

Roger Access Control System

PRxx1 Series Access Controllers

Functional Description and Programming Guide

Document version: Rev. A

This document refers to the following products:

PR311SE, PR311SE-BK, PR611, PR621, PR411



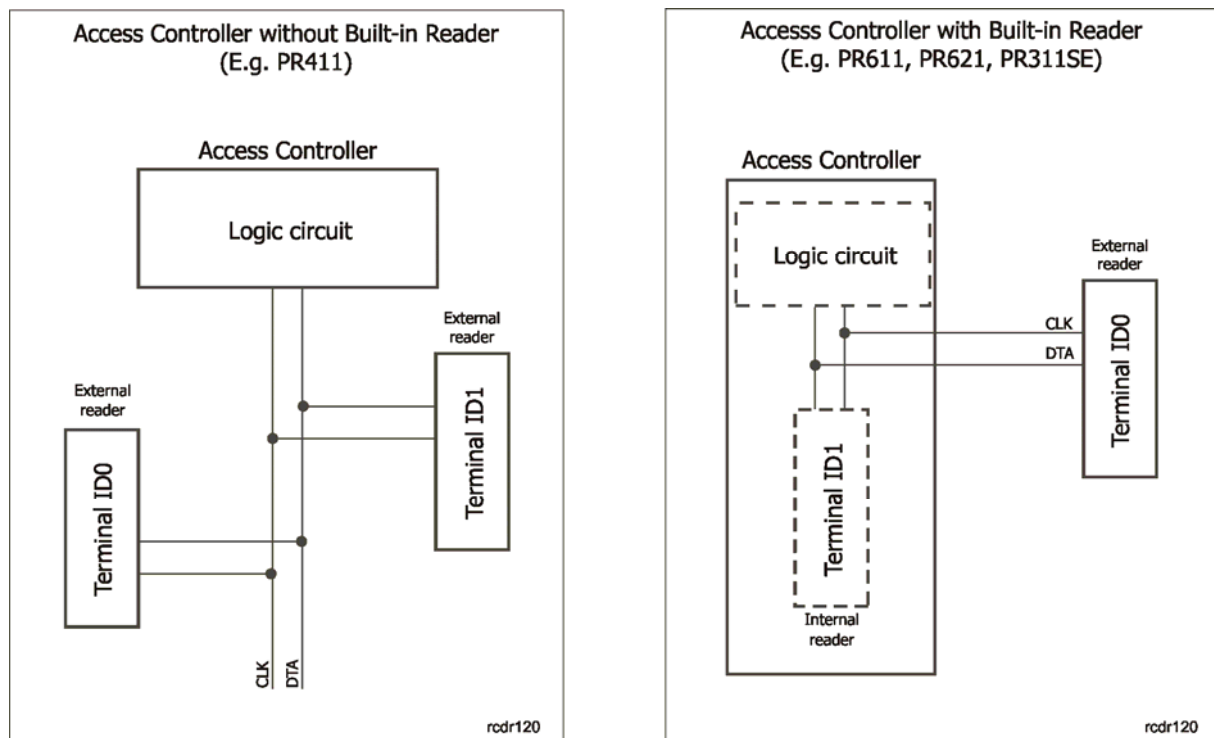
GENERAL

About this Document

This document is not valid and can not be used for old type controllers of following types: PR401, PR301 and PR201. If not clearly indicated PR411 refers to PR411DR as well. The PR411DR is PR411 controller module delivered in plastic enclosure dedicated to be installed on standard DIN Rail 35mm.

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*. The PP311SE, PR311SE-BK, PR611 and PR621 controllers have a built-in reader which is logically treated as *Terminal ID1*, nevertheless still they can operate with one external reader logically treated as *Terminal ID0*. The PR411 controller is not equipped with any built-in access point instead, it can work with two external readers. Generally, the PRxx1 controllers are designed to operate with PRT series readers (from Roger) configured to RACS data protocol, however PR411 can work with *Wiegand 26-66bit* readers as well.



PRxx1 controller can register up to 1000 users plus 8 special ones called *Guests*. Each user has its own ID number and may have card and PIN code.

Controller's firmware can be upgraded on-site through RS485 serial transmission and what's important the firmware upgrade process doesn't require unit to be removed from its original place of installation.

PRxx1 controllers can operate fully autonomously (*Standalone System*) or in the networked system equipped with CPR32-SE network unit (*Networked System*).

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 connected to the programmed controller (the external reader which is used to program controller should be equipped with keypad and configured to **RACS mode address ID0**). Later, for some user programming functions a so called *Function Cards* can be used.

Communication with controllers requires a dedicated interface circuit to convert serial data from the PC into RS485 signals (e.g. RUD-1, UT-2, UT-2USB or UT-4).

Controller	PR311SE	PR311SE-BK	PR411	PR611	PR621
Power supply	10-15VDC	10-15VDC	18VAC or 12VDC	10-15VDC	10-15VDC
Inputs NO/NC	3	3	8	3	3
Relay outputs	1	1	1	1	1
Transistor outputs	2	2	2	2	2
Built-in internal reader	Yes	Yes	No	Yes	Yes
External PRT series readers	1	1	2	1	1
External Wiegand 26-66bit readers	No	No	2	No	No
Built-in keypad	Yes	No	No	Yes	No
Function keys	Yes	Yes	No	No	No
Other	Outdoor operations, pig tail connection cable	Outdoor operations, pig tail connection cable	Built-in PWM power supply 1.2A with battery management circuit	Outdoor operations, pig tail connection cable or skrew terminals	Outdoor operations, pig tail connection cable or skrew terminals

Features

- Single door, two-way access control
- Standalone or networked systems
- 1000 users
- 250 Access Groups (*)
- 99 Time Schedules (*)
- 128 time periods within one single schedule (*)
- 4 Holiday Schedules (H1-H4) (*)
- Automatic winter-summer time change (*)
- Time and Attendance registration (*)
- Built-in keypad (PR311SE, PR611)
- Programmable inputs/outputs
- Relay output 1.5A/30V
- Relay output 1.5A/230V (PR411 only)
- RS485 communication interface (free topology)
- Firmware upgrade through RS485 serial port
- Windows XP/Vista software
- Outdoor operation (PR311SE, PR311SE-BK, PR611 and PR621)
- DIR RAIL 35mm enclosure
- Management thorough LAN/WAN (UT-4 interface required)
- 10-15 VDC supply (PR311SE, PR311SE-BK, PR611 and PR621)
- 18VAC or 12VDC supply (PR411)
- CE mark

(*) - features available only in systems equipped with CPR32-SE network controller

FUNCTIONAL DESCRIPTION

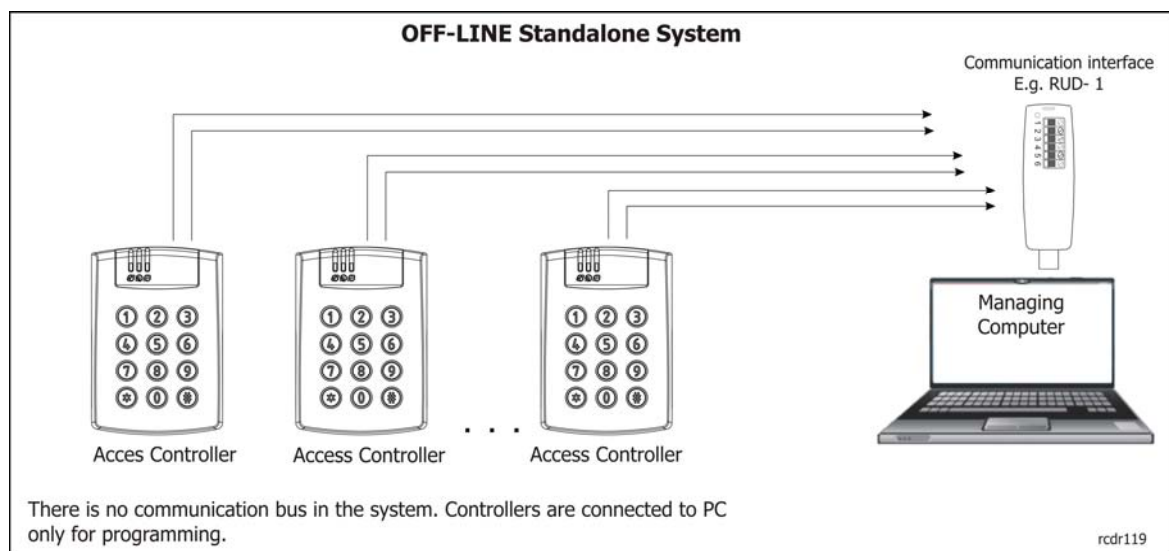
The PRxx1 controller can work in two different scenarios:

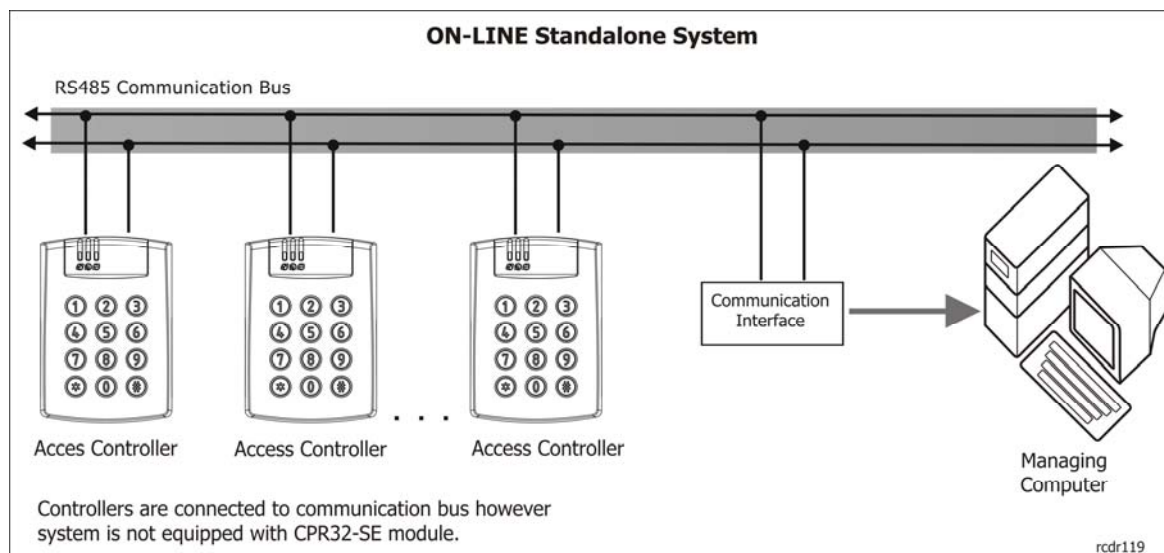
- in Standalone System (without CPR32-SE system controller)
- in Networked System (with CPR32-SE system controller)

Standalone System

When PRxx1 controller work autonomously without CPR32-SE network controller it doesn't offer neither time related functions (e.g. timed access rights) nor event log. In this mode all users belong to the same (default) group of users and have full access rights which are neither restricted by day nor time (every user programmed to the controller has permanent access authorisation). Controller can be programmed manually or from PC however care must be taken using PC programming because managing software (PR Master) doesn't disable to program functionalities which are available in networked systems with CPR32-SE unit.

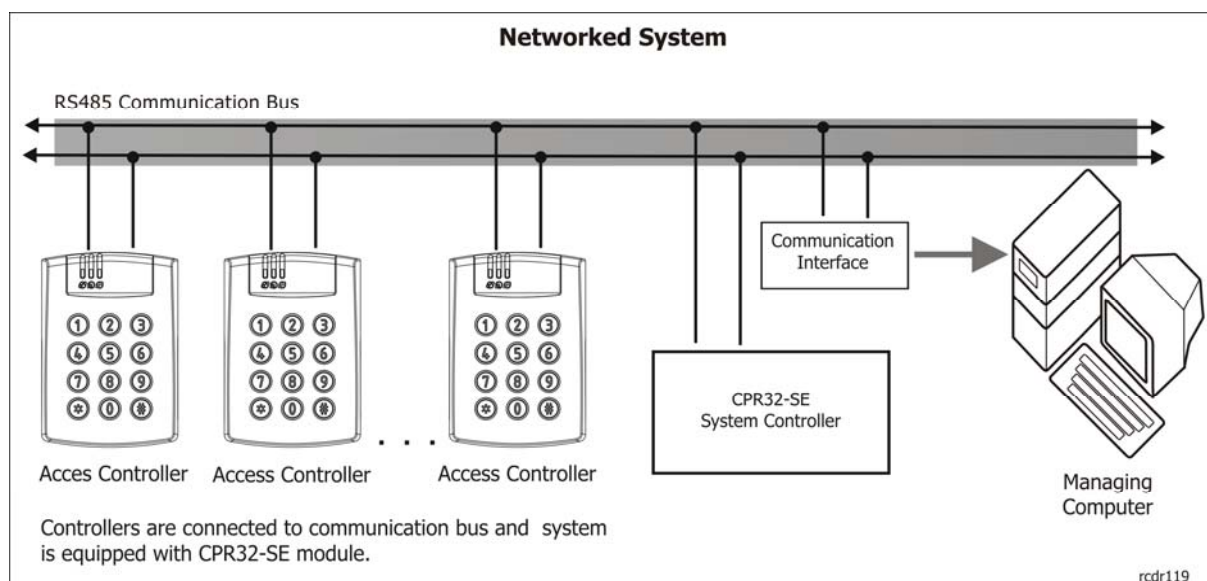
Note: The standalone scenario doesn't implicate that controllers can't be connected to RS485 communication bus and programmed from PC.





Networked System

When controller operates in a system equipped with CPR-32SE module users can be divided into different access groups and with access rights according to the programmed time schedules. Also, CPR-32SE will provide event buffer, time and calendar plus global type functionalities like Alarm Zones and Global Anti-passback. It is necessary to use PC for programming and management of such systems.



Communication

RS485 Communication Bus

PRxx1 controllers feature the RS485 communication interface which is also called *External Communication Bus* or simply *Communication Bus*. Connecting controller to the communication bus requires it to be assigned a unique address (ID=00-99). A single communication bus may accommodate up to 32 access controllers and one CPR unit as an option. The RACS system communication bus topology is fairly flexible. Tree-like

structures as well as star-like topologies are allowed. The so-called *loop* topology is forbidden. On the configuration side, the communication bus can be cabled and setup using any type of regular signal cables, however, twisted-pair unshielded wire is recommended. Terminating resistors at either end of the communication bus are not required. Shielded cables should be used whenever strong electromagnetic interferences exist in the area.

Maximum cable lengths in the RACS 4 system are as follows:

- Any controller to CPR: 1200 m
- Any controller to communication interface: 1200 m
- CPR-to-communication interface: 1200 m

Note: All units connected to the RS485 type bus must share the same ground potential which is clearly the case when all devices are supplied from the same DC power supply source. If more than one power source is used, all negative DC outputs terminals of each power supply need to be tied together using a separate wire – it can be a signal one. If such connection is not feasible (for assembly reasons), negative DC output of each power supply unit should be earthed on its own, however, the difference in earth potential across all units cannot exceed +/-2V.

As mentioned earlier, any structure incorporating a communication bus, access controllers and (optional) CPR32-SE unit is called an *Access Network* or simply a *Network*. Every network in the RACS system needs to be connected to a managing PC via a separate communication port. It can be the ordinary COM type or VCP type (Virtual COM Port), respectively. For VCP type ports, users can use interfaces emulating real serial ports, e.g. RUD-1, UT-2USB, UT-4 (Ethernet) and others.

Every PRxx1 controller manages one door passage in one-way or two-way mode, respectively. At the present moment, RACS 4 permits integrating up to 250 *Networks* of 32 controllers each. Regardless of the fact that each *Network* requires a separate communication port, all of them are logically managed as one integrated access control system.

Note: The same communication interfaces can be used for controller's programming as well as for the entire access control system management. For in-filed programming the RUD-1 interface is suggested because it provides built-in DC output which can be used to supply programmed device.

Controller Address

Each controller connected to RACS system communication bus must have its own address ranged 00-99 however the factory new controller is preprogrammed to address ID=00. By default controller address is a "software one" and can be changed either using software (PR Master) or manually via Memory Reset procedure. Moreover, it is possible to assign a so called "fixed address" to the controller so it can not be changed neither by software nor manually (Memory Reset). This option is especially useful when there is a risk that someone will accidentally change controller address thus system operation will be corrupted. The fixed address can be set, changed or unset using RogerISP program.

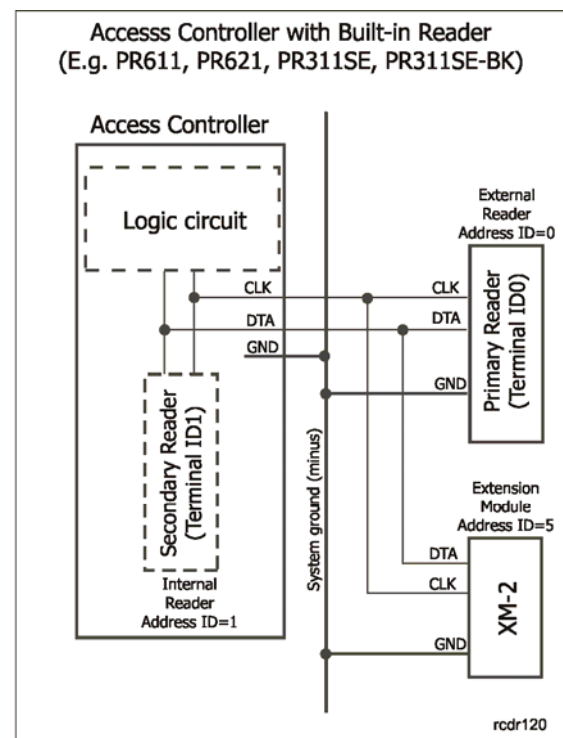
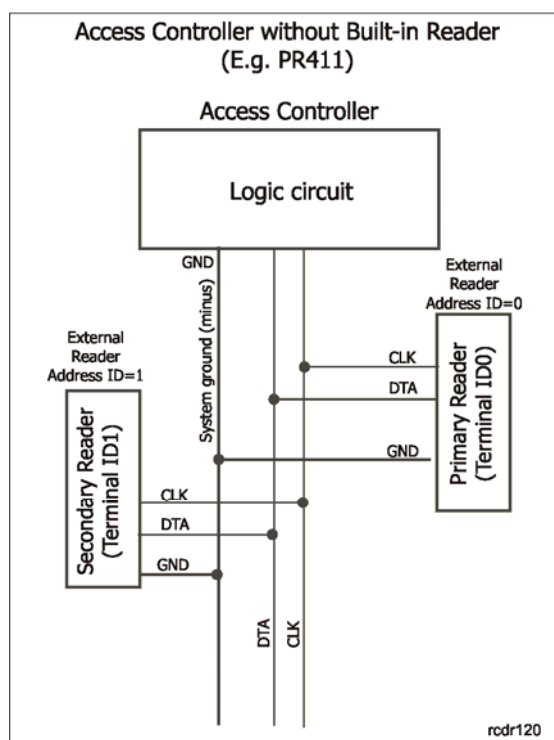
Besides this addressing mechanisms the PR411 controller offers the option to set address by means of programming jumpers. If the programming jumpers indicate valid address (ID=00-99) controller will forbid software address. For detail regarding various address settings refer to the relevant Installer Manual.

Note: The fixed address (FixedID) has always the highest priority – if programmed both software address and jumper address are ignored.

RACS Clock and Data Interface

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

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



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

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 run between controller and external reader and/or XM-2 extension module is limited to 150m. It is possible to use free topology for this bus as well.

All units connected to the given CLK/DTA bus must share common supply minus. This is assured automatically when all unit are powered from the same source of power however if more the one power source is used in system the special wire must be used to connect all minuses (ground) of all power supplies used in the system. This rule is identical as for RS485 bus.

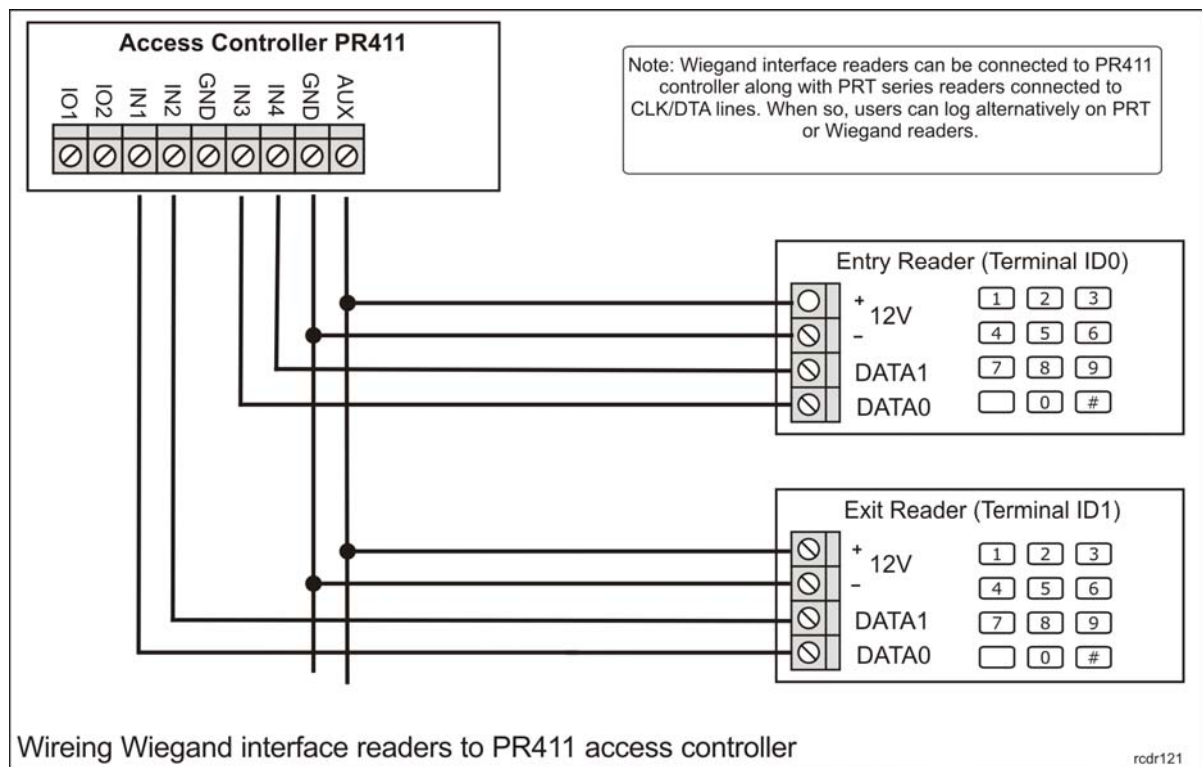
XM-2 Extension Module

Controller can operate with one 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 on the same rules as internal inputs/outputs of the controller. The XM-2 can be used to extend number of available inputs and outputs and/or to separate controller from the controlled device or system. XM-2 module connected to controller must be configured to address ID=5.

Note: Communication between controller and XM-2 module is made digitally what makes that even in case when someone gain access to CLK/DTA communication lines he will not be able to control XM-2 outputs.

Wiegand Readers

Only PR411 can work with Wiegand interface readers. For connection with these kind of readers controller uses separate input lines as presented on the drawing below.



Generally, Wiegand readers can be connected to PR411 controller along with PRT series readers. If so, users can login either on Wiegand or PRT reader.

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*. There are two lists of users in the controller:

- Standard Users (ID=000-999)
- Guest Users (ID=4000-4007)

Name	ID	Description
MASTER	000	This user has 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.7= Yes
SWITCHER Full	ID=001-049	SWITCHER FULL users are allowed for both normal access and arming/disarming of the controller
SWITCHER Limited	ID=050-099	SWITCHER LIMITED users are allowed solely for arming/disarming of the controller, they are not allowed for door access
NORMAL	ID=100-999	NORMAL users are allowed solely for door access only, they are not allowed to arm/disarm controller
GUEST	ID=4000..4007	GUEST users are defined individually on every controller in the system, they may have authorization for door access and for arming/disarming as well

Standard Users

Standard Users is the list of 1000 users common for all controllers in the access control system – they exist on every controller in the system. The so called *Guest Users* is the list of 8 users programmed individually on each controller.

Guests Users

Beside the main list of common access system users (ID=000-999) controller offers an extra, separate list of 8 special users called Guests. These users are programmed and managed by means of special programming procedures. Not like the standard system users (ID=000-999) the Guest users are defined individually on each controller in the system. 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 of more special User Options as any other standard user of the system. If the controller works in integrated access control system (system equipped with CPR32-SE network controller) Guest users can be assigned to the Access Group – as a result their access rights will be under control of time schedule.

User Options

There are 8 special options (called Op.1 - Op.8) possible to assign to every individual user in the controller including Standard Users, Guest Users and Facility Code cardholders as well. These options have the following meanings:

Table 3: User options		
Number	Name	Function
Op.1	Access disabled	When option set user don't have access rights
Op.2	Enabled for authorization of F1 key on term.ID0	When option set user will be allowed to use its identifier for authorization of F1 key on terminal ID0 (when F1 requires authorization)
Op.3	Enabled for authorization of F2 key on term.ID0	When option set user will be allowed to use its identifier for authorization of F2 key on terminal ID0 (when F2 requires authorization)
Op.4	Enabled for authorization of F1 key on term.ID1	When option set user will be allowed to use its identifier for authorization of F1 key on terminal ID1 (when F1 requires authorization)
Op.5	Enabled for authorization of F2 key on term.ID1	When option set user will be allowed to use its identifier for authorization of F2 key on terminal ID1 (when F2 requires authorization)
Op.6	Enabled for authorization of User Commands	When option set user will be allowed to use its identifier for authorization of User Commands (if authorization is required)
Op.7	Enabled for arming/disarming	When option set user will be allowed to change current arming mode of the controller
Op.8	Enabled for authorization of Function Cards	When option set user will be allowed to use its identifier for authorization of Function Cards (if authorization is required)

Groups

Access system users can be divided into various Groups or may belong to special (predefined) Group called: **No Group**. The maximum number of user groups on PRxx1 controllers is 250. The access group membership determines a user's access rights within a given access control system. All users assigned to a particular user group share the same (identical) access rights. One access group can incorporate as little as one system user. **No Group** members are given unlimited 24 h access to all Access Zones. By default, every new user in a RACS type system is assigned to the No Group.

Identification Modes

For user identity authentication purposes a controller applies one of the following Identification Modes:

Mode	Description
Card or PIN	Controller requires a card or a PIN code
Card and PIN	Controller requires a card and a PIN code
Card Only	Controller requires a card only, PINs are not accepted
PIN Only	Controller requires a PIN code only, Cards are not accepted

Identification Modes are defined on per-side basis for every access controlled passage. Unless explicitly specified, a controller applies the so-called Default Identification Mode for user identification purposes. Identification rules apply to all users. Identification Modes control can be accomplished through:

- Time Schedule (when controller work in networked system with CPR32-SE unit)
- Function key
- Input lines

Door Modes

Door Modes determine lock/unlock rules for access controlled doors. In every access control system there exist the following Door Modes:


Mode	Description
Normal	Door is locked, open upon access granted event only
Unlocked	Door is unlocked, no authoristaion required for entry. Door lock is activated for the entire time when controller is in this mode
Conditional unlocked	Initially, door is in the Normal Mode. As soon as a first user is granted access, a controller switches to the Unlocked mode
Locked	Door is always locked, no entry at all. Door lock is disabled for the entire time when controller is in this mode

By default, the active Door Mode is always the Normal Mode. Modes can be changed or altered as a result of following functions/mechanisms:

- Time scheduling (when controller work in networked system with CPR32-SE unit)
- Function key
- Onput lines

Arming and Disarming

Concept of Arming Modes


PRxx1 controllers feature 2 arming modes: Armed and Disarmed. The current mode is indicated on the controller's LED STATUS . The LED's red color always refers to the Armed mode, whereas the green one indicates the Disarmed mode.

Arming mode control can be accomplished through

- Manual changes by means of an access card or a PIN code
- Time schedule (when controller work in networked system with CPR32-SE unit)
- Input lines
- Function keys
- Alarm Zones logic (when controller work in networked system with CPR32-SE unit)
- Remote command from a PC

Arming and Disarming

Every controller can be re-armed using the following card/PIN: MASTER, SWITCHER Full or SWITCHER Limited. For MASTER and SWITCHER Full users the re-arming sequence is as follows:

- Input an a card, a PIN or either one of them according to the current Identification Mode
- Upon a successful authorization, the controller might grant access to a user releasing the door lock (depends on general access rights and some options)
- The user should wait till the LED SYSTEM  starts blinking
- While LED is blinking, the user should input card/PIN once again (this time using card or PIN no matter what Identification Mode)

Re-arming using the so-called SWITCHER Limited requires from users a single card/PIN input only. In this scenario, re-arming does not result in the access granted event.

Automatic Arming/Disarming

A controller's arming mode can be altered automatically via time 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 (time schedule, user activity or any other logic). If a controller is not assigned to any Alarm Zone, it may be assigned any time schedule which will control its arming mode. Assigning the controller the so-called NEVER time schedule forces it to remain always in the armed mode. On the contrary, applying the ALWAYS time schedule makes the controller operate continuously in the disarmed mode.

A re-arming schedule by itself is a regular time schedule (a so-called General Purpose Schedule - GPS) used for purpose of automatic arming and disarming. The GPS schedule is composed of time periods *From/To* which when used for arming control purpose will specify time periods when controller will automatically switch to disarmed mode. While

outside the specified time periods, a controller will automatically return into the armed mode.

The time schedule based re-arming is as follows: at a time instant indicated by the *From* parameter, a controller switches into the disarmed mode. For comparison, at a time instant determined by the *To* parameter, the controller returns to the armed mode. Switching back to the armed mode may be disabled provided the input line (**[13]: Arming disabled**) was already triggered or a door was opened.

Option: Enable Arm/Disarm Schedule

Whenever this option is activated, the current armed mode on a controller changes automatically according to the specified time schedule. The time schedule can be defined exclusively for the Alarm Zone the controller is assigned to. Alternatively, a non-group controller may follow an arbitrary time schedule. Deactivating the option switches off the time schedule based arming control.

Access Rights

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

- Assigning users to Groups
- Defining time schedules (calendars)
- Linking user Groups to Access Zones and Time Schedules. During that stage users indicate a time schedule (hours, days) for user access for a particular Access Zone
- Configuring other access control mechanisms for access control (e.g. Door Modes, inputs, function keys, APB 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
- Access decision

Access Signalling

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

Door Lock Control

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

- applying supply voltage for the actuator (e.g. door strike)
- removing supply voltage from the actuator (e.g. magnetic lock)
- applying electric pulse (e.g. rotary gates)

- triggering servo motor (e.g. motor lock)

Controllers carry out door lock control procedures using the following outputs: **[97]: Entry door lock, [98]: Exit door lock, [99]: Door lock.**

A controller may activate the output [99] on an access granted event on either side of the controlled door (Terminal ID0 or Terminal ID1). The other outputs ([97], [98]) are activated depending on which side of the door access was granted. In general, the two outputs are used for the rotary gate control where in general it is important to locate the gate rotation direction.

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

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 system users regardless of their access rights to that room/access controlled area. The purpose of this option is to enable users with controller re-arming access to deny/grant access for the remaining system users. This option overrides time schedule settings.

Option: Door Lock Controlled in Latch Mode

When activated, every access granted event switches the actuator control output into the revers state. The output remains in that state till access is granted again. Under normal circumstances, the actuator control output is activated only for the time period determined by the following parameter: **Door Unlock Time**. Once the prescribed time interval has elapsed, the output returns automatically to the previous state.

Auto-relock

This function allows for advanced door lock control process. Normally, when Auto-relock function is disabled controller activates door lock output 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** or **Activate door lock upon door closing detection**. In first case controller will de-energise 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 the door has been closed. This first scenario is usually used for door locks which unblock doors upon energizing electric lock (e.g. door strike). While, second is used for door locks which unblock doors upon deenergizing electric lock (e.g. magnetic lock). The Auto-relock function makes sense only if a controller cooperates with a door opening detector (door contact).

Facility Code

The so called Facility Code (also called: Site Code) is a part of the entire card code which is located on positions between 16th and 24th and intended to characterize some group of cards customized and produced for individual order. For example if the card has following code (presented in binary form):

0001000000000000111011100010001010110111 the underline characters 11101110 are treated as Facility Code (Site Code).

The ISO, PVC and key fobs provided by Roger have card code printed in two forms: full card code in decimal system e.g. 68735083191 and reduced form 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 are equal to the card's Facility Code.

When Facility Code function is active controller allows for access not only to users which have valid access rights but to all other cards which are characterized with the same specific Facility Code as programmed in the controller. Thanks to this feature controller can be used to grant access to large number of cardholders whose cards comply to a given Facility Code.

Also, the group of cards which comply with Facility Code can be assigned to specific Group of users thus they will have the same access rights as user which belong to given Group. Moreover, Facility Code cards can be granted with special options (Op.1 - Op.8) as any other user of the system.

Duress PIN Entry

This function is used to recognize and signal situation when PIN code is enrolled under duress. When the option is active, controller will assume that entry of the PIN code which differs by "1" on the last digit from the original one will be treated as duress entry of the PIN. When that happens, the system raises the FORCE ENTRY state.

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

Note: For fault-free operation in this mode user access codes need to differ by more than "1" at the code's last digit. The PR Master managing software verifies that condition and informs of any exceptions to that rule. Finally, the option can be switched off and the system will allow for arbitrary PIN code assignments.

When activating option Disable Duress codes system deactivates the PIN code input under duress mode. As a result, PIN codes under duress do not raise the FORCED ENTRY event.

System Flags

System flags or simply *flags* are logic states in a controller's memory to reflect certain situations/events on a controller. A number of flags are predefined reflecting a defined event set (TAMPER, DURESS, INTRUDER, TROUBLE), whereas others are fairly universal and can be used for arbitrary user-defined purposes (AUX1, AUX2 and LIGHT).

Initially, every flag is switched off. Flags can only be switched on upon certain system events. Flags return to previous states autonomously after a preset time interval has elapsed or a proper event has taken place forcing it to return to the passive state.

The flag's turn-on time is determined by a relevant timer. Flags return to the original state autonomously after a preset time determined by the timer has elapsed. Selected flag timers can be set into a bi-state type mode (*latch mode*) – in this mode flag state

changes are permanent till controller gets disarmed. The state of every flag can be signalled on output lines.

Table 6: System flags		
Flag	Activation mechanisms	Desctivation mechanisms
AUX1	<p>Programming Cards [F12]: Set AUX1 output ON and [F14]: Toggle AUX1 output ON/OFF</p> <p>Inputs:</p> <p>[71]: Set AUX1</p> <p>[73]: Set/clear AUX1</p> <p>Function keys:</p> <p>[71]: Set AUX1 timer</p> <p>[73]: Set/clear AUX1 timer</p>	<p>Programming Cards [F13]: Set AUX1 output OFF and [F14]: Toggle AUX1 output ON/OFF</p> <p>Inputs line [72]: Cancel AUX1 timer and [73]: Toggle AUX1 timer</p> <p>Function keys [72]: Clear AUX1 timer and [73]: Toggle AUX1 timer</p> <p>In addition to that, the flag is switched off after a preset time to be determined by the timer has elapsed</p>
AUX2	<p>Programming Cards [F20]: Set AUX2 output ON and [F22]: Toggle AUX2 output ON/OFF</p> <p>Inputs line [74]: Start AUX2 timer and [76]: Toggle AUX2 timer</p> <p>Function keys [74]: Start AUX2 timer and [76]: Toggle AUX2 timer</p>	<p>Programming Cards [F21]: Set AUX2 output OFF and [F22]: Toggle AUX2 output ON/OFF</p> <p>Inputs line [75]: Cancel AUX2 timer and [76]: Toggle AUX2 timer</p> <p>Function keys [75]: Clear AUX2 timer and [76]: Toggle AUX2 timer</p> <p>In addition to that, the flag is switched off after a preset time to be determined by the timer has elapsed</p>
LIGHT	<p>Programming Cards [F15]: Set LIGHT output ON and [F17]: Toggle LIGHT output ON/OFF</p> <p>Inputs line [68]: Start LIGHT timer and [70]: Toggle LIGHT timer</p> <p>Function keys [78]: Start LIGHT timer and [70]: Toggle LIGHT timer</p>	<p>Programming Cards [F16]: Set LIGHT output OFF and [F17]: Toggle LIGHT output ON/OFF</p> <p>Inputs line [69]: Cancel LIGHT timer and [70]: Toggle LIGHT timer</p> <p>Function keys [69]: Clear LIGHT timer and [70]: Toggle LIGHT timer</p> <p>In addition to that, the flag is switched off after a preset time to be determined by the timer has elapsed</p>
TAMPER	Input line [08]: TAMPER	<p>Disarming of the controller</p> <p>After a preset time (to be determined by a timer) has elapsed</p>

INTRUDER	Input line [09]: Intruder	Disarming of the controller After a preset time (to be determined by a timer) has elapsed
DURESS	Duress PIN entered	After a preset time (to be determined by a timer) has elapsed
TROUBLE	Input line [05]: AC lost Input line [06]: Low battery Lost of communication with the XM-2 module	Rearming of the controller After a preset time (to be determined by a timer) has elapsed
ENTRY DELAY	Input line [15] Intruder – delayed	Disarming of the controller After a preset time (to be determined by a timer) has elapsed
EXIT DELAY	Arming of the controller	Disarming of the controller After a preset time (to be determined by a timer) has elapsed

Door Alarm

The PRxx1 controllers has 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 on dedicated output 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 states. For Door Alarm signaling the PRxx1 uses different signal modulation of an output 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

Alarm Type	Description	Priority	Metoda sygnalizacji
Prealarm	Raised upon five consecutive PIN input attempts within a five minute interval.	Low	Single pulse repeated periodically every 2 s.
Door Ajar	Raised when a door was not closed within a preset time interval. The time is determined by the following parameter: Door lock time.	Medium	Two pulse repeated periodically every 2 s.
Forced Entry	Raised upon an unauthorized door opening event detection or a PIN under duress input case.	High	Single 1s pulse repeated periodically every 1 s.

PREALARM

The so-called PREALARM state is used to inform of five consecutive unauthorized access attempts that have occurred within a 5-minute time interval. The state can be detected at the following outputs: **[01]: Prealarm**, **[03]: Prealarm + Door Ajar** and **[07]: Prealarm +Door Ajar + Forced Entry**.

Option: Disable reader when in PREALARM

Activating the option disables card access as well as PIN access for a period of five minutes after the PREALARM state was raised.

Anti-passback

When anti-passback function is active with the first time user can log either on entry or exit reader however every next time he must login on opposite side of the given door. Controller offers anti-passback function in two forms:

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

When Soft APB is selected controller grants access event incase when APB rules are violated however adequate event (APB Violation) is generated. When operating with Hard APB option violating APB rules will cause that controller will reject access for particular user.

True Anti-passback

When option True APB is active controller assumes user went through passage when access was followed by door opening. If access is granted but door has not been opened controller assumes user did not pass through door and his anti-passback status remains unchanged.

APB Reset Time

Controller allows for definition of two times (within one day) when its APB Register will be cleared and set to default values. This functionality is available for system equipped with CPR network. controller only.

Note: Once the APB Register is cleared all users have status Not logged and initially (first time) can login either on entry or exit side of the door

Anti-passback Zones

An APB Zone is a selected access controlled area in which a user access is controlled by 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. Of the 2 readers connected to a controller, one monitors the APB zone entrance, whereas the other one monitors the exit from that zone. It is forbidden 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 access control system incorporates the 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: RACS 4 systems permit APB zones to incorporate controllers operating within one access network only. The APB Zone definition does not allow for controllers from various access networks.

APB Register

The APB Register is a section on controller memory which keeps information where (on terminal ID0 or ID1) each user has been logged lately. The APB Register may have following

Table 8: APB Status	
Type	Description
Logged on Terminal ID0	User logged last time on Terminal ID0
Logged on Terminal ID1	User logged last time on Terminal ID1
Logged OFF	The location of last login is missing. In such a case user can log either on Terminal ID0 or Terminal ID1.
Disabled	No matter if user will login on Terminal ID0 or ID1 access will be denied.

APB Reset

The APB Reset clears APB Register and set APB Status for all users as Logged OFF. Once the reset procedure is completed, the users may attempt to login either on Terminal ID0 or Terminal ID1. Note, however, upon the first user login after the register reset the APB rules start to work again and users are required to login on alternate sides of the door.

The system initiates the APB Register Reset procedure automatically on start-up, however, the reset procedure can be accomplished in the following manner

- Input line [60]: APB Register reset
- Function key [60]: APB Register reset
- Automatically according to APB Reset Schedule

APB Zone Hierarchy

APB Zone Hierarchy reflects zonal relationships between various APB zones defined within one particular access network. In access control systems with global ABPs users are allowed to re-locate only within neighboring APB Zones. Neighboring APB Zones are adjacent passage controlled zones. 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 via software. With the APB Hierarchy switched off, users are allowed to leave the APB Zones they are in, and enter another one. In this case, the APB zones are not required to be adjacent APB Zones.

Notes:

1. The term Passage refers to a controller located at a border of 2 ABP Zones.
 2. Neighbouring APB Zones are zones connected with a Passage.
 3. The APB Hierarchy is setup automatically on reader assignment to particular ABP Zones in a system. The hierarchy can be modified only upon changes in the reader assignment structure, i.e., by assigning readers to other APB Zones.
-

Hard APB

Activating the so-called Hard APB mode on a controller causes it to raise an access denied event accompanied by 2 long sound signals upon any APB rule violation attempt. The event is registered as the APB Violation.

Soft APB

Activating the Soft APB mode on a controller causes it, in case of an APB rule violation, to register the APB violation event only. However, the system does not raise any access denied event.

APB Hard/APB Soft Schedule

Switching APB modes on a controller can be accomplished by setting up an APB Mode Schedule. Such schedule forces a controller to switch between Hard APB and Soft APB modes, respectively. Any NEVER type schedule forces a controller to operate in the Hard APB mode, whereas ALWAYS type schedules make it to follow Soft APB settings. Any other schedule forces a controller to switch into the Soft mode within time intervals defined by the schedule, then switching back to the Hard mode when beyond the scope of the schedule.

Alarm Zones

An Alarm Zone is a group of controllers intended to operate in a concurrent arming mode. If any controller of an alarm zone changes its arming mode, the remaining controllers follow the mode change. It is not relevant what made the controller to have its arming mode changed. The concurrent re-arming is by CPR-32SE unit means. The central unit keeps monitoring modes on all access controllers within an Alarm Zone. If any single controller changes its arming mode, the unit alters the modes on the other controllers. As a result, all controllers within one Alarm Zone maintain the same arming mode at any time.

Uwaga: Using Alarm Zone does not block other arming methods.

With the armed mode control via the following input line [03]: Disarmed mode (toggle switch) the current mode on a controller cannot be altered remotely by any monitoring hardware (CPR unit) or any other mechanism. Such controllers can be still a part of an

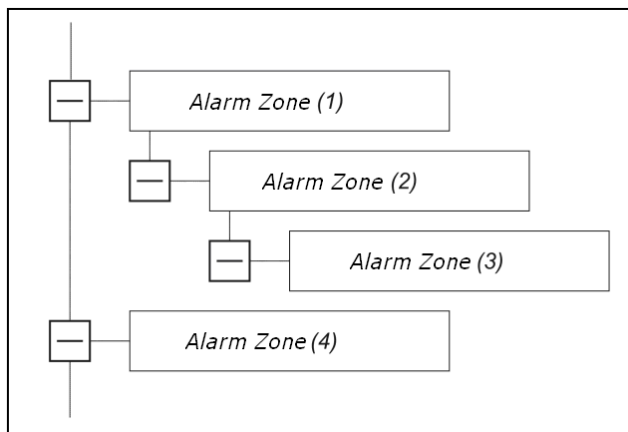
Alarm Zone, however, their modes are not subject to any CPR based controls, thus depending on the input line states only.

Alarm Zone Hierarchy

An Access Control system can incorporate at least one Alarm Zone. The zones are capable of independent operation, or they can be setup into a hierarchic structure. In the independent zones, any armed mode changes within one zone do not affect other zones. Hierarchic structures may assume a master/slave type relationship between corresponding alarm zones. In this case, the following rules are valid:

- Arming a master zone makes all slave zones armed
- Disarming a master zone does not affect slave zones operation
- Arming a slave zone does not affect the master zone
- Disarming a slave zone does not affect the master zone

Defining an alarm zone hierarchy in a RACS 4 type system takes the form of a tree structure. The structure reflects mutual relationships and dependencies between all alarm zones. One example is illustrated below.



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 zone 1 causes zones 2 and 3 to be armed accordingly. Finally, arming the zone 2 arms the zone 3 e.t.c.

Inputs

Controller itself offers three programmable inputs configurable as normally open (NO) or normally closed (NC) lines. The normally open line becomes triggered when shorted to ground (supply minus). The normally closed output needs to be normally shorted to ground (supply minus), it becomes triggered when connection with ground is discontinued. Internally, each input is pulled up to supply plus through 15kΩ resistor. The average threshold voltage between low and high logical level on inputs is around 3V in respect to ground (supply minus). Inputs can be programmed to several functions listed in the table below:

Table 9: Input functions		
Code	Name	Function
[00]	None	Disables inputs from any function
[01]	Door contact	Condition of this input indicates whether the door is open or close
[02]	Exit button	When triggered controller activates door lock according to the same rules when normal access is granted
[03]	Disarmed mode (toggle)	When active it forces controller to Disarmed mode and vice versa when not active controller remains in Armed mode
[04]	AUX	Activating/deactivating this line generates event in report only
[05]	AC lost	Triggering this input activates Trouble Alarm
[06]	Low battery	Triggering this input activates Trouble Alarm
[07]	Door bell	Triggering this input activates Door bell signaling on internal buzzer and on the output line [15] (if programmed)
[08]	Tamper	Triggering of this input either in Armed or Disarmed mode will activate Tamper Alarm and Intruder Alarm simultaneously
[09]	Intruder	When in Armed mode triggering this inputs activates Intruder alarm
[11]	Access disabled	When active controller will totally forbid access
[13]	Arming disabled	When active controller cannot be armed
[14]	Door lock switch	When triggered activates door lock
[15]	Intruder-delayed	When in Armed mode triggering of this input starts counting of the Time for Entry timer. If during this time controller will be not switched to Disarmed mode the Intruder alarm will occur
[60]	APB Register reset	It resets the APB Register. All system users are assigned the Logged Off APB status.
[61]	Arm/Disarm switch (momentary)	Changes current arming mode of the controller
[64]	Normal door mode	Switches controller to Normal door mode
[65]	Unlocked door mode	Switches controller to Unlocked door mode
[66]	Cond. Unlocked door mode	Switches controller to Conditional Locked door mode
[67]	Locked door mode	Switches controller to Locked door mode

[68]	Set LIGHT	Starts counting process for LIGHT timer
[69]	Cancel LIGHT timer	Clears counting process for LIGHT timer
[70]	Toggle LIGHT timer	Switches LIGHT timer to reverse state
[71]	Set AUX1 timer	Starts counting process for AUX1 timer
[72]	Cancel AUX1 timer	Clears counting process for AUX1 timer
[73]	Toggle AUX1 timer	Switches AUX1 timer to reverse state
[74]	Set AUX2 timer	Starts counting process for AUX2 timer
[75]	Cancel AUX2 timer	Clears counting process for AUX2 timer
[76]	Toggle AUX2 timer	Switches AUX2 timer to reverse state
[78]	Disarmed mode (momentary)	Switches controller to Disarmed mode
[79]	Armed mode (momentary)	Switches controller to Armed mode
[80]	Card or PIN mode	Switches controller to Card or PIN mode
[81]	Card only mode	Switches controller to Card only mode
[82]	PIN only mode	Switches controller to PIN only mode
[83]	Card and PIN mode	Switches controller to Card and PIN mode

Note: You can assign only one input 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 listed function no other input can be programmed to the same one.

Outputs

Controller itself offers one relay output (REL1) and two transistor outputs IO1 and IO2. When operating with XM-2 module two extra relay outputs are available. When not triggered the IO1 and IO2 outputs represent high impedances while triggered they short to the ground. Moreover, when controller doesn't work with external reader nor extension module it allow to program CLK and DTA lines as ordinary outputs. For maximum current/voltage ratings of outputs please refer to technical data presented later in this document.

Note: PR411 offers an extra relay output (marked REL2) which can be programmed in the same way as any other controller output.

Each output line can be programmed to function listed in the table below:

Table 10: Output functions			
Code	Name	Function	Notes
[00]	Disarmed mode	Active when controller Armed	
[01]	Prealarm	Active when controller indicates Prealarm state	Modulated according to the Prealarm pattern
[02]	Door Ajar	Active when controller indicates Door Ajar state	Modulated according to the Door Ajar pattern
[03]	Prealarm+ Door Ajar	Active when controller indicates either Prealarm or Door Ajar state	Modulated according to the Prealarm or Door Ajar pattern depending on the existed state and its priority
[04]	Forced Entry	Active when controller indicates Door Ajar state	Modulated according to the Forced entry pattern
[05]	Prealarm+Forced Entry	Active when controller indicates either Prealarm or Forced entry state	Modulated according to the Prealarm or Door ajar pattern depending on the existed state and its priority
[06]	Door Ajar+Forced entry	Active when controller indicates either Door ajar or Forced entry state	Modulated according to the Prealarm or Door Ajar pattern depending on the existed state and its priority
[07]	Prealarm+Door Ajar+Forced Entry	Active when controller indicates one from following states: Prealarm, Door ajar or Forced entry	Modulated according to the Prealarm, Door Ajar or Forced Entry pattern depending on the existed state and its priority
[09]	Access granted	Activated for 2s whenever access is granted	

[10]	Door status	Active when door is open	Used to indicate if the monitored door is now open or closed
[11]	Access denied	Activated for 2s whenever access is denied	
[14]	User logged on term. ID0	Once the user has been identified on terminal ID0 this output switches to active state and remains in it till then moment when next user is identified from terminal ID1	Output can be used to organize two way door passage (e.g. turn style gate). Condition of this output determines in which way user is moving depending on the reader used for identification (terminal ID0 or ID1)
[15]	Door bell	Indicates Door Bell for 5s	Door bell signaling can be activated using function key, input line or [#] key when pressed separately
[18]	Normal door mode	Active when controller operates in Normal door mode	Output remains triggered as long as Normal mode is active
[19]	Unlocked door mode	Active when controller operates in Unlocked door mode	Output remains triggered as long as indicated mode is active
[20]	Cond. Unlocked door mode	Active when controller operates in Conditional Unlocked door mode	Output remains triggered as long as Conditional Unlocked mode is active
[21]	Locked door mode	Active when controller operates in Locked door mode	Output remains triggered as long as Locked mode is active
[25]	Pulse upon disarming	Active for 2s upon controller switches to Disarmed mode	
[26]	Pulse upon arming	Active for 2s upon controller switches to Armed mode	
[64]	LIGHT	Presents current state of LIGHT flag	Depending on the method this output can be triggered for limited time determined by LIGHT Timer or for unlimited period when configured to latch mode
[65]	Tamper Alarm	Presents current state of TAMPER flag	Duration of Tamper Alarm is determined by Tamper

			Timer
[66]	AUX1	Presents current state of AUX1 flag	Depending on the method this output can be triggered for limited time determined by AUX1 Timer or for unlimited period when configured to latch mode
[67]	AUX2	Presents current state of AUX2 flag	Depending on the method this output can be triggered for limited time determined by AUX2 Timer or for unlimited period when configured to latch mode
[68]	Intruder Alarm	Active when Intruder Alarm in progress	Duration of Intruder Alarm is determined by Intruder Timer
[69]	Duress Alarm	Active when Duress Alarm in progress	Duration of Duress Alarm is determined by Duress Timer
[70]	Trouble Alarm	Active when Trouble Alarm in progress	Duration of Trouble Alarm is determined by Trouble Timer
[71]	Exit delay in progress	Active when EXIT DELAY is in progress	Time determined by Exit Delay Timer
[72]	Entry delay in progress	Active when ENTRY DELAY is in progress	Time determined by Entry Delay Timer
[80]	Card or PIN mode	Active when when controller operates in Card or PIN identification mode	Output remains triggered as long as Card or PIN mode is active
[81]	Card only mode	Active when when controller operates in Card only identification mode	Output remains triggered as long as Card only mode is active
[82]	PIN only mode	Active when controller operates in PIN only identification mode	Output remains triggered as long as PIN only mode is active
[83]	Card and PIN mode	Active when when controller operates in Card and PIN identification mode	Output remains triggered as long as Card and PIN mode is active
[97]	Entry door lock	Activated when access was granted from Terminal ID1	Output activated when access is granted upon identification made on terminal ID1 only. Activation time same as for

			output [99]. Output is usually used for two way door passage.
[98]	Exit door lock	Activated when access was granted from Terminal ID0	Output activated when access is granted upon identification made on terminal ID0 or through exit button . Activation time same as for output [99]. Output is usually used for two way door passage.
[99]	Door lock	Activated when access was granted either from Terminal ID0 or ID1	Whenever access is granted (no matter which way) controller activates this output for time determined by Door Unlock Time

Function Keys

Logically, controller offers four function keys: two located on terminal ID1 and two others located on terminal ID0. No matter if the function key is located on terminal ID1 or ID0 they can be programmed in the same way to one from several options explained in table below. Optionally, usage of function key can be restricted for users with special authorization (see section: User Options). The need for authorization can be set individually for each function key defined in the system.

Function keys options:

Code	Name	Function
[00]	None	No function assigned to key
[01]	Door bell	Triggers door bell signaling
[02]	Exit button	Pressing key activates door lock according to the same rules when normal access is granted
[04]	Key pressed (event only)	Pressing key is registered in event log only
[09]	Intruder Alarm	When in Armed mode pressing key activates Intruder Alarm
[60]	APB Register reset	Pressing the key clears the APB register.
[61]	Armed/Disarmed mode	Pressing key changes current arming mode of the controller
[64]	Normal door mode	Pressing key switches controller to Normal door mode
[65]	Unlocked door mode	Pressing key switches controller to Unlocked door

		mode
[66]	Cond. Unlocked door mode	Pressing key switches controller to Conditional Locked door mode
[67]	Locked door mode	Pressing key switches controller to Locked door mode
[68]	Set LIGHT	Pressing key activates LIGHT flag for time defined by LIGHT timer
[69]	Cancel LIGHT	Pressing key clears LIGHT flag
[70]	Toggle LIGHT	Pressing key switches LIGHT flag to opposite state (either switches it to ON or OFF depending on the previous state)
[71]	Set AUX1	Pressing key activates AUX1 flag for time defined by AUX1 timer
[72]	Cancel AUX1	Pressing key clears AUX1 flag
[73]	Toggle AUX1	Pressing key switches AUX1 flag to opposite state (either switches it to ON or OFF depending on the previous state)
[74]	Set AUX2	Pressing key activates AUX2 flag for time defined by AUX2 timer
[75]	Cancel AUX2	Pressing key clears AUX2 flag
[76]	Toggle AUX2	Pressing key switches AUX2 flag to opposite state (either switches it to ON or OFF depending on the previous state)
[77]	Cancel Intruder and Tamper alarms	Pressing key clears both: Intruder Alarm and Tamper Alarm
[78]	Set Disarmed mode	Pressing key switches controller to Disarmed mode
[79]	Set Armed mode	Pressing key switches controller to Armed mode
[80]	Card or PIN mode	Pressing key switches controller to Card or PIN mode
[81]	Card only mode	Pressing key switches controller to Card only mode
[82]	PIN only mode	Pressing key switches controller to PIN only mode
[83]	Card and PIN mode	Pressing key switches controller to Card and PIN mode

Function Cards

Function Cards are standard proximity cards which were assigned specific programming functions. Function Cards can be defined during device's configuration process. Each *Programming Card* may have assigned only one programming function but

many Programming Cards may be assigned to a single user programming function. The following programming functions can be assigned to *Programming Cards*:

- Function [01]: Add card for NORMAL user
- Function [03]: Add card for SWITCHER FULL user
- Function [05]: Add card for SWITCHER LIMITED user
- Function [06]: Delete card
- Function [07]: Delete all user cards
- Function [08]: Set door to Normal mode
- Function [09]: Set door to Unlocked mode
- Function [10]: Set door to Cond.Unlocked mode
- Function [11]: Set door to Locked mode
- Function [12]: Set AUX1
- Function [13]: Clear AUX1
- Function [14]: Toggle AUX1
- Function [15]: Set LIGHT
- Function [16]: Clear LIGHT
- Function [17]: Toggle LIGHT
- Function [19]: Add multiple cards
- Function [20]: Set AUX2
- Function [21]: Clear AUX2
- Function [22]: Toggle AUX2
- Function [25]: Delete all GUEST cards

PROGRAMMING

General

Controller can be programmed in three ways:

- From PC
- Manually from local keypad
- Manually from remote keypad located on the external reader

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-synchronised from the settings entered manually.

Programming from External Reader

In this case controller which is being programmed must be connected with an external (slave) PRT series reader equipped with keypad. When programming from the external reader all programming steps and procedures are identical to programming from the local keypad. Also, LED/buzzer signaling is identical and occur simultaneously on both units (controller and reader). It is obvious, that this method of manual programming has practical sense for units not equipped with internal keypad (e.g. PR621, PR311BK and PR411) and only in case when system cannot be configured from PC.

Note: The external reader should be configured for RACS address ID=0 online mode and connected to controller via CLK and DTA lines. It is not required to disconnect the XM-2 module from system being programmed.

Memory Reset



The **Memory Reset** is a programming procedure which:

- clears all existing data in controller's memory
- restores default settings
- allows for programming of a new MASTER card
- allows for programming of a new MASTER PIN
- allows for programming of a new address (ID number)

Simplified Memory Reset Procedure - version 1




This method allows for programming of the new MASTER card only. This procedure doesn't require use of keypad. Programming steps:

- Remove all connections from CLK and DTA lines
- Short CLK and DTA lines
- Restart device (switch power supply off and then on or short RST contacts for a while) – all LED indicators become active

- Remove the bridge between CLK and DTA lines — the LEDs on the reader will be off, and the LED OPEN  (green) will start pulsing
- While the LED OPEN  is pulsing, read any card — this will be a new MASTER card
- The reader restarts automatically and switch to normal mode with address ID=00


Simplified Memory Reset Procedure - version 2

This method allows for programming of the new MASTER card and new address however it doesn't require use of a keypad.



- Remove all connections from CLK and IN3 lines
- Short CLK and IN3 lines
- Restart device (switch power supply OFF/ON or short RST programming contacts for a while) – all LED indicators become active
- Remove connection between CLK and IN3 lines — LED STATUS  (red) and LED OPEN  (green) will start pulsing
- While LED OPEN  is pulsing, read any card — this will be a new MASTER card
- Read MASTER card X times where X must be equal to the first digit of the required address then wait for two short beeps
- Read MASTER card Y times where Y must be equal to the second digit of the required address
- The reader will restart automatically and return to normal work with new (XY) address

Full Memory Reset Procedure

This procedure can be performed directly from the controller's keypad (if the controller has it) 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 mode address ID0** and be equipped with a keypad. This method of Memory Reset allows for programming of a new MASTER card and MASTER PIN and setting the new address (ID number).

- Remove all connections from CLK and DTA lines.
- Short CLK and DTA lines.
- Restart device (switch power supply off and then on or short RST contacts for a while) – all the LED indicators on the reader will be lit.
- Remove the bridge between CLK and DTA lines — the LEDs on the reader will be off, and the LED OPEN  (green) will start flashing.
- If the controller is equipped with keypad go to the next step if not then without switching the power off connect an external PRT series reader to it. It should be configured to the RACS mode address=ID0. The rest of the steps should be performed using this additional reader.
- Enter a new MASTER PIN code (3-6 digits) followed with the [#] key or skip this step pressing the [#] key alone.

- Read any card — it will be a new MASTER card — or skip this step by pressing the [#] key.
- Enter two digits (from 00 to 99 range). These digits program a new ID address of the controller. Eventually, instead of programming controller's address can press the [#] key alone. In the latter case, the controller will automatically assume address ID=00.
- After this action, the reader will restart automatically and return to normal working mode (enters Armed mode).

After **Memory Reset** procedure, controller resumes normal operation with new address. You can test it by means of MASTER card or PIN (if they were programmed). Using the MASTER card or PIN once, activates output REL1 and LED OPEN  for 4 seconds. Using MASTER card or PIN twice will switch the IO1 output to the opposite state and change a current controller's armed mode (LED STATUS  will change its color).

User Programming

The *User Programming* offers several programming commands which are accessible through two digits numbers. Optionally, programming commands may require authorization by means of proximity cards however by default it is not required.

Note: In locations indicated by <AUTH> abbrev. reader might require reading of the user card which is authorized for User Programming function. The need to use of authorized card can be switch on/off by setting adequate option for each User Programming command.

Symbols and abbreviations:

<AUTH> - authorisation request, controller wait for the user to enter its identifier. By default all function require authorization through valid user card and/or PIN. If required request for authorization can be removed by installer.

INSTALLER – INSTALLER identifier (card and/or PIN)

MASTER – MASTER identifier (card and/or PIN)

[NNN] – three digits which indicate user ID number (001..999)

<Card> - request to read user card

<PIN> - request to enter user PIN

(SK) – proprompt signal, encourage user to continue command

OK – OK signal, three short beeps, confirms success in programming or command

ERROR – error signal, informs about error in programming function or user command

[10][#]<AUTH>[10] Removing all users from memory

Command removes both Standard Users and Guest Users from the controller's memory.

[11][#]<AUTH>[NNN][Card] Programming card for the user with ID=NNN

Command programs card for the user with given ID=NNN number. If the presented card is already programmed to another user controller will generate ERROR signal and leave function.

[12][#]<AUTH>[NNN][PIN] Programming PIN for the user with ID=NNN

Command programs PIN for the user with given ID=NNN number. If the entered PIN is already programmed to another user controller will generate ERROR signal and leave function.

Note: When controller has to signal PIN code entry under duress, every programmed PIN code must differ from any other code by +/- 1 on last position.

[13][#]<AUTH>[NNN] Deleting user with ID=NNN

The given ID number is released and can be used to program new card/PIN.

[14][#]<AUTH>[NNN] Checking memory location for the user ID=NNN

Signal OK (***) means location is not occupied, ERROR signal (long beep) indicates user location is already occupied.

[15][#]<AUTH> [Card_1] [Card_2] ... [Card_N] Programming multiple cards

The ID numbers of programmed users is unknown, reader assigns them in first free (unoccupied) ID-s starting with address ID=100.

Note: If the controller has empty user list the new cards programmed by this function are assigned starting ID=100 and then going higher ID numbers. Thanks to this feature user can deduct which ID number will be assigned to programmed cards allowing to delete them selectively by corresponding ID.

[16][#]<AUTH>[NNN][P] Programming special options for the user with ID=NNN

The P value can be from range 1-8 and has following meanings:

P=[1] : Access disabled

P=[2] : Enabled for authorization of F1 key on terminal ID0

P=[3] : Enabled for authorization of F2 key on terminal ID0

P=[4] : Enabled for authorization of F1 key on terminal ID1

P=[5] : Enabled for authorization of F2 key on terminal ID1

P=[6] : Enabled for authorization of User Commands

P=[7] : Enabled for arming/disarming

P=[8] : Enabled for authorization of Function Cards

[17][#]<AUTH>[NNN][P] Deactivating option [P] for the user with ID=NNN

Command switches off given option for given user. The P value can be from range 1-8 and has the same meaning as in function [16].

[18][#]<AUTH> [P] Deactivating option [P] for all users

Command switches off given option for all users. The P value can be from range 1-8 and has the same meaning as in function [16].

[20][#]<AUTH>[20] Deleting all GUEST users

Once this command is entered all GUEST users are removed from the controller memory.

[21][#]<AUTH>[G][Card] Programming card for the GUEST with ID=[G]

Command programs card for the GUEST with given ID number. The [G] indicates GUEST number on the list and can be from range 0-7.

[22][#]<AUTH>[G][PIN] Programmin PIN for the GUEST with ID=[G]

Command programs PIN for the GUEST with given ID number. The [G] indicates GUEST number on the list and can be from range 0-7.

[23][#]<AUTH>[NNN] Removing GUEST with ID=[G]

Comands rmoves both card and PIN programmed for the GUEST user with ID=[G]. The [G] indicates GUEST number on the list and can be from range 0-7.

[31][#]<AUTH>[F] Programming AUX1 Flag

Command enables for the direct control of AUX1 Flag and thus corresponding output (when programmed). The F value can be from range 0-2 and has following meanings:

F=[0]: Clear flag

F=[1]: Set flag

F=[2]: Toggle flag on/off (switch to opposite state)

[32][#]<AUTH>[F] Programming AUX2 Flag

Command enables for the direct control of AUX2 Flag and thus corresponding output (when programmed). The [F] value can be from range 0-2 and has the same meanings as in function [31].

[33][#]<AUTH>[F] Programming LIGHT Flag

Command enables for the direct control of LIGHT Flag and thus corresponding output (when programmed). The [F] value can be from range 0-2 and has the same meanings as in function [31].

[34][#]<AUTH>[F] Programming Door Mode

Command enables for the direct control of Door Mode. The [F] value can be from range 0-3 and has following meanings:

F=[0]: Normal door mode

F=[1]: Unlocked door mode

F=[2]: Conditional Unlocked door mode

F=[3]: Locked door mode

[35][#]<AUTH>[F] Programming Identification Mode

Command enables for the direct control of Identification Mode. The [F] value can be from range 0-3 and has following meanings:

[F]=0: Card or PIN

[F]=1: Card only

[F]=[2]: PIN only

[F]=[3]: Card and PIN

[39][#]<AUTH> Activates Intruder Alarm Flag

Command activates (triggers) Intruder Alarm.

Installer Programming

In order to enter Installer Programming mode operator must use following command:

[01][#]<MASTER><INSTALLER> Entry to the Installer Programming mode

Once in the Installer Programming mode controller activates LED STATUS \otimes (to red) and LED SYSTEM \otimes . There are tens of commands available in this mode to allow detailed setup of the unit. Every command consist of few key as presented further in this section. With the first key pressed of the programming command LED-s start pulsing and continue in this state till moment when programming function is completed or terminated by programming error. If the function is accomplished properly controller generates <OK> acoustic signal or the <ERROR> sound when something went wrong. If operator stop programming for 4 minutes controller will automatically exit Installer Programming mode and return to the arming mode (either Armed or Disarmed) depending on the state it was before entering Installer Programming. Following programming commands are available in the Installer Programming mode:

[00][#] Exit from the Installer Programming mode

Command makes the controller leave the Installer Programming mode. Also, it can leave this mode automatically if no programming step is done through 4 minutes period.

[40][MN] Programing controller ID number (address)

Command programs controller address which can be from 00-99 range. Default: <ID=00> or another programmed during Memory Reset

[41][P][FW] Programming function for input IN1

The FW determines code of the function and [P] is used to program line as NO or NC. Setting P=0 configures line as normally open line while P=1 sets it as normally closed. The list of available FW functions is described in section Inputs. Default: <P=1>, <FW=01>, Door Contact, NC.

[42][P][FW] Programming function for input IN2

Programming rules as for IN1 input. Default: <P=1>, <FW=02>, Exit Button, NO

[43][P][FW] Programming function for input IN3

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO

[44][P][FW] Programming function for input IN4

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO. Line is available on PR411 controller only.

[45][P][FW] Programming function for input IN5

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO. Line is available on PR411 controller only.

[46][P][FW] Programming function for input IN6

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO. Line is available on PR411 controller only.

[47][P][FW] Programming function for input IN7

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO. Line is available on PR411 controller only.

[48][P][FW] Programming function for input IN8

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO. Line is available on PR411 controller only.

[49][P][FW] Programming function for IN1 on XM-2 I/O module

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO.

[50][P][FW] Programming function for IN2 on XM-2 I/O module

Programming rules as for IN1. Default: <P=1>, <FW=00>, None, NO.

[51][P][FW] Programming function for REL1 relay output

The FW determines code of the output function. The list of available FW functions is described in section Outputs. Default: <FW=99>, Door Lock.

[52][P][FW] Programming function for IO1 transistor output

Programming rules as for REL1 output. Default: <FW=07>, Prealarm + Door Ajar + Forced Entry.

[53][P][FW] Programming function for IO2 transistor output

Programming rules as for REL1 output. Default: <FW=00>, Disarmed mode.

[54][P][FW] Programming function for CLK transistor output

Programming rules as for REL1 output. Default: <FW=100>, Reserved.

[55][P][FW] Programming function for DTA transistor output

Programming rules as for REL1 output. Default: <FW=100>, Reserved.

Note: Note that CLK and DTA lines are allowed as general purpose output lines if they are not used for communication whit external PRT series reader nor XM-2 extension module.

[59][P][FW] Programing REL1 output on XM-2 I/O module

Programming rules as for REL1 output. Default: <FW=99>, Door Lock.

[60][P][FW] Program REL2 output on XM-2 I/O module

Programming rules as for REL1 output. Default: <FW=07>, Prealarm + Door Ajar + Forced Entry.

[61][P][Q][R][S] Programming readers

Programming rules:

[P]=0: Terminal ID0, interface RACS is disabled

[P]=1: Terminal ID0, interface RACS is enabled

[Q]=0: Terminal ID1, interface RACS is disabled

[Q]=1: Terminal ID1, interface RACS is enabled

[R]=0: Terminal ID0, interface Wiegand is disabled (valid for PR411 controller only)

[R]=1: Terminal ID0, interface Wiegand is enabled (valid for PR411 controller only)

[S]=0: Terminal ID1, interface Wiegand is disabled (valid for PR411 controller only)

[S]=1: Terminal ID1, interface Wiegand is enabled (valid for PR411 controller only)

Notes: Enabling RACS terminal ID0, RACS terminal ID1 or XM-2 extension module causes automatically CLK and DTA lines are forbidden as general purpose outputs. Also, enabling Wiegand terminal ID0 forbids IN1 and IN2 as programmed inputs while enabling Wiegand terminal ID1 forbids IN3 and IN4 inputs respectively.

[62][X] Programming XM-2 I/O extension module

Programming [X]=1 enables XM-2 module while [X]=0 disables it. Default: <X=0>, XM-2 disabled.

Note: When XM-2 is enabled it automatically cause the CLK and DTA lines are forbidden as general purpose outputs.

[63][OT] Programming Door Unlock Time

The OT must be within 00-99 range and determines door unlock time in seconds. Setting [OT]=00 makes door will be controlled in bistable (latch) mode – whenever access is granted it will switch to reverse state for unlimited time till moment when access is granted again. Default: <OT=04>.

[64][CD] Programming Door Open Timeout

The CD must be within 01-99 range and determines time allowed to close the door in seconds. Setting [CD]=00 is forbidden. Default: <OT=09>.

[65][A] Programming Identification Mode

Commands switches controller to Identification Mode selected through [A] parameter. The [A] must be within 0-3 range and has following meanings:

[A]=0: Card or PIN mode

[A]=1: Card only mode

[A]=2: PIN only mode

[A]=3: Card and PIN mode

[66][F] Programming option: Device temporary blocked after 5 wrong cards/PINs

When [F]=1 option is enabled while [F]=0 makes option disabled.

[67][F] Programming Duress function

When [F]=1 controller will signal entry of the PIN code under duress, when [F]=0 function will be forbidden.

[68][1] Programming Auto-relock function

When [F]=1 function will be enabled, when F=0 disabled.

[69][NF][F] Programming autohorisation request for User Commands

The [NF] indicates the User Command ID number, if [F]=0 the given User Command doesn't require authorization, if [F]=1 User Command requires authorization.

[69][*][0] Removing authorization request for all User Commands

Command removes necessity for authorization for for all User Commands.

[69][*][1] Setting authoristaion request for all User Commands

Command activates necessity for authorization for for all User Commands.

Note: By default, all User Commands require authorization.

[70][X] Programming option: Enable Door Alarm signalling on internal buzzer

When [X]=1 option is enabled, when [X]=0 disabled.

[71][FF][A] Programming [F1] key on Terminal ID0

[FF] represents the function code according to table in section Function Keys (earlier in this document) while [A] sets autohorisation request on/off. Program:

A=1: Authorization required

A=0: Authorization not required

[72][FF][A] Programming [F2] key on Terminal ID0

Programming rules same as for [F1] key.

[73][FF][A] Programming [F1] key on Terminal ID1

Programming rules same as for [F1] key.

[74][FF][A] Programming [F2] key on Terminal ID1

Programming rules same as for [F1] key.

[75][Card] Programming new MASTER card

The old MASTER card is deleted and replaced by the new one.

[76][PIN][#] Programming new MASTER PIN

The old MASTER PIN is deleted and replaced by new one.

[77][Card] Programming new INSTALLER card

The old INSTALLER card is deleted and replaced by new one.

[78][PIN] Programming new INSTALLER PIN

The old INSTALLER PIN is deleted and replaced by new one.

[79][APB] Programming Anti-passback function

Command sets the APB function. Default: <APB=0>, APB disabled. Program:

[APB]=0: Anti-passback disabled

[APB]=1: Soft Anti-passback enabled

[APB]=2: Hard Anti-passback enabled

[80][TA] Programming True Anti-passback option

Program:

[TA]=0: True Anti-passback disabled

[TA]=1: True Anti-passback enabled

[81][SS] Program AUX1 Timer in seconds

Command defines the AUX1 Timer period which can be in range SS=00..99 (seconds). When SS=00 AUX1 Timer operates in latch mode – it switches to opposite state till next command will change its state again.

[81][*][MM] Program AUX1 Timer in minutes

Command defines the AUX1 Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[82][SS] Program AUX2 Timer in seconds

Command defines the AUX2 Timer period which can be in range SS=00..99 (seconds). When SS=00 AUX2 Timer operates in latch mode – it switches to opposite state till next command will change its state again.

[82][*][MM] Program AUX2 Timer in minutes

Command defines the AUX2 Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[83][SS] Program LIGHT Timer in seconds

Command defines the LIGHT Timer period which can be in range SS=00..99 (seconds). When SS=00 LIGHT Timer operates in latch mode – it switches to opposite state till next command will change its state again.

[83][*][MM] Program LIGHT Timer in minutes

Command defines the LIGHT Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[84][SS] Program TAMPER timer in seconds

Command defines the TAMPER Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[84][*][MM] Program TAMPER Timer in minutes

Command defines the TAMPER Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[85][SS] Program INTRUDER Timer in seconds

Command defines the INTRUDER Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[85][*][MM] Program INTRUDER Timer in minutes

Command defines the INTRUDER Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[86][SS] Program DURESS Timer in seconds

Command defines the DURESS Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[86][*][MM] Program DURESS Timer in minutes

Command defines the DURESS Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[87][SS] Program TROUBLE Timer in seconds

Command defines the TROUBLE Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[87][*][MM] Program TROUBLE Timer in minutes

Command defines the TROUBLE Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[88][SS] Program ENTRY DELAY Timer in seconds

Command defines the ENTRY DELAY Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[88][*][MM] Program ENTRY DELAY Timer in minutes

Command defines the ENTRY DELAY Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[89][SS] Program EXIT DELAY Timer in seconds

Command defines the EXIT DELAY Timer period which can be in range SS=01..99 (seconds). Setting SS=00 is forbidden.

[89][*][MM] Program EXIT DELAY Timer in minutes

Command defines the EXIT DELAY Timer period which can be in range MM=01..99 (minutes). Setting MM=00 is forbidden.

[90] [*] Disables Facility Code function

Commands deactivates entirely Facility Code function.

[90][WCN][ABCDEFGH] Programming Facility Code function

Command enables definition of so called Facility Code (Site Code) and accompanying parameters. Programming:

[WCN]: Defines Facility Code number, range 000..255

[ABCDEFGH]: Each letter represent status of individual option and may be set to 0 or 1, 0 means option deactivated, while 1 means option is active. Assignments:

A : Option 1 (Op.1: Access disabled)

B : Option 2 (Op.2: Enabled for authorization of F1 key on terminal ID0)

C : Option 3 (Op.3: Enabled for authorization of F2 key on terminal ID0)

D : Option 4 (Op.4: Enabled for authorization of F1 key on terminal ID1)

E : Option 5 (Op.5: Enabled for authorization of F2 key on terminal ID1)

F : Option 6 (Op.6: Enabled for authorization of User Commands)

G : Option 7 (Op.7: Enabled for arming and disarming)

H : Option 8 (Op.8: Enabled for authorization of Function Cards)

Example: programming [70][128][00110001] sets Facility Code=128 and activates options: Op.3, Op.4 and Op.8 for cards which comply with programmed Facility Code.

[91] [C] Programming option: Access disabled when controller armed

When [C]=1 option is enabled, when [C]=0 disabled.

[92][NK][FN][A][Card] Programming Function Cards

Command defines so called Function Cards and accompanying parameters: Program:

[NK]: Specifies Function Card ID number, range 00..31

[FN]: Specifies action for programmed Function Card according to table in section Function Cards (earlier in this document)

[A]: Toggles on/off request for authorization when Function Card is used, if [A]=0 Function Card doesn't require authorization, if [A]=1 it will require authorization.

[93][Card] Removing given Function Card

Command removes presented card from the list of Function Cards.

[93][NK] Removing Function Card with given index

Command removes the Function Card with entered ID number.

[93][*] Removing all Function Cards

Command removes all Function Cards already defined in the device.

[94][BK] Programming keypad backlight level

Command allows to set keypad backlight level. Programming:

BK = 0 for 0% keypad backlight level (no backlight)

BK = 1 for 20% keypad backlight level

BK = 2 for 40% keypad backlight level

BK = 3 for 60% keypad backlight level

BK = 4 for 80% keypad backlight level

BK = 5 for 100% keypad backlight level (max. backlight)

[95][BK] Programming Buzzer loudness level

Command allows to set keypad backlight level. Programming:

BK = 0 for 0% buzzer loudness level (no buzzer signal)

BK = 1 for 20% buzzer loudness level

BK = 2 for 40% buzzer loudness level

BK = 3 for 60% buzzer loudness level

BK = 4 for 80% buzzer loudness level

BK = 5 for 100% buzzer loudness level (max. loudness)

Acoustic and Optical Signals




Acoustic Signals

PR311SE, PR311SE-BK, PR611 controllers as well as PR621 ones generate acoustic signals using internal speakers and thorough external PRT reader units. The PR411 controller is not equipped with internal buzzer, it generates acoustic signals via buzzers located on the external PRT series readers.

Type	Description
One short signal (1 x BEEP)	Card read or key pressed.
Two short signals (2 x BEEP)	Prompt signal, command accepted however system waits for further steps.
Three short signals (3 x BEEP)	Signal OK. Command correct or access granted.
One long signal	Error or unknown card/PIN
Two long signals	Correct card/PIN however access denied due to the other rules

Optical Signals

PRxx1 controllers feature optical signals generated using LED displays available on ID0/ID1 terminals. PR411 controllers feature optical signals on external readers and LEDs located on the electronic module as well.

Type	Color	Description
LED STATUS 	Dual color: red or green	RED, the controller is in the armed mode. GREEN, the controller is disarmed.
LED OPEN 	Green	Blinking while door is unlocked. While pulsating, a controller awaits for a user to complete its login process.
LED SYSTEM 	Orange	It indicates a controller is in the wait mode to complete a command. When permanently activated, a system malfunction is detected and the controller stops operating until all problems solved.

Contact

Roger sp.j.

82-400 Sztum

Gościszewo 59

Tel.: +48 55 272 0132

Fax: +48 55 272 0133

e-mail: biuro@roger.pl