers to other APB Zones.
-

2.7.16 Alarm Zones

Alarm Zone is a group of controllers, which change their Armed/Disarmed Modes concurrently. If any controller within particular Alarm Zone changes its Armed/Disarmed mode, then the remaining controllers follow such change. It is not relevant what made the controller to change its Armed/Disarmed Mode. The concurrent arming/disarming is executed by CPR-32SE network controller, which continuously monitors Armed/Disarmed Modes of all access controllers within an Alarm Zone. As a result, all controllers within one Alarm Zone maintain the same Armed/Disarmed Mode at any time.

Note: Alarm Zones do not block other methods for changing Armed/Disarmed Mode.

If arming/disarming is controlled by means of input line **[03]: Disarmed mode (toggle switch)** then the current mode at controller cannot be changed remotely (including CPR32-SE). Such controller can be still a part of an Alarm Zone, however, its Armed /Disarmed Mod is not subject to any CPR32-SE based controls and it depends exclusively on input line **[03]**.

Alarm Zone Hierarchy

RACS4 access control system can incorporate at least one Alarm Zone. Zones can operate independently, or they can be arranged into a hierarchic structure. In case of independent Alarm Zones, any change of Armed/Disarmed Mode within one zone do not affect other zones. Hierarchic structures may adopt master/slave type relationship between corresponding alarm zones. In such case following rules are valid:

- Arming a master zone makes all slave zones armed
- Disarming a master zone does not affect slave zones mode
- Arming a slave zone does not make the master zone armed
- Disarming a slave zone does not make the master zone disarmed

The Alarm Zone Hierarchy in RACS4 system is in the form of tree structure. The structure reflects mutual relationships and dependencies between all Alarm Zones.

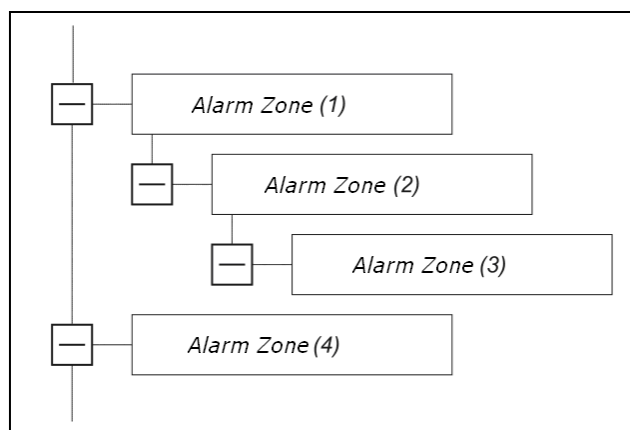


Figure 8 Example of Alarm Zones Hierarchy

In the above example, the zone no. 4 is independent of all other Alarm Zones. The Alarm Zone 1 is a master zone for the Alarm Zone 2 and Alarm Zone 3, whereas the Alarm Zone 3 is a slave zone for the zone 2 and 1. Arming of zone 1 causes zones 2 and 3 to be armed accordingly. Finally, arming the zone 2 arms the zone 3, etc.

2.8 Inputs

Controller PR411DR has eight input lines (IN1...8), whereas other controllers of PRxx1 series (PR311SE, PR611 and PR621) have three input lines (IN1...3). As an option additional two input lines can be provided by connection of XM-2 extension module. Each input line can be configured as normally opened (NO) or normally closed (NC). The normally open line becomes triggered when shorted to ground (supply minus), while normally closed line is triggered when disconnected from ground (supply minus). Internally, each input is pulled up to supply plus through 15kΩ resistor. The average threshold voltage between low and high logical level is around 3V in respect to ground (supply minus). All input lines can be programmed to following functions:

Table 9: Input functions		
Code	Name	Function
[00]	None	Input line can be switched to [00] if it is not used
[01]	Door contact	The input is dedicated to connection of door contact and monitoring of door opening. If the line is triggered then controller detects that door is opened, otherwise the door is closed
[02]	Exit button	When the input line is triggered then controller activates door lock and grants normal access. This input line can be connected to exit button
[03]	Disarmed mode (toggle)	When the input line is activated then controller is switched to Disarmed Mode and when not activated then controller remains in Armed Mode. Only one such input can be defined in controller. If the input line is selected then other methods for arming/disarming are disabled
[04]	AUX	This input line is used only for reporting events (activated, not activated)

[05]	AC lost	This input line is used for reporting the event and triggering TROUBLE flag (see 2.7.9 System Flags)
[06]	Low battery	This input line is used for reporting the event and triggering TROUBLE flag (see 2.7.9 System Flags)
[07]	Door bell	When the input line is active then bell sound is emitted by internal buzzer and optionally output line [15] Door bell is activated
[08]	Tamper	Activation at this input line is interpreted as sabotage and TAMPER flag is triggered (see 2.7.9 System Flags)
[09]	Intruder	Activation at this input line is interpreted as signal from alarm detector and INTRUDER flag is triggered (see 2.7.9 System Flags)
[11]	Access disabled	When the input line is active then the controller completely disables the access
[13]	Arming disabled	When the input line is active then the controller cannot be armed
[14]	Door lock switch	When the input line is active then the controller unconditionally unlocks door i.e. it activates door lock switch
[15]	Intruder-delayed	When in Armed Mode triggering of this input starts ENTRY DELAY timer. If controller disarming does not occur within elapsed time then INTRUDER flag is activated
[60]	APB Register reset	When the input line is activated then APB Register Reset occurs (see 2.7.15 Anti-passback Zones (APB Zones)) and all users are assigned Not Logged status (see Table 8)
[61]	Arm/Disarm switch (momentary)	The input line is used for switching between Armed and Disarmed Modes (see 2.6 Armed and Disarmed Modes)
[64]	Normal door mode	The input line is used for switching the controller into Normal Door Mode (see 2.5 Door Modes)
[65]	Unlocked door mode	The input line is used for switching the controller into Unlocked Door Mode (see 2.5 Door Modes)
[66]	Cond. Unlocked door mode	The input line is used for switching the controller into Cond. Unlocked Door Mode (see 2.5 Door Modes)
[67]	Locked door mode	The input line is used for switching the controller into Locked Door Mode (see 2.5 Door Modes).
[68]	Set LIGHT	When the input line is activated then LIGHT flag is switched on and respective Timer counts down (see 2.7.9 System Flags)
[69]	Clear LIGHT	When the input line is activated then LIGHT flag is switched off and respective Timer is cleared (see 2.7.9 System Flags)
[70]	Toggle LIGHT	The input line is used for switching LIGHT flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[71]	Set AUX1	When the input line is activated then AUX1 flag is switched on and respective Timer counts down (see 2.7.9 System Flags)
[72]	Clear AUX1	When the input line is activated then AUX1 flag is switched off and respective Timer is cleared (see 2.7.9 System Flags)

[73]	Toggle AUX1	The input line is used for switching AUX1 flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[74]	Set AUX2	When the input line is activated then AUX2 flag is switched on and respective Timer counts down (see 2.7.9 System Flags)
[75]	Clear AUX2	When the input line is activated then AUX2 flag is switched off and respective Timer is cleared (see 2.7.9 System Flags)
[76]	Toggle AUX2	The input line is used for switching AUX2 flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[78]	Disarmed mode (momentary)	When the input line is activated then the controller is switched to Disarmed Mode (see 2.6 Armed and Disarmed Modes)
[79]	Armed mode (momentary)	When the input line is activated then the controller is switched to Armed Mode (see 2.6 Armed and Disarmed Modes)
[80]	Card or PIN mode	The input line is used for setting Identification Mode (see 2.4 Identification Modes) into Card or Pin
[81]	Card only mode	The input line is used for setting Identification Mode (see 2.4 Identification Modes) into Only Card
[82]	PIN only mode	The input line is used for setting Identification Mode (see 2.4 Identification Modes) into Only PIN
[83]	Card and PIN mode	The input line is used for setting Identification Mode (see 2.4 Identification Modes) into Card and PIN

Note: You can assign only one input line to the following functions: **[01] Door contact**, **[03] Disarmed mode (toggle)**, **[05] AC lost** or **[06] Low battery**. Once the given line is programmed to one of mentioned functions, then no other input line can be programmed to that particular function.

2.9 Outputs

All controllers of PRxx1 series (except for PR411DR) have one relay output (REL1) and two transistor outputs IO1 and IO2. The PR411DR has additional relay output (REL2). As an option two additional output lines can be provided by connection of XM-2 extension module. When not triggered the IO1 and IO2 outputs represent high impedances and when triggered they short to the ground. Moreover, when controller doesn't work with external reader nor XM-2 extension module then its CLK and DTA lines can be used as standard outputs. All output lines can be programmed to following functions:

Note: PR411DR controller has additional relay output (REL2) which can be programmed in the same way as any other controller output.

Table 10: Output functions		
Code	Name	Function
[00]	Disarmed mode	The output line is inactive when the controller is in Armed Mode and active when the controller is in Disarmed Mode (see 2.6 Armed and Disarmed Modes)
[01]	Prealarm	The output is used for signaling PREALARM (see 2.7.10 Door Alarm)

[02]	Door Ajar	The output is used for signaling DOOR AJAR (see 2.7.10 Door Alarm)
[03]	Prealarm + Door Ajar	The output is used for signaling PREALARM + DOOR AJAR (see 2.7.10 Door Alarm)
[04]	Forced Entry	The output is used for signaling FORCED ENTRY (see 2.7.10 Door Alarm)
[05]	Prealarm + Forced Entry	The output is used for signaling PREALARM + FORCED ENTRY (see 2.7.10 Door Alarm)
[06]	Door Ajar + Forced Entry	The output is used for signaling DOOR AJAR + FORCED ENTRY (see 2.7.10 Door Alarm)
[07]	Prealarm +Door Ajar + Forced Entry	The output is used for signaling PREALARM + DOOR AJAR + FORCED ENTRY (see 2.7.10 Door Alarm)
[09]	Access granted	The output line is activated whenever the controller grants the access. The time can be set by means of Door Unlock Time parameter
[10]	Door status	The output line is activated when the door is opened and remains active as long as the door is opened. The output line practically transmits signals from door contact i.e. from [01] Door contact input line
[11]	Access denied	The output line is activated for 2 seconds every time the controller denies the access
[14]	User logged on term. ID0	Once the user has been identified at terminal ID0 this output switches to active state and remains active until identification at terminal ID1. This function may be used for control of tripod or two way passage (where it shows direction of passage)
[15]	Door bell	The output line is activated for 2 sec. when door bell is triggered. Door bell can be triggered by means of Function Key or Input line
[18]	Normal door mode	The output line is active as long as the controller operates in Normal Door Mode (see 2.5 Door Modes)
[19]	Unlocked door mode	The output line is active as long as the controller operates in Unlocked Door Mode (see 2.5 Door Modes)
[20]	Cond. Unlocked door mode	The output line is active as long as the controller operates in Cond. Unlocked Door Mode (see 2.5 Door Modes)
[21]	Locked door mode	The output line is active as long as the controller operates in Locked Door Mode (see 2.5 Door Modes)
[25]	Pulse upon disarming	The output line is activated for 2 sec. when the controller switches to Disarmed Mode (see 2.6 Armed and Disarmed Modes)
[26]	Pulse upon arming	The output line is activated for 2 sec. when the controller switches to Armed Mode (see 2.6 Armed and Disarmed Modes)
[37]	AC failure	The output line is active if AC power supply failure lasts for more than 6 minutes. Signaling at the output line is ceased after approx. 1 minutes from AC power supply recovery. The function is available in PR411DR controller only

[38]	Low battery	The output line is active if battery voltage drops below 11,7V for at least 8 minutes. Signaling at the output line is ceased after approx. 6 minutes from AC power supply recovery. The function is available in PR411DR controller only
[64]	LIGHT	The output line signals actual state of LIGHT flag. The output is active when flag is on and the output is inactive when flag is off (see 2.7.9 System Flags)
[65]	Tamper Alarm	The output line signals actual state of TAMPER flag. The output is active when flag is on and the output is inactive when flag is off
[66]	AUX1	The output line signals actual state of AUX1 flag (see 2.7.9 System Flags)
[67]	AUX2	The output line signals actual state of AUX1 flag (see 2.7.9 System Flags)
[68]	Intruder Alarm	The output line signals actual state of INTRUDER flag (see 2.7.9 System Flags)
[69]	Duress Alarm	The output line signals actual state of DURESS flag (see 2.7.9 System Flags)
[70]	Trouble Alarm	The output line signals actual state of TROUBLE flag (see 2.7.9 System Flags)
[71]	Entry Delay	The output line is active as long as ENTRY DELAY timer is counting down (see 2.7.9 System Flags)
[72]	Exit Delay	The output line is active as long as EXIT DELAY timer is counting down (see 2.7.9 System Flags)
[73]	Proximity card present	The output line is active as long as any EM125kHz (UNIQUE) standard card is present in card holder of PR-621-CH controller plus the time specified by means of timer CARD PRESENT – SWITCH OFF DELAY. The function is also available in PR311SE, PR611 and PR621 controllers.
[74]	Authorized proximity card present	The output line is active as long as EM125kHz (UNIQUE) standard card of user with access rights is present in card holder of PR621-CH controller plus the time specified by means of timer CARD PRESENT – SWITCH OFF DELAY. The function is also available in PR311SE, PR611 and PR621 controllers..
[80]	Card or PIN mode	The output line is active when Card or PIN Identification Mode at the controller is active (see 2.4 Identification Modes).
[81]	Card only mode	The output line is active when Card Only PIN Identification Mode at the controller is active (see 2.4 Identification Modes).
[82]	PIN only mode	The output line is active when PIN Only Identification Mode at the controller is active (see 2.4 Identification Modes).
[83]	Card and PIN mode	The output line is active when Card and PIN Identification Mode at the controller is active (see 2.4 Identification Modes).

[97]	Entry door lock	The output is triggered for the time specified by means of Door Unlock Time parameter if access is granted from ID0 Terminal. The output is intended for two way passages where distinguishing of passage direction is required (e.g. rotary gate) (see 2.7.2 Door Lock Control)
[98]	Exit door lock	The output is triggered for the time specified by means of Door Unlock Time parameter if access is granted from ID1 Terminal. The output is intended for two way passages where distinguishing of passage direction is required (e.g. rotary gate), (see 2.7.2 Door Lock Control)
[99]	Door lock	The output is triggered for the time specified by means of Door Unlock Time parameter regardless of Terminal at which the access is granted. This is the standard output used for door unlocking in most applications, (see 2.7.2 Door Lock Control)

2.10 Function Keys

Function Keys are available at some PRT readers (Roger) and at PR311SE controller. User can operate four Function Keys (if they are available at the keypads of Terminals ID0 and ID1), or two Function Keys (if they are available at the keypad of Terminal ID0 or ID1). In RACS4 system it does not matter if the Function Key is located at Terminal ID1 or ID0, as they can be programmed individually in the same way by means of functions specified in Table 11.

Table 11: Function keys		
Code	Name	Function
[00]	No function	No function is assigned to that key
[01]	Door bell	The key activates door bell.
[02]	Release door	The key releases door lock and door is opened as in case of standard access granting
[04]	Key pressed (event only)	Each use of key is only registered in event log. No other action assigned to that function
[09]	Intruder alarm	The key activates INTRUDER flag (see 2.7.9 System Flags)
[60]	APB Register Reset	The key resets APB Register (see 2.7.15 Anti-passback Zones (APB Zones))
[61]	Armed/Disarmed mode	The key switches the controller between Armed and Disarmed Modes. The mode shall not be switched unconditionally i.e. it shall be switched if other rules set by user do not block it.
[64]	Set Normal Door Mode	They key is used for switching the controller into Normal Door Mode (see 2.5 Door Modes)
[65]	Set Unlocked Door Mode	They key is used for switching the controller into Unlocked Door Mode (see 2.5 Door Modes)
[66]	Set Cond. Unlocked Door Mode	They key is used for switching the controller into Cond. Unlocked Door Mode (see 2.5 Door Modes)
[67]	Set Locked Door Mode	They key is used for switching the controller into Locked Door Mode (see 2.5 Door Modes)

[68]	Set LIGHT	The key switches LIGHT flag on (see 2.7.9 System Flags)
[69]	Clear LIGHT	The key switches LIGHT flag off (see 2.7.9 System Flags)
[70]	Toggle LIGH	The key is used for switching LIGHT flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[71]	Set AUX1	The key switches AUX1 flag on (see 2.7.9 System Flags)
[72]	Clear AUX1	The key switches AUX1 flag off (see 2.7.9 System Flags)
[73]	Toggle AUX1	The key is used for switching AUX1 flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[74]	Set AUX2	The key switches AUX2 flag on (see 2.7.9 System Flags)
[75]	Clear AUX2	The key switches AUX2 flag off (see 2.7.9 System Flags)
[76]	Toggle AUX2	The key is used for switching AUX2 flag to opposite state i.e. ON/OFF (see 2.7.9 System Flags)
[78]	Set Disarmed Mode	When the key is pressed then the controller is switched to Disarmed Mode (2.6 Armed and Disarmed Modes)
[79]	Set Armed Mode	When the key is pressed then the controller is switched to Armed Mode (2.6 Armed and Disarmed Modes)
[80]	Set Card or PIN mode	The key is used for setting Identification Mode (see 2.4 Identification Modes) into Card or PIN.
[81]	Set Card Only mode	The key is used for setting Identification Mode (see 2.4 Identification Modes) into Card Only.
[82]	Set PIN Only mode	The key is used for setting Identification Mode (see 2.4 Identification Modes) into PIN Only.
[83]	Set Card and PIN mode	The key is used for setting Identification Mode (see 2.4 Identification Modes) into Card and PIN.

2.11 Function Cards

Function Cards are standard proximity cards with assigned specific programming functions. Function Cards can be defined manually (see III. Programming) or from PC by means of PR Master software. Only one programming function can be assigned to particular Function Card. Following programming functions are available:

- Function [01]: Register NORMAL card (see 2.3 Users)
- Function [03]: Register SWITCHER FULL card (see 2.3 Users)
- Function [05]: Register SWITCHER LIMITED card (see 2.3 Users)
- Function [06]: Delete card
- Function [07]: Delete all cards
- Function [08]: Set door to Normal Mode (see 2.5 Door Modes)
- Function [09]: Set door to Unlocked Mode (see 2.5 Door Modes)
- Function [10]: Set door to Cond.Unlocked Mode (see 2.5 Door Modes)
- Function [11]: Set door to Locked Mode (see 2.5 Door Modes)
- Function [12]: Set AUX1 (see 2.7.9 System Flags)
- Function [13]: Clear AUX1 (see 2.7.9 System Flags)
- Function [14]: Toggle AUX1 (see 2.7.9 System Flags)
- Function [15]: Set LIGHT (see 2.7.9 System Flags)
- Function [16]: Clear LIGHT (see 2.7.9 System Flags)
- Function [17]: Toggle LIGHT (see 2.7.9 System Flags)
- Function [19]: Add multiple cards (see 2.7.9 System Flags)

- Function [20]: Set AUX2 (see 2.7.9 System Flags)
- Function [21]: Clear AUX2 (see 2.7.9 System Flags)
- Function [22]: Toggle AUX2 (see 2.7.9 System Flags)
- Function [24]: Register Guest card ((see 2.3.1 Standard and Guest Users)
- Function [25]: Delete all Guest cards (see 2.3.1 Standard and Guest Users)

III. PROGRAMMING

Controllers of PRxx1 series can be programmed manually by means of keypad or remotely by means of PC with PR Master software. More details on remote programming can be found in PR Master manual. Manual programming can be executed by means of controller keypad (PR611 and PR311SE) or by means of keypad on PRT reader connected to particular controller (the reader must be equipped with keypad and configured to RACS Clock&Data interface, ID0 Terminal – see 2.2.3 RACS Clock and Data Interface). Manual programming consists in specifying User Commands (see 3.2 User Commands) and entering Installer Programming Mode (see 3.3 Installer Programming Mode). User Functions enable management of cards and/or PINs and they can be used to control some of the controller functions (e.g. Identification Mode, Door Mode). Installer Programming Mode can be used for configuration of the controller, specifying functions for input and output lines as well as other options.

If the access system is managed and programmed from PC it is critical not to use any other of programming method otherwise system behavior can be corrupted because the computer database will be de-synchronized from the settings entered manually.

Note: Installer Programming and User Commands can be entered by means of keypads of both the controller (Terminal ID1) and external reader (Terminal ID0) connected to that controller.

3.1 Memory Reset – Setting MASTER identifier and ID address of the controller

Memory Reset results in clearing of all settings in the controller, restoring defaults and enables setting of new MASTER card and/or PIN as well as new ID address of controller. After Memory Reset, the controller automatically enters normal working mode and Armed Mode (LED STATUS Ⓢ is red).

Note: If MASTER identifier (card and/or PIN) is not set then it is not possible to enter Installer Programming Mode.

Simplified Memory Reset procedure

The procedure allows for specifying MASTER identifier (card) without setting controller ID address.

- Remove CLK and DTA wires from terminals
- Connect CLK wire with DTA wire
- Restart the controller (switch power supply off/on or short RST contacts for a while) – all LED indicators become active
- Disconnect CLK and DTA wires— the LEDs shall be off, and then LED OPEN Ⓢ (green) shall pulsate
- While the LED OPEN Ⓢ is pulsing, read any card at the controller — this will be a new MASTER card
- The controller restarts automatically and switches to normal mode with address ID=00
- Memory Reset procedure is finished and further adjustments (including ID address) can be conducted in Installer Programming Mode (see 3.3 Installer Programming Mode) or by means of User Commands (see 3.2 User Commands)

Simplified Memory Reset procedure for the controller without keypad (PR621 or PR411DR)

The procedure results in clearing the controller settings, programming new MASTER card and setting new ID address for the controller.

- Remove CLK and IN3 wires from terminals
- Connect CLK wire with IN3 wire

- Restart the controller (switch power supply off/on or short RST contacts for a while) – all LED indicators become active
- Disconnect CLK and IN3 wires - the LEDs shall be off, then LED STATUS ⚡ (red) and LED OPEN Ⓢ (green) shall pulsate
- While both LEDs pulsate, read any card at the controller - this will be a new MASTER card. Then controller shall proceed to the next step i.e. setting ID address.
- Read new MASTER card X times where X must be equal to the first digit of the required ID address, then wait for two short acoustic signals (beeps)
- Read new MASTER card Y times where Y must be equal to the second digit of the required ID address
- The controller restarts automatically and switches to normal mode

Full Memory Reset procedure

This procedure can be conducted directly from the controller keypad (if available) or from an additional PRT series reader connected to the controller through CLK and DTA lines. The external reader used for this purpose should be configured to the RACS Clock&Data mode with address ID0 and obviously be equipped with a keypad. Full Memory Reset allows for programming of new MASTER identifier (card and/or PIN) and setting controller ID address.

- Remove CLK and DTA wires from terminals
- Connect CLK wire with DTA wire
- Restart the controller (switch power supply off/on or short RST contacts for a while) – all LED indicators become active
- Disconnect CLK and DTA wires— the LEDs shall be off, and then LED OPEN Ⓢ (green) shall pulsate
- If the controller is not equipped with keypad, connect PRT series reader configured to RACS Clock&Data mode with ID0 address (or ID1 in case of PR411DR) and proceed with further steps by means of that reader. If the controller is equipped with keypad, external reader is not needed
- Enter new MASTER PIN (3-6 digits) followed with the [#] key or skip this step just pressing the [#] key
- Read any card at the controller — this will be a new MASTER card or skip this step just pressing the [#] key
- Enter two digits (in range of 00 to 99) by means of controller keypad – this will be new ID address or skip this step just pressing the [#] key and then default ID=00 shall be set
- The controller restarts automatically and switches to normal mode

Notes:

1. Unless INSTALLER identifier (see 3.3 Installer Programming Mode) is programmed then MASTER identifier can be used instead of INSTALLER identifier (i.e. MASTER = INSTALLER). Therefore MASTER identifier can be used for entering Installer Programming Mode.
 2. Controller address must be in range of ID=00-99
-

In case of PRxx1 series controllers, when setting ID address, it is possible to assign a so called "FixedID" to the controller. This option is particularly useful if there is a risk that someone will accidentally change controller address resulting in disruption of the whole system. The fixed address can be set, changed or cleared only by means of RogerISP software (see Download section at Roger website) during firmware upgrade procedure.

Besides mentioned methods of addressing, the PR411DR controller offers the option to set address by means of programming jumpers. The whole range of possible address is 0-127. If controller address is set in range of 0-99 then it cannot be changed neither by means of PR Master nor manually. It can be modified only if jumper address is set above 99. For details regarding various address settings refer to the relevant Installation Guide.

3.2 User Commands

In case of PRxx1 series controllers, User Commands are programming functions, which can be entered by means of controller keypad or keypad available at external reader connected to that

controller. User Commands can be entered both in Armed and Disarmed Modes (see 2.6 Armed and Disarmed Modes). By default, each User Command requires MASTER identifier (card or PIN) but this requirement can be cancelled for desired User Commands by means of PR Master software or by means of function [69] in Installer Programming Mode (see 3.3 Installer Programming Mode). Each User Commands is identified with two digit code. Upon entering particular code LED SYSTEM  and LED OPEN  pulsate until command is property entered or any programming error occurs.

Symbols and abbreviations:

<AUTH> - authorization, controller requires adequate identifier. By default MASTER card or PIN can be used. Additionally any other identifier defined by PR Master software or function [69] in Installer Programming Mode can be used for authorization

INSTALLER - INSTALLER identifier (always card or PIN); If INSTALLER identifier is not defined then use MASTER identifier instead.

MASTER - MASTER identifier (card or PIN)

[NNN] – Three digit user ID=001..999 (see 2.3 Users)

<Card> - proximity card read or its code entered by means of keypad and followed with [#] key.

<PIN> - PIN (3 – 6 digits) always followed with [#] key

(SK) - prompt acoustic signal (two beeps), encourages user to continue entering of particular command i.e. card read, code entering or key pressing

OK – acoustic signals (three very short beeps), usually used for confirming successful entering of the whole command

Error – error acoustic signal (long beep), informs about error in programming

[10#] <AUTH> (SK) [10] - Remove all users from controller memory

The command erases all cards and PINS for all users (including Guest users).

[11#] <AUTH> (SK) [NNN] <Card> - Program the card for the user with ID=NNN

Read card shall be assigned to the user with ID=NNN. If particular card is already assigned to another user then controller shall generate Error signal.

[12#] <AUTH> (SK) [NNN]<PIN> - Program the PIN for the user with ID=NNN

Entered PIN shall be assigned to the user with ID=NNN.

[13#] <AUTH> (SK) [NNN] - Delete the user with ID=NNN

The user with ID=NNN shall be removed from controller memory.

[14#] <AUTH> (SK) [NNN] - Check if user ID=NNN is available

If neither card nor PIN has been already assigned to user ID=NNN, then OK signal is generated (three very short beeps). If either card or PIN has already been assigned to user ID=NNN then error signal (long beep) is generated.

[15#] <AUTH> (SK) <Card-1>(SK) <Card-2>(SK)...<Card-N> [#] - Program multiple cards

The command enables programming of multiple cards for Normal users. The command should be concluded by means of [#] or else it shall be automatically concluded in 20 seconds after the last card read. New users are assigned the first free IDs in range ID=100...999.

[16#] <AUTH> (SK) [NNN][P] - Set User Option [P] for the user with ID=NNN

Following values of P parameter are available (see also 2.3.2 User Options):

P = [1] Access disabled

P = [2] Enabled for authorization of F1 key at Terminal ID0

P = [3] Enabled for authorization of F2 key at Terminal ID0

P = [4] Enabled for authorization of F1 key at Terminal ID1

P = [5] Enabled for authorization of F2 key at Terminal ID1

P = [6] Authorization for User Commands

P = [7] Authorization for arming/disarming

P = [8] Authorization for Function Cards

[17#] <AUTH> (SK) [NNN][P] - Deactivate User Option [P] for the user with ID=NNN
See command [16] above.

[18#] <AUTH> (SK) [P] - Deactivate User Option [P] for all users
See command [16] above.

[20#] <AUTH> (SK) [20] - Delete all Guest users
The command erases all cards and PINS for all Guest users (see 2.3.1 Standard and Guest Users).

[21#] <AUTH> (SK) [G] <Card> - Program the card for the Guest user with ID=[G]
[G] parameter must be in range 0-7 as it corresponds to Guest ID in range of 4000 – 4007 (see 2.3.1 Standard and Guest Users).

[22#] <AUTH> (SK) [G]<PIN> - Program the PIN for Guest user with ID=[G]
[G] parameter must be in range 0-7 as it corresponds to Guest ID in range of 4000 – 4007 (see 2.3.1 Standard and Guest Users).

[23#] <AUTH> (SK) [G] - Delete Guest user with ID=[G]
[G] parameter must be in range 0-7 as it corresponds to Guest ID in range of 4000 – 4007 (see 2.3.1 Standard and Guest Users).

[31#] <AUTH> (SK) [F] - Define AUX1 flag
Enter: [F] = [0] to clear the flag, [F] = [1] to set the flag or [F] = [2] to toggle the flag to opposite state (see 2.7.9 System Flags)

[32#] <AUTH> (SK) [F] - Define AUX2 flag
Enter: [F] = [0] to clear the flag, [F] = [1] to set the flag or [F] = [2] to toggle the flag to opposite state (see 2.7.9 System Flags).

[33#] <AUTH> (SK) [F] - Define LIGHT flag
Enter: [F] = [0] to clear the flag, [F] = [1] to set the flag or [F] = [2] to toggle the flag to opposite state (see 2.7.9 System Flags).

[34#] <AUTH> (SK) [T] - Define Door Mode
Following values of [T] parameter are available (see also 2.5 Door Modes):
[T] = [0] Normal Door Mode
[T] = [1] Unlocked Door Mode
[T] = [2] Cond. Unlocked Door Mode
[T] = [3] Locked Door Mode

[35#] <AUTH> (SK) [A] - Define Identification Mode
Enter: [A] = [0] to set Card or PIN, [A] = [1] to set Card Only, [A] = [2] to set PIN Only, [A] = [3] to set Card and PIN. See also 2.4 Identification Modes.

Note: After setting PIN Only Identification Mode, MASTER card cannot be used. Similarly after setting Card Only Identification Mode, MASTER PIN cannot be used.

[39#] <AUTH> - Set INTRUDER flag
The command is used for activation of INTRUDER flag (see 2.7.9 System Flags).

3.3 Installer Programming Mode

The mode enables detailed configuration of the controller in order to adapt it to specific requirements at site. This is the manual programming (keypad), opposite to remote programming by means of PR Master software. Installer Programming can be started both in Armed and Disarmed Modes (see 2.6 Armed and Disarmed Modes) by means of following command:

[01#] (SK) <MASTER> (SK) <INSTALLER> - Entry to Installer Programming Mode

Applied abbreviations and symbols are explained in 3.2 User Commands. Upon entering Installer Programming Mode, LED SYSTEM  (orange) and LED STATUS  (red) are switched on. When any key is pressed then both LEDs pulsate until command is properly entered or any programming error occurs. In case of error, the controller remains in Installer Programming Mode and long acoustic signal is generated and both mentioned LEDs cease to pulsate. If command is entered correctly then the controller generates OK signal (three short acoustic signals), both mentioned LEDs cease to pulsate and the controller remains in Installer Programming Mode. Upon exiting the Installer Programming Mode, the controller returns to previous Armed or Disarmed Mode (see 2.6 Armed and Disarmed Modes). The controller exits Installer Programming Mode automatically after 4 minutes if no key is pressed or instantly if following command is entered:

[00#] - Exit from Installer Programming Mode

Installer Programming Mode is exited instantly

[40][MN] - Program the controller address (ID address)

Instead of [MN] enter required digits corresponding to the controller ID address (in range of 00-99). Default value: <ID=00> or other value entered during Memory Reset (see 3.1 Memory Reset – Setting MASTER identifier and ID address of the controller).

[41][P][FW] - Program the function for IN1 input line

[P] parameter specifies type of the input line i.e.: [P]=0 for NO (normally opened) or [P]=1 for NC (normally closed). [FW] parameter specifies function of the input line (see 2.8 Inputs). Default values: <FW=01>, [P] = 1.

[42][P][FW] - Program the function for IN2 input line

See command [41]. Default values: <FW=02>, [P] = 0.

[43][P][FW] - Program the function for IN3 input line

See command [41]. Default values: <FW=04>, [P] = 0.

[44][P][FW] - Program the function for IN4 input line (only PR411DR controller)

See command [41]. Default values: <FW=00>, [P] = 0.

[45][P][FW] - Program the function for IN5 input line (only PR411DR controller)

See command [41]. Default values: <FW=00>, [P] = 0.

[46][P][FW] - Program the function for IN6 input line (only PR411DR controller)

See command [41]. Default values: <FW=00>, [P] = 0.

[47][P][FW] - Program the function for IN7 input line (only PR411DR controller)

See command [41]. Default values: <FW=00>, [P] = 0.

[48][P][FW] - Program the function for IN8 input line (only PR411DR controller)

See command [41]. Default values: <FW=00>, [P] = 0.

[49][P][FW] - Program the function for IN1 input line at XM-2 extension module (additional input)

See command [41]. Default values: <FW=00>, [P] = 0.

[50][P][FW] - Program the function for IN2 input line at XM-2 extension module (additional input)

See command [41]. Default values: <FW=00>, [P] = 0.

[51] [FW] – Program the function for REL1 relay output line

[FW] parameter specifies function of the output line (see 2.9 Outputs). Default value: <FW=99>.

[52] [FW] – Program the function for IO1 output line

See command [51]. Default value: <FW=07>.

[53] [FW] - Program the function for IO1 output line

See command [51]. Default value: <FW=00>.

[54] [FW] - Program the function for CLK output line

See command [51]. Default value: <FW=100>.

[55] [FW] - Program the function for DTA output line

See command [51]. Default value: <FW=100>.

Note: CLK and DTA lines are used for connection of PRT reader (Roger) or XM-2 module. If PRT reader or XM-2 extension module is not connected to the controller then CLK and DAT lines can be used as general purpose outputs. See also 2.2.3 RACS Clock and Data Interface.

[56] [FW] – Program the function for REL2 relay output line (only PR411DR controller)

See command [51]. Default value: <FW=07>.

[59] [FW] – Program the function for REL1 at XM-2 extension module (additional output)

See command [51]. Default value: <FW=99>.

[60] [FW] - Program the function for REL2 at XM-2 extension module (additional output)

See command [51]. Default value: <FW=07>.

[61][PP][QQ] - Specify RACS Clock&Data readers connected to the controller

[PP]=[00] – Terminal ID0 with RACS Clock&Data interface is disabled (see 2.2.3 RACS Clock and Data Interface)

[PP]=[01] – Terminal ID0 with RACS Clock&Data interface is enabled (see 2.2.3 RACS Clock and Data Interface)

[QQ]=[00] – Terminal with RACS Clock&Data interface is disabled (see 2.2.3 RACS Clock and Data Interface)

[QQ]=[01] – Terminal with RACS Clock&Data interface is enabled (see 2.2.3 RACS Clock and Data Interface)

[61] [RR][SS] – Specify Wiegand readers connected to the controller (only PR411DR)

[RR]=[xx] – Terminal ID0 with Wiegand interface (see Table 12)

[SS]=[xx] – Terminal ID1 with Wiegand interface (see Table 12)

Table 12. Types of Wiegand transmission modes	
Code = [RR] and [SS]	Wiegand mode
[00]	Reader is disabled
[03]	Wiegand 26..66 bit, transmits PIN (HEX)
[24]	Wiegand 26..66 bit, transmits PIN (BIN)
[04]	Wiegand 26..66 bit, transmits card code
[05]	Wiegand 26..66 bit, transmits user ID (HEX)
[17]	Wiegand 26..66 bit, transmits user ID (BIN)
[15]	Wiegand 26..66 bit, transmits card code or PIN (HEX)
[16]	Wiegand 26..66 bit, transmits card code or PIN (BIN)

[20]	Wiegand 26..66 bit, transmits PIN (HEX), no parity
[25]	Wiegand 26..66 bit, transmits PIN (BIN), no parity
[21]	Wiegand 26..66 bit, transmits card code, no parity
[22]	Wiegand 26..66 bit, transmits user ID (HEX), no parity
[23]	Wiegand 26..66 bit, transmits user ID (BIN), no parity
[18]	Wiegand 26..66 bit, transmits card code or PIN (HEX), no parity

Notes: Enabling RACS terminal ID0, RACS terminal ID1 or XM-2 extension module automatically disables functioning of CLK and DTA lines as general purpose outputs.

Enabling Wiegand terminal ID0 automatically disables functioning of IN1 and IN2 lines as input lines in PR411DR controller while enabling Wiegand terminal ID1 disables IN3 and IN4 lines respectively in PR411DR controller.

[62][X] – Program XM-2 extension module

Enter [X]=0 to disable XM-2 module

Enter [X]=1 to enable XM-2 module

Default value: <X=0>.

[63][OT] – Set Door Unlock Time

[OT] parameter specifies time in seconds for activation of door lock and consequently door opening. [OT] value must be in range of 00-99. If 00 value is entered then door lock operates in latch mode (see 2.7.2 Door Lock Control and 2.7.4 Option: Door Lock Controlled in Latch Mode (toggle)). Default value: <OT=04>.

[64][CT] – Set Door Open Timeout

[CT] specifies time in seconds for door closing or else Door Ajar alarm in output line can be activated (see 2.7.10 Door Alarm). [CT] must be in range of 01-99. The function Door Open Timeout can be used only if door contact is connected. Default value: <CT=09>.

[65][A] – Set Identification Mode

Following values of [A] parameter are available (see also 2.4 Identification Modes):

[A] = [0] to set Card or PIN

[A] = [1] to set Card Only

[A] = [2] to set PIN Only

[A] = [3] to set Card and PIN

[66][F] – Set the option: Device temporary blocked after 5 wrong logins

Enter [F]=0 to disable the option [F]=1 to enable the option. Default value: <F=0>. See also 2.7.12 Option: Device temporary blocked after 5 wrong logins.

[67][F] – Set the option: Disable PIN under duress

Enter [F]=1 to deactivate the option or [F]=0 to activate the option. Default value: <F=0>. See also Facility Code (also called: Site Code) is a part of the whole proximity card code which is located between 16th and 24th bit and is intended to characterize some group of cards customized and produced for individual order.

Example: If the card has following code (presented in binary form):

0001000000000000111011100010001010110111

the underline digits 11101110 are treated as Facility Code.

Proximity cards and key fobs provided by Roger have card code printed in two forms: full card code in decimal system e.g. 68735083191 and reduced code which is generated from the first 24 bits of the full card code. This reduced code is presented as three decimal digits (from range 000-255)

separated by comma from remaining 5 digits e.g. 238,08887. As a result the first 3 decimal digits before comma correspond to card Facility Code.

When Facility Code option is active, controller grants the access to all users with the same Facility Code. Thanks to this feature controller can be used to grant access to larger number of cardholders whose cards comply to a given Facility Code.

Also, the group of cards with particular Facility Code can be assigned to specific User Groups, thus all users with the same Facility Code will have the same access rights. Moreover, special options can be assigned to Facility (see 2.3.2 User Options).

2.7.7 Option: Disable PIN under duress.

[68][F] – Set the option: Auto-relock mode

Enter [F]=0 to disable the option or [F]=1 to enable blocking of door lock upon detection of door opening or [F]=2 to enable blocking of door lock upon detection of door closing. Default value: <F=0>. See also 2.7.5 Option: Auto-relock mode.

[69][NF][F] – Program the authorization for User Commands

[NF] parameter specifies particular User Command in range of 10-39. Enter [F]=0 to disable necessity for authorization <AUTH> of particular User Command or [F]=1 to enable necessity for authorization <AUTH> of particular User Command. Default value for all User Commands: <F=1>. See also 3.2 User Commands.

[69][*][0] - Disable necessity for authorization of all User Commands

The command disables the necessity for authorization <AUTH> of all User Commands.

[69][*][1] - Enable necessity for authorization of all User Commands

The command enables the necessity for authorization <AUTH> of all User Commands.

Note: By default, all User Commands require authorization by means of MASTER or other authorized identifier.

[70][X] – Set the option: Enable Door Alarm signaling on internal buzzer

Enter [X]=0 to disable the option or enter [X]=1 to enable the option. Default value: <X=0>. See also 2.7.11 Option: Enable Door Alarm signaling on internal buzzer

[71][FF][A] – Program the F1 Function Key at ID0 Terminal

[FF] parameter specifies function of the key in range of 66..72. See 2.10 Function Keys for the list of available functions. Enter [A]=0 to disable necessity for authorization of F1 key or enter [F]=1 to enable necessity for authorization of F1 key at ID0 Terminal. Default value: <F=1>.

[72][FF][A] – Program the F2 Function Key at ID0 Terminal

See command [71]. Default value: <F=1>.

[73][FF][A] – Program the F1 Function Key at ID1 Terminal

See command [71]. Default value: <F=1>.

[74][FF][A] – Program the F2 Function Key at ID1 Terminal

See command [71]. Default value: <F=1>.

[75][new MASTER card] – Program the new MASTER card

The old MASTER card is deleted and new one is recorded.

[76][new MASTER PIN][#] – Program the new MASTER PIN

The old MASTER PIN is deleted and new one is recorded.

[77][new INSTALLER card] –Program the new INSTALLER card

The old INSTALLER card is deleted and new one is recorded. By default INSTALLER card is not defined in the controller at all and MASTER card takes it role. Still, the command [77] can be used for programming the new INSTALLER card.

[78][new INSTALLER PIN][#] – Program the new INSTALLER PIN

The old INSTALLER PIN is deleted and new one is recorded. By default INSTALLER PIN is not defined in the controller at all. Still, the Command can be used for programming the new INSTALLER PIN.

[79][APB] – Program the Anti-passback mode

Enter: [APB] = [0] to disable APB

Enter: [APB] = [1] to enable Soft APB

Enter: [APB] = [2] to enable Hard APB

Default value: <APB=0>

[80][TA] – Set the option: True APB

Enter [TA]=0 to disable the option or enter [TA]=1 to enable the option. See also 2.7.14 Anti-passback (APB).

[81][SS] – Program the timer of Aux1 flag in seconds (SS = 00-99)

Enter [SS]=00 to disable the timer and set flag in latch mode. See also 2.7.4 Option: Door Lock Controlled in Latch Mode (toggle) and 2.7.9 System Flags. Default value: <SS=00>.

[81][*][MM] – Program the timer of Aux1 flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <SS=00>.

[82][SS] – Program the timer of Aux2 flag in seconds (SS = 00-99)

Enter [SS]=00 to disable the timer and set flag in latch mode. See also 2.7.4 Option: Door Lock Controlled in Latch Mode (toggle) and 2.7.9 System Flags. Default value: <SS=00>.

[82] [*][MM] – Program the timer of Aux2 flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <SS=00>.

[83][SS] – Program the timer of LIGHT flag in seconds (SS = 00-99)

Enter [SS]=00 to disable the timer and set flag in latch mode. See also 2.7.4 Option: Door Lock Controlled in Latch Mode (toggle) and 2.7.9 System Flags. Default value: <SS=00>.

[83] [*][MM] – Program the timer of LIGHT flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <SS=00>.

[84][SS] – Program the timer of TAMPER flag in seconds (SS = 00-99)

Do not enter [SS]=00. See also 2.7.9 System Flags. Default value: <MM=03>.

[84] [*][MM] – Program the timer of TAMPER flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <MM=03>.

[85][SS] – Program the timer of INTRUDER flag in seconds (SS = 00-99)

Do not enter [SS]=00. See also 2.7.9 System Flags. Default value: <MM=03>.

[85] [*][MM] – Program the timer of INTRUDER flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <MM=03>.

[86][SS] – Program the timer of DURESS flag in seconds (SS = 00-99)

Do not enter [SS]=00. See 2.7.9 System Flags. Default value: <MM=03>.

[86] [*][MM] – Program the timer of DURESS flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <MM=03>.

[87][SS] – Program the timer of TROUBLE flag in seconds (SS = 00-99)

Do not enter [SS]=00. See also 2.7.9 System Flags. Default value: <MM=03>.

[87][*][MM] – Program the timer of TROUBLE flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <MM=03>.

[88][SS] – Program the timer of ENTRY DELAY flag in seconds (SS = 00-99)

Do not enter [SS]=00. See also 2.7.9 System Flags. Default value: <SS=60>.

[88][*][MM] – Program the timer of ENTRY DELAY flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <SS=60>.

[89][SS] – Program the timer of EXIT DELAY flag in seconds (SS = 00-99)

Do not enter [SS]=00. See also 2.7.9 System Flags. Default value: <SS=60>.

[89][*][MM] – Program the timer of EXIT DELAY flag in minutes (MM=01-99)

Do not enter [MM]=00. Default value: <SS=60>.

[89][*][*] – Disable ENTRY DELAY timer

Disable timer of ENTRY DELAY flag.

[90][*] - Disable Facility Code

The command disables Facility Code, see 2.7.6 Facility Code.

[90][WCN][ABCDEFGH] - Program the Facility Code

[WCD] parameter specifies Facility Code in range of 000-255 (always three digits). [ABCDEFGH] parameter specifies User Options for all users with Facility Code cards. See also 2.7.6 Facility Code and 2.3.2 User Options. [ABCDEFGH] parameter:

A=1	Access completely disabled
B=1	Authorization for F1 key at Terminal ID0
C=1	Authorization for F2 key at Terminal ID0
D=1	Authorization for F1 key at Terminal ID1
E=1	Authorization for F2 key at Terminal ID1
F=1	Authorization for User Commands
G=1	Authorization for arming/disarming
H=1	Authorization for Function Cards

[91][C] - Set the option: Access disabled when controller armed

Enter [C]=0 to disable the option or [C]=1 to enable the option. Default value <F=0>. See 2.7.3 Option: Access Disabled when Controller Armed

[92][NK][FN][A]<Card> - Program the Function Card

[NK] parameter specifies the number of Function Card in range of 00-31. [FN] parameter specifies the function of Function Card (see 2.11 Function Cards). Enter [A]=0 to disable necessity for authorization of particular Function Card or enter [A]=1 to enable necessity for authorization of particular Function Card.

[93]<card> - Delete the Function Card

The command is used for removing particular Function Card from the access system, see 2.11 Function Cards.

[93][NK] - Delete the Function Card with NK number (NK=00-31)

The command is used for removing Function Card with NK number from the access system, see 2.11 Function Cards.

[93][*] - Delete all Function Cards

The command is used for removing all Function Cards from the access system, see 2.11 Function Cards.

[94][BK] - Adjust keypad backlight (only PR311SE controller)

[BK] = 0 0%
 [BK] = 1 20%
 [BK] = 2 40%
 [BK] = 3 60%
 [BK] = 4 80%
 [BK] = 5 100%

[95][BK] - Adjust volume level (except for PR411DR controller)

[BK] = 0 0%
 [BK] = 1 20%
 [BK] = 2 40%
 [BK] = 3 60%
 [BK] = 4 80%
 [BK] = 5 100%

[96][F] - Option: Constant activation of Output1 (REL1) by card in vicinity of reader

Enter [F]=0 to disable the option or enter [F]=1 to enable the option. Default value: <F=0>. See also 2.7.13 Option: Constant activation of Output 1 by card in vicinity of reader

[97][SS] – Program the timer of CARD PRESENT – SWITCH OFF DELAY flag in seconds (SS=01-99)

Do not enter [SS]=00, 01 or 02. By default the timer is off. See also 2.7.9 System Flags.

[97][*][MM] – Program the timer of CARD PRESENT – SWITCH OFF DELAY flag in minutes (MM=01-99)

Do not enter [MM]=00. By default the timer is off.

[97][*][*] – Disable CARD PRESENT – SWITCH OFF DELAY timer

Disable CARD PRESENT – SWITCH OFF DELAY timer

3.4 Acoustic and visible signals

3.4.1 Visible signals

In PRxx1 series controllers visible signals are presented by means of LED indicators mounted at controllers enclosures.

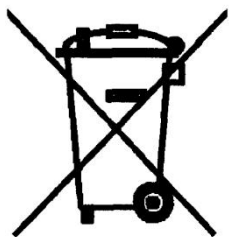
Table 13. LED indicators		
Name	Color	Function
LED STATUS 	Two colors: red or green	RED corresponds to Armed Mode (see 2.6 Armed and Disarmed Modes). GREEN corresponds to Disarmed Mode.
LED OPEN 	Green	The LED is continuously on when the access is granted and blinks if the controller awaits for logging.

LED SYSTEM 	Orange	The LED is continuously on when system malfunction is detected and the controller stops operating until all problems are solved. The LED blinks if the controller awaits for the complete command.
--	--------	--

3.4.2 Acoustic signals

All PRxx1 series controllers (except for PR411DR) generate acoustic signals by means of internal speakers as well as by speakers of external PRT series readers. The PR411DR controller is not equipped with internal buzzer, it generates acoustic signals via buzzers located in the external PRT series readers.

Table 14. Acoustic signals	
Type	Description
Single short signal (1 x BEEP)	Card read or key pressed.
Double short signals (2 x BEEP)	Prompt signal, command accepted but system awaits for further steps.
Triple short signals (3 x BEEP)	OK signal. Command entered correctly or access granted.
Single long signal	Error or unknown card/PIN
Double long signal	Correct card/PIN however access denied due to the other rules.
Periodic long signal	Settings failure. Memory Reset is necessary (see 3.1 Memory Reset – Setting MASTER identifier and ID address of the controller)

	This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may have a negative impact on the environment and health. The user is obliged to deliver equipment to the designated collection points of electric and electronic waste. For detailed information on recycling, contact your local authorities, waste disposal company or point of purchase. Separate collection and recycling of this type of waste contributes to the protection of the natural resources and is safe to health and the environment. Weight of the equipment is specified in the document..
---	---

Contact:
Roger sp.j.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: biuro@roger.pl
Web: www.roger.pl