

Roger Access Control System

Functional description of PRxx2 series controllers

Document version: Rev. K

This document refers to following products:

*PR102DR, PR402DR, PR402DR-BRD, PR402DR-12VDC, PR402DR-12V-BRD, PR402-BRD,
PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302*



Contents:

I. General	4
1.1 Introduction.....	4
1.2 Design and architecture.....	4
1.3 Features of PRxx2 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 CPR unit).....	9
2.2 Communication.....	11
2.2.1 RS485 Interface.....	11
2.2.2 Controller address.....	13
2.2.3 RACS CLK/DTA interface.....	13
2.2.4 XM-2 I/O expander.....	14
2.2.5 XM-8 I/O expander.....	14
2.2.6 PSAM-1 power supply monitoring module.....	14
2.2.7 HRT82FK function key panel.....	15
2.2.8 Wiegand/Magstripe interface readers.....	15
2.2.9 Biometric readers.....	16
2.2.10 Long range proximity readers.....	16
2.3 Users.....	16
2.4 Identification Modes.....	17
2.5 Door Modes.....	17
2.6 Armed/Disarmed Modes.....	18
2.7 Access Rights.....	19
2.8 Facility Code.....	21
2.9 Door Alarms.....	21
2.10 System Flags (Timers).....	22
2.11 Anti-passback.....	24
2.12 Alarm Zones.....	27
2.13 Inputs.....	28
2.14 Outputs.....	33
2.15 Function keys.....	38
2.16 Schedules and Auxiliary Conditions.....	41
2.17 Special options.....	43
2.17.1 Two User Mode.....	43
2.17.2 Conditional Access.....	44
2.17.3 High Security Mode.....	44
2.18 Keypad Commands.....	45
2.19 Time and Attendance (T&A).....	48
2.19.1 Time&Attendance based on Attendance Areas within PR Master software.....	48
2.19.2 Time&Attendance based on RCP Master software.....	48
2.20 Login limits.....	51
III. Programming	53
3.1 General tab.....	54
3.2 Terminal ID1 tab.....	54
3.3 Terminal ID0 tab.....	56
3.4 Access tab.....	57
3.5 Arming tab.....	59
3.6 Options tab.....	62

3.7 Advanced tab..... 66
 3.8 APB tab 69
 3.9 Timers tab 70
 3.10 Keypad commands tab 71
 3.11 Input IN1...IN8 tabs 72
 3.12 Output IO1...IO2 tabs 73
 3.13 Output REL1...REL2 tabs 74
 3.14 XM-2 Inputs tab 75
 3.15 XM-2 Outputs tab 76
 3.16 F1...F4 keys tabs 77
 3.17 HRT82FK tabs 78

Typing conventions

Functions, options and commands

bold letter

Examples

italics letters

Specific names related to RACS 4 system

with first capital letter

STATUS, FLAG OR TIMER

capital letters

Notes

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

I. GENERAL

1.1 Introduction

This document applies to PRxx2 series advanced controllers i.e. devices with built-in EM125kHz reader (PR602LCD, PR612, PR622, PR312EM and PR302), with built-in MIFARE® reader (PR312MF), with both built-in EM125kHz/MIFARE readers (PR602LCD-DT) as well as devices without built-in reader for installation inside metal box preferably in some distance from door (PR102DR, PR402-BRD, PR402DR, PR402DR-BRD). PR402-BRD controller is discontinued and it is replaced by PR402DR controller which is available both in plastic enclosure for installation on DIN 35mm rail (PR402DR) or as electronic module (PR402DR-BRD). There are also available both versions of PR402DR controller adapted to only 12VDC power supply. The name PR402 applies to all possible models of this controller while the name PR402DR applies to the latest versions. PR102DR controller was developed on the basis of popular PR402DR controller as cost effective solution with simplified hardware. PR102DR controller similarly to PR402DR controller is available both in plastic enclosure for installation on DIN 35mm rail (PR102DR) or as electronic module (PR102DR-BRD). In the present document the name PR102DR applies to all versions of the controller. PR602LCD-DT controller replaces discontinued PR602LCD controller.

This manual describes functions and options of PRxx2 series controllers which can be configured by means of PR Master software. The document includes information on architecture, communication and operation modes. Information which is useful in installation is provided in installation guides for particular controller while comprehensive information on PR Master software is available in its manual (including Schedules, Access Groups, Access Zones, Online Monitoring, Event history, etc.).

1.2 Design and architecture

The PRxx2 series controllers are single door access controllers for read in/out door control. Each PRxx2 controller can work with two logical access points (readers) called respectively: Terminal ID0 and Terminal ID1. PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302 controllers are equipped with built-in reader which is logically treated as Terminal ID1. The PR402 and PR102DR controllers are not equipped with any built-in reader but they can work with two external readers. Generally, the PRxx2 controllers are designed to operate with PRT series readers (from Roger) configured to RACS CLK/DTA format or with Wiegand 26-66bit or Magstripe formats. The PR602LCD-DT controller which is equipped with keypad and LCD, is also recommended as Time&Attendance terminal – see 2.19.2 Time&Attendance based on RCP Master software. PRxx2 series controllers contrary to PRxx1 series controllers are equipped with built in memory for event storing and with real time clock (RTC). It means that in case of PRxx2 controllers it is not required to use CPR series network controller in order to ensure time based functions and event recording. The memory buffer in controllers can store up to 32000 events. CPR series network controllers are necessary to ensure such global functions as Global APB or Alarm Zones. (see 2.11 Anti-passback and 2.12 Alarm Zones). Additionally CPR32-NET-BRD unit enables integration with intruder alarm panels of INTEGRA (SATEL) series and wireless door locks of SALLIS (SALTO) and APERIO (ASSA ABLOY) systems, it performs the role of Ethernet-RS485 interface, enables operation with event buffer on external memory card (30 million events), enables synchronization with NTP server and encrypts communication by means of AES128 CBC standard.

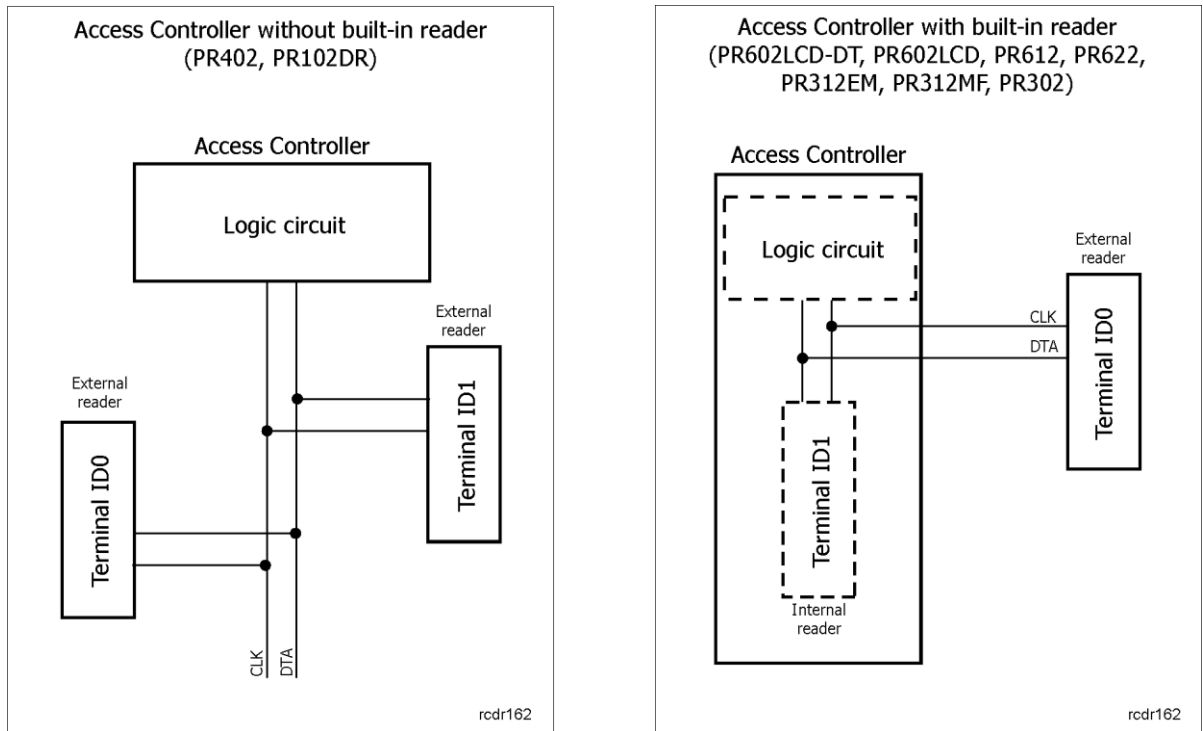


Fig. 1 General structure of controllers and readers

PRxx2 controller can operate with up to 4000 users. Each user has its own ID number and may have proximity card and/or PIN. Controller’s 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. PRxx2 controllers can operate fully autonomously (Offline and Online Standalone System) or in the Network System with or without CPR32-SE-BRD/CPR32-NET-BRD network controller. PRxx2 controllers must be programmed from PC. Contrary to PRxx1 series controllers, PRxx2 controllers cannot be programmed manually but some commands can be entered manually from keypad. These commands are rather used for device control and not programming (see 2.18 Keypad Commands). Remote programming must be done by means of PC with PR Master software (Roger). The communication with single controller or management of the whole access control system requires CPR32-NET-BRD network controller or dedicated interface device e.g.:

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

Table 1. List of PRxx2 series controllers

Controller	Power supply	NO/NC inputs	Transistor outputs	Relay outputs	Built-in reader	External readers	Built-in keypad	Other
PR402DR/ PR402DR-BRD	12VDC, 24VDC, 18VAC	8	2	1 x 1.5A/30V, 1 x 5A/30VDC and also 5A/230VAC	-	2 x PRT, Wiegand or Magstripe	-	- in DIN35 mm enclosure (PR402DR) or as electronic module (PR402DR-BRD), - built-in 1.2A/12VDC power supply unit, - direct connection of backup battery enabled
PR402DR-12VDC/ PR402DR-12V-BRD	12VDC	as above	as above	as above	as above	as above	as above	as above
PR402-BRD	12VDC, 18VAC	4	as above	2 x 5A/30VDC and also 5A/230VAC	as above	as above	as above	- electronic module, - built-in 1.2A/12VDC power supply unit, - direct connection of backup battery enabled.
PR102DR/ PR102DR-BRD	12VDC	2	1	1 x 1.5A/30V	-	2 x PRT	-	- in DIN35 mm enclosure (PR102DR) or as electronic module (PR102DR-BRD).
PR602LCD-DT	12VDC	3	2	1 x 1.5A/30V	EM125kHz and MIFARE	1 x PRT, Wiegand or Magstripe	keypad with 4 function keys	- outdoor and indoor versions available, - LCD.
PR602LCD	as above	as above	as above	as above	EM125kHz	as above	as above	as above
PR612	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	+	- outdoor version, - screw terminals.
PR622	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	-	as above
PR312EM	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT	keypad with 2 function keys	- outdoor version, - connection cable, - version without keypad available.
PR312MF	as above	as above	as above	as above	MIFARE	as above	as above	as above
PR302	12VDC	3	2	1 x 1.5A/30V	EM125kHz	1 x PRT or Wiegand	+	- indoor version, - screw terminals, - possible refitting to version without keypad.

1.3 Features of PRxx2 series controllers

Features of PRxx2 series controllers:

- Single door, read in/out access control
- Connection of PRT series readers (Roger)
- Connection of Magstripe or Wiegand third party readers (PR402, PR602LCD-DT, PR602LCD and PR302)
- Operation in Standalone or Network systems
- Real Time Clock with a battery back-up
- Programmable inputs/outputs
- DIN RAIL 35mm enclosure (only PR402DR and PR102DR)
- Elevator access control (max. 32 floors, XM-8 expander required)
- Support for XM-2 I/O expander
- Firmware upgrade through RS485 serial port
- Communication with controllers by RS485 bus
- Management through LAN/WAN (CPR32-NET-BRD, UT-4DR or UT-4 required)
- PR Master management and monitoring software (Windows XP and newer)
- Integration with alarm systems via I/O lines and Alarm Zones (max. 32 Alarm zones in the system)
- Integration with CCTV systems
- User identification by means of proximity card or PIN
- 32000 event buffer (FIFO)
- 4000 users
- 250 Access Groups
- 99 General Purpose Schedules
- 128 time periods within single Schedule
- 4 Holiday Schedules (H1-H4)
- Programmable validity time for user proximity card or PIN
- Programmable user login limits (not renewable and renewable)
- Two User Mode (two users required to open door)
- Conditional Access (access allowed when authorized user present)
- High Security Mode (identification on both readers required)
- View Map, Evacuation Monitor, Access Point Monitor (in Online Monitoring)
- Random user inspection
- Local Anti-passback (single door)
- Global Anti-passback (multiple doors, CPR32-SE-BRD or CPR32-NET-BRD required)
- Time&Attendance registration
- CE mark

II FUNCTIONAL DESCRIPTION

2.1 Available scenarios of operation

2.1.1 Standalone System

In standalone mode access controllers operate autonomously and they do not exchange information with other devices in the system. In this mode events are stored in the internal memory buffer of the access controller. All time related functions are controlled by internal clock circuit which is equipped with a battery back-up. Connection to RS485 communication bus is required only for uploading the configuration to the controller and downloading events from the controller. It is not necessary to maintain permanent connection with PC (PR Master software) but such connection can be ensured in order to facilitate further servicing. No global functions (Global APB, Alarm Zones) are available in Standalone system. Offline Standalone System consists of individual controllers which are not connected RS485 communication bus. They must be configured separately by means of temporary connection through communication interface device (e.g. RUD-1). Online Standalone System is based on permanent connection of all controllers to RS485 bus in order to facilitate their programming and event downloading. Such system is not recognized as Network System because RS485 bus in such case is used only for management of standalone controllers.

Note: PRxx2 series controller cannot be programmed manually by means of keypad, therefore it is recommended to configure its ID address before installation in the building. The connection to a PC requires an adequate interface device (e.g. RUD-1, UT-2USB, UT-4DR) or CPR32-NET-BRD. Factory default address of the controller is ID=0 and devices connected to RS485 bus must have different addresses in range of 00..99 or communication conflict occurs (see 2.2.2 Controller address).

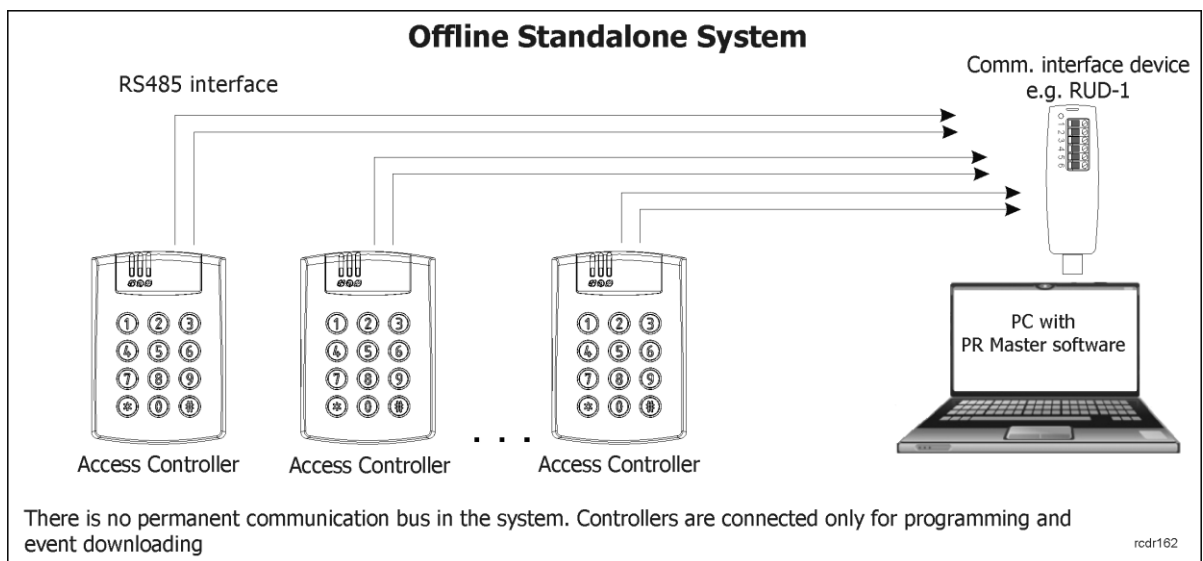


Fig. 2 Standalone system (Offline)

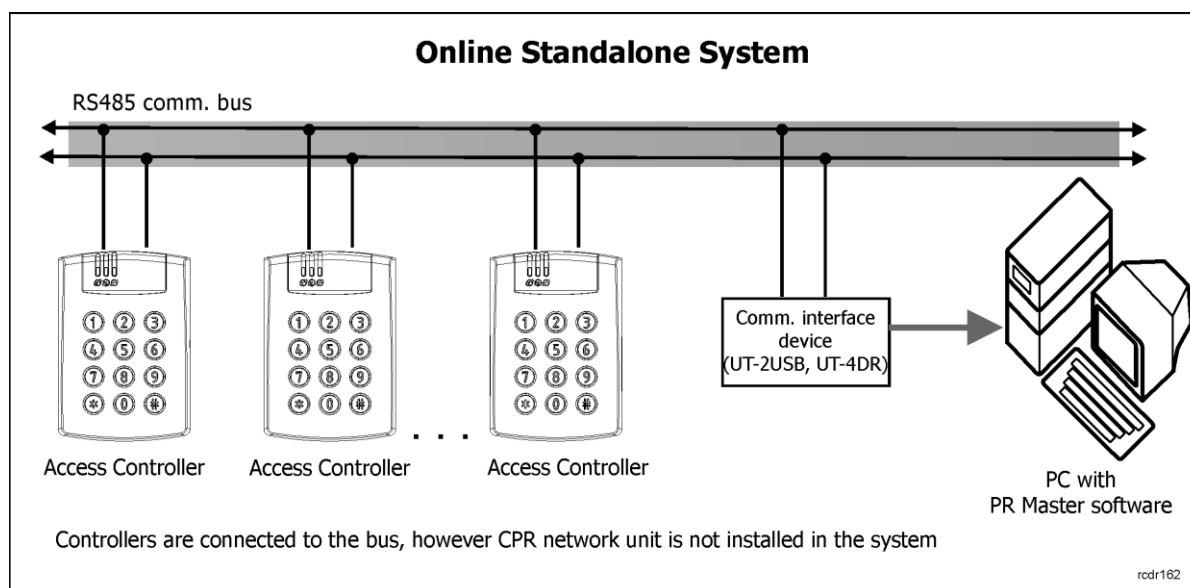


Fig. 3 Standalone System (Online)

2.1.2 Network System (with CPR unit)

Whenever an access control system is equipped with RS485 communication bus and it is used for data transmission between various devices connected to the bus, then such system is Network System and is called Integrated Access Control System (IACS). In the RACS 4 system the presence of a CPR32-SE-BRD or CPR32-NET-BRD unit makes the system IACS type. It is recommended to use Network System in particular when global functions such as Global APB or Alarm Zones are required or new features offered by CPR32-NET-BRD are required.

Note: The presence of communication bus does not imply that particular access control system is IACS type. If communication bus is used only for controller programming and event downloading then such system is called Online Standalone system.

In case of PRxx2 series controllers CPR32-SE-BRD and CPR32-NET-BRD offer following functionalities:

- Events are not stored in controller memory buffers but in CPR memory buffer (250 000 events)
- Global APB (see 2.11 Anti-passback),
- Alarm Zones (see 2.12 Alarm Zones),
- Controller's date/time synchronization by the CPR internal clock

Additionally, CPR32-NET-BRD offers:

- Software integrations with INTEGRA (SATEL) alarm system and SALLIS (SALTO) wireless door locks or APERIO (ASSA ABLOY) wireless door locks
- Built-in Ethernet-RS485 communication interface
- Event buffer on optional AX-9 memory card (33 million events)
- Communication encrypted with AES128 CBC standard
- Clock synchronization with NTP servers

In case of CPR failure the system automatically switches to online standalone mode and all controllers operate in this mode till communication with CPR is restored. In case of such failure the system still operates properly i.e. users and their access rights are maintained, controllers open doors properly and events are recorded in controller buffers.

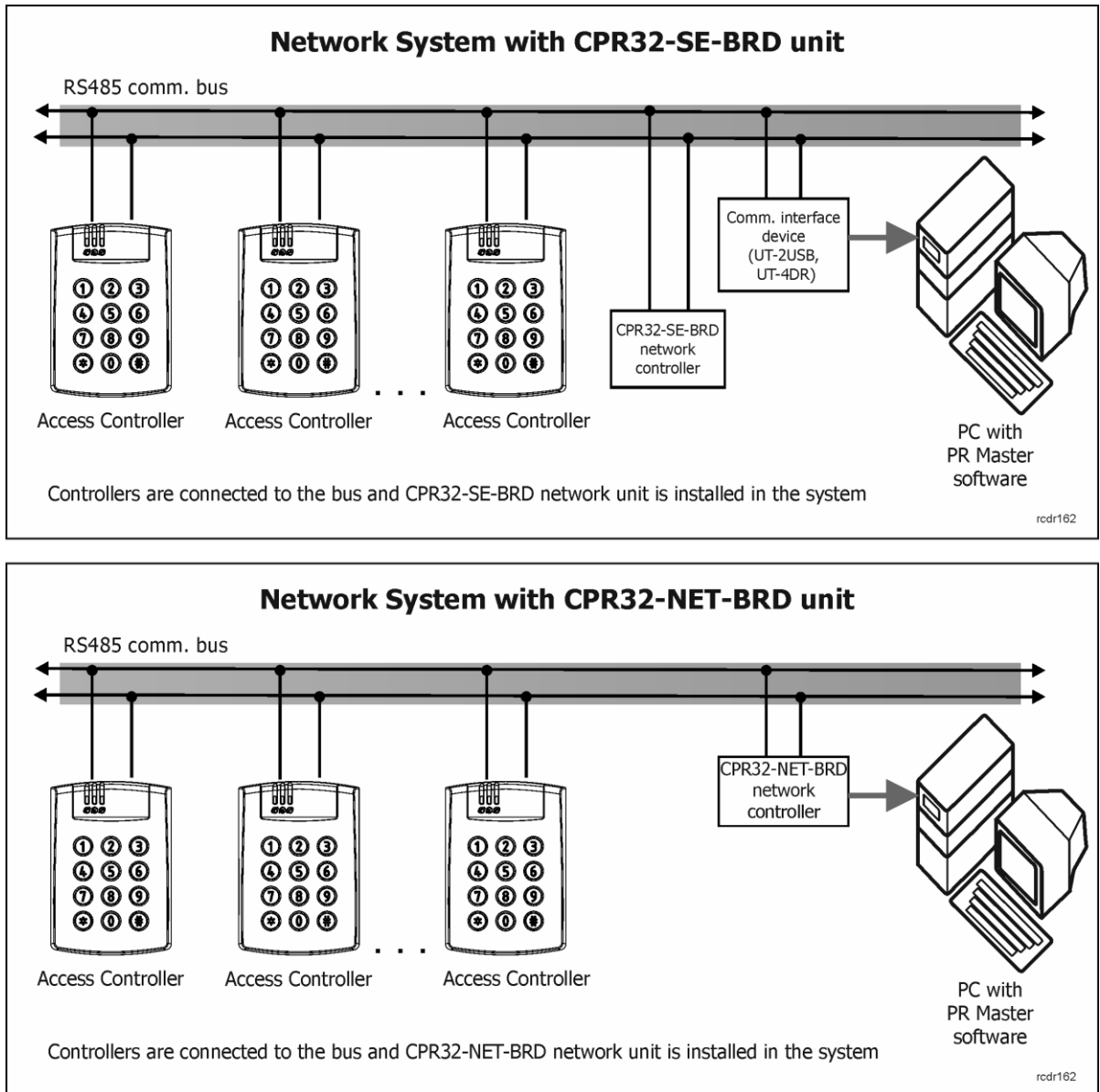


Fig. 4 Network System (with CPR unit)

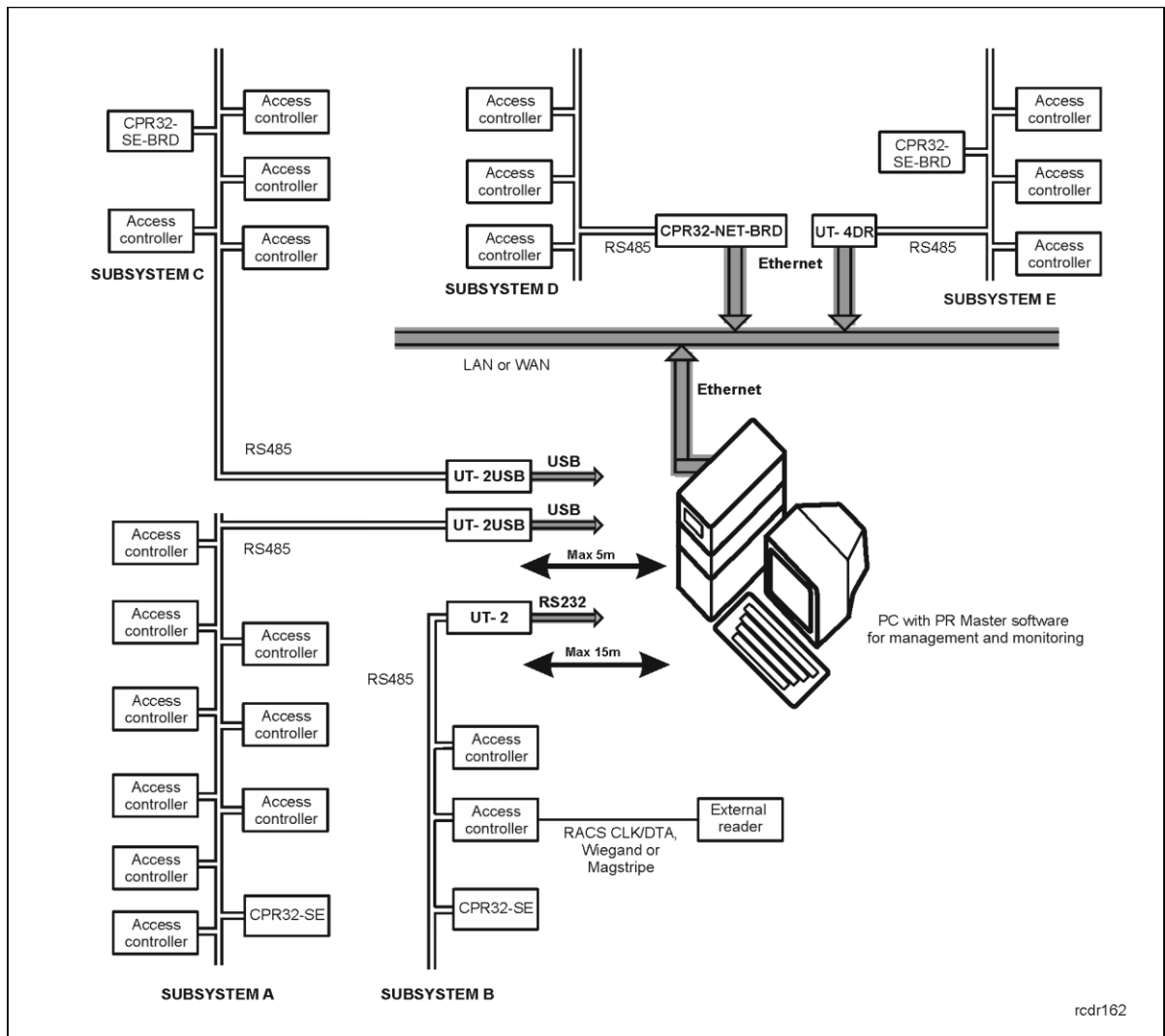


Fig. 5 Example of RACS 4 architecture in Network System

Following rules are valid for RACS 4 system shown in figure 5:

- The maximal number of subsystem connected to PC cannot exceed 250 and the maximal number of access controllers within the subsystem cannot exceed 32 units,
- Each subsystem must be connected to PC by individual communication interface device (number of USB ports can be increased by means of USB hub and in case of Ethernet a switch or router can be used),
- All access controllers are single door controllers for read in/out door control and external readers can be connected to the controllers,
- CPR units are optional devices and they enhance functionality of RACS 4 system,
- PC with PR Master software does not have to be switched on or connected all the time in order to ensure operation of access control system. It is necessary only if the administrator requires monitoring of event and alarms and wants to supervise the system,
- All cable connections to access control devices can be made by means of unshielded twisted pair (UTP cat. 5) or any other signal cables.

2.2 Communication

2.2.1 RS485 Interface

PRxx2 controllers are equipped with RS485 communication interface. The interface can be used for communication and programming. Controller connected to RS485 bus must their addresses

configured in range of 00..99. The communication bus may accommodate up to 32 access controllers and single CPR unit which does not require address setting. The RACS 4 system communication bus topology is fairly flexible. Tree-like structures as well as star-like topologies are allowed while loop topology is forbidden (see fig. 6). Any signal cables can be used for RS485 communication bus, however unshielded twisted-pair (U/UTP cat. 5) is recommended. Terminating resistors at either end of the communication bus are not required. Shielded cables can be used if strong electromagnetic interferences are expected in the area. Maximum cable lengths in the RACS 4 system are as follows::

- between any controller and CPR32-NET-BRD unit: 1200m,
- between any controller and communication interface device: 1200m,
- between CPR32-SE-BRD and communication interface device: 1200m.

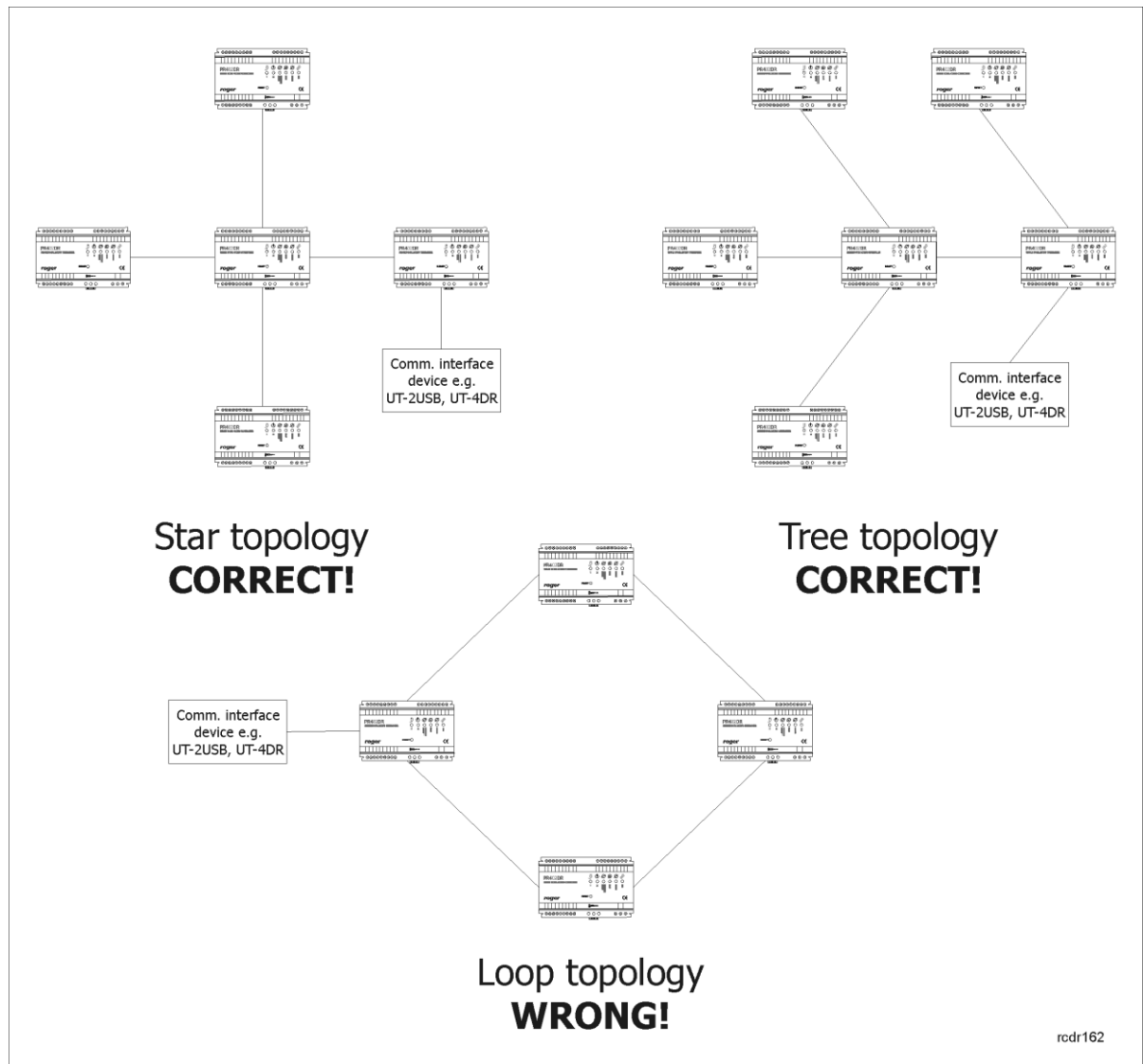


Fig. 6 Possible topologies of RS485 bus connections

Note: All devices connected to RS485 bus must have 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 built-in power supply units (PR402).

The structure with RS485 communication bus, access controllers and CPR unit is called the Access Control Network or simply Network (or Subsystem). Each Network in the RACS 4 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. VCP is available in such communication interfaces as RUD-1 or UT-2USB while Ethernet port is available in UT-4, CPR32-NET-BRD and UT-4DR.

Each type of PRxx2 controller can manage single door in read in or read in/out mode. Presently, RACS 4 permits integration of up to 250 Networks (Subsystems), each including up to 32 controllers (but maximal number of controllers equals to 1000). 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, RUD-1 interface device is recommended as it provides built-in 12VDC output.

2.2.2 Controller address

Every controller connected to RACS 4 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), manually during reset (see Installation Guide of particular controller), by means of jumpers (PR402DR, PR102DR) or by assigning "FixedID" to the controller. The last option is particularly useful if there is a risk that someone will accidentally change controller address causing disruption of the whole system. The fixed address can be set, changed or cleared only by means of RogerISP software during firmware upgrade procedure.

PR402DR and PR102DR controllers offer 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 by any other method. For details regarding various address settings refer to the relevant Installation Guide.

2.2.3 RACS CLK/DTA interface

Besides the RS485 communication bus, PRxx2 controllers feature also RACS CLK/DTA interface which is used for connection of Roger peripheral devices. Following devices can be connected to the RACS CLK/DTA bus:

- primary reader (Terminal ID0, address ID=0),
- secondary reader (Terminal ID1, address ID=1),
- auxiliary reader at Terminal ID0, address ID=2 – see 2.17.3 High Security,
- auxiliary reader at Terminal ID1, address ID=3 - see 2.17.3 High Security,
- XM-2 I/O expander, address ID=5 – see 2.2.4 XM-2 I/O expander,
- XM-8 I/O expander, address range ID=8...11 – see 2.2.5 XM-8 I/O expander,
- PSAM-1 module, address ID=4 – see 2.2.6 PSAM-1 power supply monitoring module
- HRT82FK function key panel, address ID=12 – see 2.2.7 HRT82FK function key panel

For CLK/DTA lines any type of signal cable can be used. There is no need to use shielded cables and usually U/UTP cat. 5 is applied. The maximum cable length between controller and external reader and/or XM expander is limited to 150m. Similarly as in case of RS485 bus, all devices connected to CLK/DTA line should have common negative supply terminals. Such condition is usually satisfied because devices connected to CLK/DTA line are usually directly supplied from controller (PR402). Otherwise negative terminal of each reader must be connected to respective controller's GND or COM terminals.

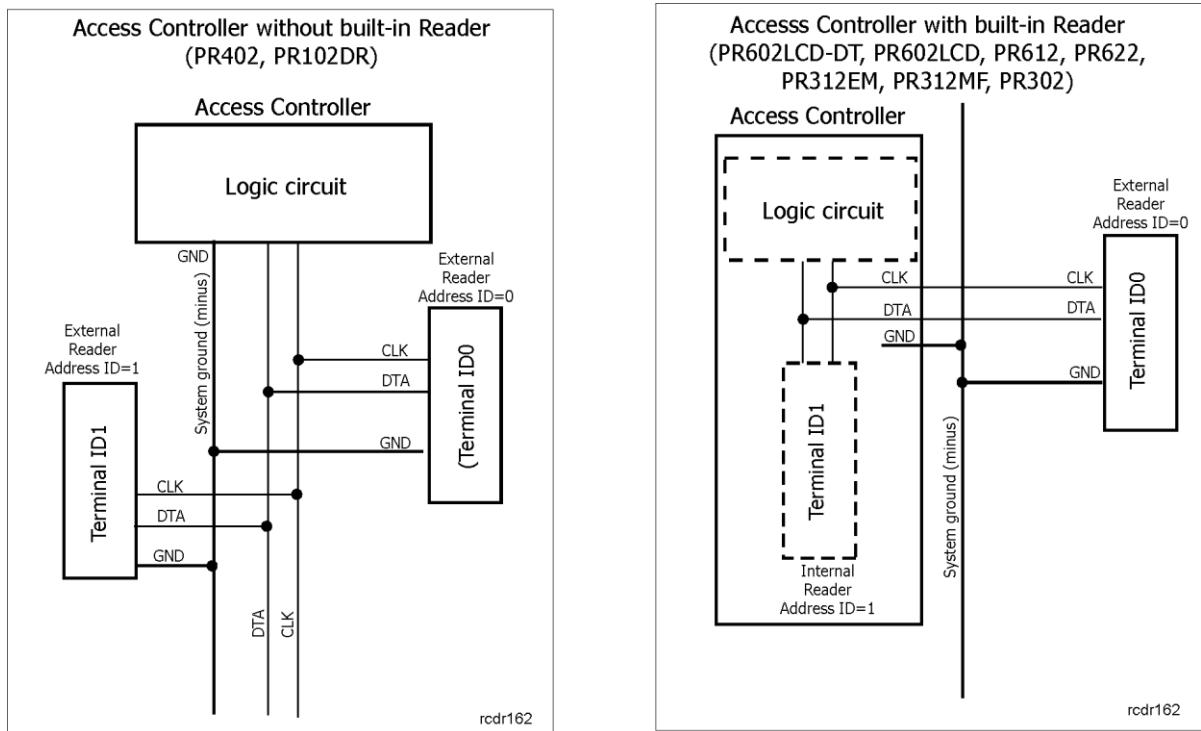


Fig. 7 RACS CLK/DTA interface

2.2.4 XM-2 I/O expander

PRxx2 series controller can operate with single XM-2 I/O expander. This expander offers two NO/NC inputs and two relay outputs. Both inputs and outputs of XM-2 can be programmed in the same way as inputs/outputs of the controller. The XM-2 can be used to extend number of available inputs/outputs and/or separate relay output from terminal. Such separation may be beneficial in case of PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302 controllers as they are installed near the door and can suffer from intruder. The XM-2 expander connected to controller must be configured with address ID=5. Digital communication between controller and XM-2 expander is performed by means of RACS CLK/DTA bus. For more information on XM-2 module refer to its Installation Guide which is available at www.roger.pl.

2.2.5 XM-8 I/O expander

PRxx2 series controller can operate with up to four XM-8 I/O expanders in address range ID=8...11. The XM-8 expander is used in elevator access control. It offers 8 relay outputs at each XM-8 expander and in case of four XM-8 it can control up to 32 floors in the building. Digital communication between controller and XM-8 expander is performed by means of RACS CLK/DTA bus. For more information on XM-8 expander refer to its Installation Guide which is available at www.roger.pl.

2.2.6 PSAM-1 power supply monitoring module

PRxx2 series controller can operate with single PSAM-1 module (address ID=4). The module can be optionally used with PS10, PS20 and PS15v24 power supply units from Roger or with any third party units. The PSAM-1 module can operate in standalone or network mode. In standalone mode, alarm signals are available at the module output lines. In network mode, digital communication between controller and PSAM-1 is performed by means of RACS CLK/DTA bus. In standalone mode, the module can operate with all PRxx1 and PRxx2 series controllers. In network mode it can operate only with PRxx2 series controllers. The PSAM-1 module can monitor and alarm following states:

- Low backup battery
- Backup battery failure

- No 230VAC voltage
- Actual voltage level at power supply unit output (in network mode only)

For more information on PSAM-1 module refer to its Installation Guide which is available at www.roger.pl.

2.2.7 HRT82FK function key panel

Prxx2 series controller can operate with single HRT82FK touch key panel (address ID=12). The panel is optional device offering additional four function keys. Each key can be assigned two functions which are activated by short and long pressing of the button. List of available functions is specified in table 9 (see 2.15 Function keys). LED indicators at the panel can also be assigned functions. In practical applications, indicator is assigned the function associated with the function of key in order to signal that the key was used and adequate function or state was activated. In order to use the panel it must be enabled and configured with PR Master software see - 3.17 HRT82FK tabs. Digital communication between controller and HRT82FK panel is performed by means of RACS CLK/DTA bus. For more information on HRT82FK panel refer to its Installation Guide which is available at www.roger.pl.

2.2.8 Wiegand/Magstripe interface readers

Some of PRxx2 series controllers can operate not only with PRT series readers but also with Wiegand and Magstripe third party readers (see table 1). Details on such connection are specified in Installation Guide of particular controller. The communication is performed by means of controller input lines (PR402DR) or by means of RACS CLK/DTA interface (PR402-BRD, PR602LCD-DT, PR602LCD).

In order to use Wiegand/Magstripe readers it is necessary to configure the controller by means of PR Master software i.e. select the controller in the main window of PR Master software in order to display controller properties and then in **Terminal ID0** tab and/or **Terminal ID1** tab (see 3.2 Terminal ID1 tab) select the adequate communication interface from the list allowing for:

- Electric standard,
- Transmitted data type,
- Data coding method.

The electric standard corresponds to electric characteristics of signal used in communication between controller and reader. Prxx2 series controllers use following electric standards:

- Wiegand,
- Magstripe (ABA Track II Emulation),
- RACS CLK/DTA (Roger).

Note: The negative power supply terminals of all devices connected to CLK/DTA line (incl. readers) should be connected together.

The PRxx2 series controllers are compatible with Wiegand formats varying from 26 up to 66 bytes with or without parity bytes. It is not necessary for the administrator to select number of bits as controllers recognize the reader bit stream length and adjust accordingly.

The data type parameter determines data transmitted by a reader i.e.:

- Card or PIN,
- Only Card,
- Only PIN,
- User ID.

In case of Card or PIN the controller attempts to recognize the source of the signal transmitted by the reader and interprets the data accordingly. In the remaining cases it is always interpreted according to particular controller settings (card, PIN, user ID).

The coding system setting determines digit/number coding. The following coding systems may be used:

- BIN, i.e. binary format,
- HEX, i.e. hexadecimal format,
- BCD, i.e. binary coded decimal format.

2.2.9 Biometric readers

All PRxx2 series controllers can operate with RFT1000 fingerprint reader. The communication between controller and RFT1000 is performed by means of RACS CLK/DTA or Wiegand interface while the communication between computer and RFT1000 is performed by means of Ethernet or RS485.

For more information on RFT1000 fingerprint reader with built-in Mifare reader refer to RFT1000 manuals which are available at www.roger.pl.

2.2.10 Long range proximity readers

Some of PRxx2 series controllers can operate with GP60 and GP90 long range proximity readers offered by Roger (see table 1). The communication of controller with these readers is performed by means of Magstripe interface (recommended) or Wiegand interface. The configuration of controller by means of PR Master software is necessary. The administrator must select the controller in the main window of PR Master software in order to display controller properties and then in **Terminal ID0** tab and/or **Terminal ID1** tab (see 3.2 Terminal ID1 tab) select the function **[31]: Magstripe reader, card only** or **[04]: Wiegand 26...66 bit reader, card only**. If two long range readers are connected to single controller then it might be necessary to use PR-GP interface device (Roger).

For more information on GP60 and GP90 long range proximity readers refer to their Installation Guides which are available at www.roger.pl.

2.3 Users

Access control users

Up to 4000 users can be stored in PRxx2 series controllers. Every user within the system can be identified according to its unique ID (ID=0000-3999) as well as assigned proximity card and/or PIN (3 to 6 digits). Upon entering PIN at the keypad of controller or PRT series reader operating with RACS CLK/DTA interface it is necessary to conclude the PIN with [#] key. In case of Wiegand/Magstripe different methods of PIN entering are accepted e.g. without [#] at the end or based on immediate transmission of every digit.

Users can be assigned to 4 classes: NORMAL, SWITCHER FULL, SWITCHER LIMITED and MASTER. Moreover, NORMAL users with ID above 1000 can be assigned the Local SWITCHER attribute and be able to arm/disarm particular controller (see 3.5 Arming tab). Each type of user features different rights in regard of programming and arming/disarming.

Name	ID range	Description
MASTER	000	Door opening and arming/disarming rights. MASTER user can be defined within Memory Reset procedure or by means of PR Master software. The MASTER user identifier (card or PIN) can be used for simple controller testing during installation i.e. relay output activation (which corresponds to door opening) and controller arming/disarming. In order to arm/disarm a controller it is necessary to use card or PIN twice. The MASTER user is by default assigned to No Group, thus he has access rights in the whole access control system regardless of any Schedule (unless it is limited by other special options).
SWITCHER Full	ID=001-049	Door opening and arming/disarming rights. In order to arm/disarm a controller it is necessary to use card or PIN twice.

SWITCHER Limited	ID=050-099	Only arming/disarming rights. In order to arm/disarm a controller it is necessary to use card or PIN once.
NORMAL	ID=100-999	Only door opening rights. The NORMAL users with ID above 1000 can be assigned Local SWITCHER attribute. In such case the user can arm/disarm particular controller. Contrary to Full and Limited SWITCHERS the Local SWITCHER attribute is assigned to particular user at particular controller. In order to arm/disarm a controller it is necessary to use card or PIN twice.

Access Groups

Access control users can be assigned to following groups: No Group, No Access Group or group defined by administrator of RACS 4. The first ones are default groups and the latter can be defined by means of the option **Groups** in the main window of PR Master software. The maximum number of user groups in PRxx2 controllers equals to 250. The access group membership determines user access rights within a given access control system. All users assigned to particular user group share the same access rights. It is possible and sometimes even required to specify group with single user. All users within specific Group have right to access particular Access Zones according to specified Schedule. 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.

Note: In the RACS 4 system particular user may belong only to single Access Group.

2.4 Identification Modes

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

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 specified individually 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 activated or switched by:

- Schedule – **Schedule** option in the main window of PR Master software and **Terminal ID0** tab and/or **Terminal ID1** tab (see 3.2 Terminal ID1 tab) within properties of particular controller
- Input line – see 2.13 Inputs
- Function key – see 2.15 Function keys
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands

2.5 Door Modes

Door Modes determine rules for locking/unlocking of access controlled doors. Following Door Modes are available in RACS 4 system:

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 activated or changed by:

- Schedule – **Schedule** option in the main window of PR Master software and **Access** tab (see 3.4 Access tab) within properties of particular controller
- Input line – see 2.13 Inputs
- Function key – see 2.15 Function keys
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands
- Remote command from PR Master software – options can be selected from the list by right clicking particular controller in the main window of PR Master software

2.6 Armed/Disarmed Modes

The concept of Armed/Disarmed Modes

PRxx2 controllers feature two arming modes: Armed and Disarmed. The current mode of controller is always displayed by means of bicolour  STATUS LED. The red colour refers to Armed Mode while the green colour refers to Disarmed Mode. Both modes are also displayed at PRT series reader, if it is connected to PRxx2 series controller.

Armed and Disarmed Modes can be switched by means of:

- User identifier i.e. proximity card or PIN, see 2.3 Users,
- Schedule - **Schedule** option in the main window of PR Master software and **Arming** tab (see 3.5 Arming tab) within properties of particular controller,
- Input line - see 2.13 Inputs,
- Function key - see 2.15 Function keys,
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands,
- Remotely from CPR network unit – Alarm Zones logic, see 2.12 Alarm Zones,
- Remote command from PR Master software - options can be selected from the list by right clicking particular controller in the main window of PR Master software.

All arming/disarming methods can be used concurrently i.e. all methods have the same level of priority. The only exception is the input line with the function **[03]: Arm/Disarm switch (momentary)**. When the input function is assigned to the controller then all other methods for arming/disarming are ignored by the controller.

The purpose of Armed/Disarmed Modes in RACS 4 system is to provide:

- additional level of access control,
- integration with intruder alarm systems.



The additional access control level can be achieved if the option **Access disabled when controller armed** (see 3.4 Access tab) is selected. When the option is inactive the user with adequate access rights can get access regardless of current Armed/Disarmed Mode. When the option is active then it is necessary to disarm the controller prior to use of authorized identifier (proximity card, PIN). Regardless of the option, if the controller is disarmed only user with adequate access right can get the access. By default the option is switched off.

Input and output lines of the controller are used in the integration of RACS 4 with intruder alarm system. Alarm Zones are also useful in such integration (see 2.12 Alarm Zones).

Manual arming/disarming by user

PRxx2 series controller can be armed/disarmed by means of identifier (proximity card, PIN) assigned to following user types: MASTER, SWITCHER Full, SWITCHER Limited and NORMAL with Local Switcher attribute (see 2.3 Users).

Arming/disarming procedure for SWITCHER Full, MASTER and NORMAL with Local SWITCHER attribute:

- Swipe the card and/or enter PIN (depending on current Identification Mode - see 2.4 Identification Modes),
- Wait till LED SYSTEM  blinks,
- When the LED SYSTEM  blinks use identifier once more (proximity card, PIN). In case of Card and PIN Identification Mode, in this step use only one identifier (proximity card or PIN).

In case of Switcher Limited user it is enough to use identifier (proximity card, PIN) once.

Arming/disarming by Schedule

The controller can change its Armed/Disarmed Mode according to Arming/Disarming Schedule (i.e. General Purpose Schedule defined by administrator). Arming/Disarming Schedule operates in such way that in time specified by From... parameter the controller switches to Disarmed Mode while in time specified by To... parameter it switches to Armed Mode. It is possible to delay scheduled arming (see 3.5 Arming tab). All schedules in RACS 4 system are defined by means of **Schedules** option in the main window of PR Master software.

Arming/disarming can be based on the Schedule assigned to particular Alarm Zone (affecting controllers assigned to that Alarm Zone) or on the Schedule assigned to particular controller. If the administrator selects Never schedule then the controller shall be armed after controller settings upload or reset. If the administrator selects Always schedule then the controller shall be disarmed after controller settings upload or reset. Both built-in schedules can be easily overridden by any method used for arming/disarming.

Note: The selection of schedule for arming/disarming does not mean that controller monitors and controls if it is actual Armed/Disarmed Mode conforms to the schedule. The schedule only specifies time when Armed/Disarmed Mode is automatically switched. If the administrator requires the controller to maintain Armed Mode (auto-arming) within specified time period then it is necessary to use following option: **Automatically restore Armed Mode after time** (see 3.5 Arming tab).

The moment of auto-arming can be delayed by means of following methods:

- Function key – see 2.15 Function keys,
- Input line – see 2.13 Inputs,
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands,
- When access is granted.

Delay for auto-arming can be defined by administrator in range of 5 to 99 minutes. It is also possible to specify warning before auto-arming in range of 1 to 99 minutes. The warning is an acoustic signal generated by controller/reader.

For more information on auto-arming and acoustic warning refer to description of PR Master options – see 3.5 Arming tab.

2.7 Access Rights

In order to define access rights in RACS 4 system it is necessary to specify who, where and when can be granted the access. It is recommended to use following procedure in order to define access rights in RACS 4 system:

- Specify Access Groups by means of **Access Groups** option in the main window of PR Master software,

- Add or import users and assign them to User Groups by means of **Users** option in the main window of PR Master software,
- Specify Access Zones by means of **Access Zones** option in the main window of PR Master software,
- In the properties of controllers assign Terminal ID0 or Terminal ID1 (readers) (see 3.2 Terminal ID1 tab) as entrance to previously specified Access Zone,
- Specify Schedules by means of **Schedules** options in the main window of PR Master software (see also 2.16 Schedules and Auxiliary Conditions),
- Select the option Access Groups in the main window of PR Master software, edit particular Group and assign Schedules to Access Zones in order to define access rights,
- Use **Access Map** option in the main window of PR Master software in order to verify previous settings,
- Optionally define additional access control mechanisms (e.g. Door Modes, input lines for exit buttons, APB zones, etc.)

The controller in RACS 4 system grants the access according to following procedure:


- User identification (proximity card, PIN),
- Determining to which User Group particular user belongs,
- Determining if particular User Group has access rights at particular controller/reader in particular moment,
- Verification of additional access control mechanisms (APB, Special options, Door Mode, etc.),
- Access granted or access denied decision,
- Door unlocking

Note: In RACS 4 system in order to define access rights it is necessary to specify who, where and when can be granted the access. User assigned to No Access Group cannot open any door while user assign to No Group can open all doors 24h/7d.

Controller denies access under the following circumstances:

- Unknown user,
- Incomplete identification e.g. correct PIN is entered but user is expected also to use proximity card when Card and Pin Identification Mode is selected for the reader.
- User is SWITCHER Limited type,
- User cannot enter particular Access Zone because of Schedule,
- Controller is armed and the option: **Access disabled when controller armed** is on
- Input line of the controller with the function **[11]: Access disabled** is activated.

Note: If user is unknown at the controller, long beep type acoustic signal is generated upon identification (proximity card, PIN). If the user is known but currently has no access rights then two long acoustic signals are generated.

Whenever controller grants the access, it activates LED OPEN . The LED remains lit as long as controller relay output connected to door lock is activated.

Door lock control

Following parameters related to door opening/closing can be configured by means of PR Master software (see 3.4 Access tab):

- **Door Unlock Time** (time of door strike release),
- **Door Unlock delay** (delay of door strike release),
- **Door Open Timeout** (when the time elapses and door is still opened, the DOOR AJAR alarm is raised – see 2.9 Door Alarms. It is necessary to install door contact and connect it to controller in order to use this option).

Optionally, the door can be controlled in latch mode i.e. door lock is released infinitely i.e. until the next access granting.

Typically, there are four methods for the door lock control:

- applying voltage for the lock (e.g. door strike),
- disconnecting voltage from lock (e.g. magnetic lock or fail-safe door strike),
- applying electric pulse (e.g. barrier, turnstile),
- triggering servomotor

The PRxx2 series controller can operate the lock by means of following functions which are usually assigned to controller relay outputs REL1 and/or REL2:

- **[97]:Door lock (term. ID0)**
- **[98]:Door lock (term. ID1)**
- **[99]:Door lock**

The controller activates output function **[99]** for access granting regardless of identification point (Terminal ID0 or Terminal ID1). Output function **[97]** is activated for access granting if the identification occurs at Terminal ID0 and output function **[98]** is activated for access granting if the identification occurs at Terminal ID1. In practice, output functions **[97]** and **[98]** can be used for turnstile control when it is required to determine direction of rotation. If access is granted then door is opened for the time specified by the parameter **Door Unlock Time** within PR Master software.

2.8 Facility Code

Facility Code (also called Site Code) is a part of the EM125kHz proximity card number which is located between 16th and 24th bits 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.

When Facility Code option is activated, then controller grants the access to all users with the same Facility Code. Due to this feature controller can be used to grant access to larger number of cardholders whose cards comply to a given Facility Code. Options related to Facility Code are available in controller properties which can be accessed in the main window of PR Master software (see 3.4 Access tab).

2.9 Door Alarms

Following Door Alarms are available in PRxx2 series controllers:

- PREALARM
- DOOR AJAR
- FORCED ENTRY

All mentioned above alarms can be raised at individual output lines **[28]: FORCED ENTRY**, **[29]: DOOR AJAR** and **[30]: PREALARM** or cumulatively in the output line with function **[256]: Door alarm**. If alarm is raised in **[256]** output then the type of alarm can be recognized based on electric signal modulation (see Table 5). If more than one alarm type is raised in **[256]** output, then controller signals alarm with highest priority. Door Alarm can also be signalled by means of internal buzzer. The logic is the same as for electric signal at controller output line.

Options related to Door Alarm are available in controller properties which can be accessed in the main window of PR Master software (see 3.6 Options tab).

Table 5. Door Alarms			
Alarm	Description	Priority	Signalling (modulation)
PREALARM	The alarm is raised in case of five consecutive attempts of identification at particular controller by unknown user within 5 minutes. The user, who is in the system but does not have access right at particular controller does not trigger PREALARM.	Low	Single pulse lasting 0,5 sec. repeated with 4 sec. period
DOOR AJAR	The alarm is raised if door is not closed after time specified by parameter Door Open Timeout (see 3.4 Access tab). It is necessary to install door contact and connect it controller in order to use that option.	Medium	Double pulses (each lasts 0,5 sec.) repeated with 4 sec. period
FORCED ENTRY	The alarm is raised if controller detects door opening when access is not granted. It is necessary to install door contact and connect it to controller in order to use this alarm. The alarm is also raised in case of PIN entry under duress (see 3.6 Options tab).	High	Single pulse lasting 2 sec. repeated with 4 sec. period

2.10 System Flags (Timers)

System 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 administrator defined purposes (AUX1, AUX2).

Initially, every flag is switched off. Flags can only be switched on upon certain system events/conditions. Flag returns to off state when preset time interval elapses (Timer) or when specific event occurs. 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. Flag state can be signalled at controller's output if certain function is assigned to the output.

For more information on Flags activation and deactivations refer to Table 6. Timer settings are available in controller properties which can be accessed in the main window of PR Master software (see 3.9 Timers tab).

Table 6. System Flags (Timers)		
Flag (timer) activation	Flag (timer) deactivation	Flag activation result
LIGHT flag		
- Input lines: [68]:Set LIGHT [70]:Toggle LIGHT - Function keys: [68]:Set Light [70]:Toggle LIGHT - Keypad Commands: [F21]:Set LIGHT [F23]:Toggle LIGTH	- Automatically when time specified for LIGHT flag elapses; - Output lines: [69]:Clear LIGTH [70]:Toggle LIGTH - Function keys: [69]:Clear LIGTH [70]:Toggle LIGTH - Keypad Commands: [F22]:Clear LIGTH [F23]:Toggle LIGTH	- Output line: [64]: LIGTH

TAMPER flag		
<p>- Input line: [08]:TAMPER</p>	<p>- Automatically when time specified for TAMPER flag elapsed</p> <p>- Controller disarming</p> <p>- Function key: [77]: Clear INTRUDER and TAMPER</p> <p>- Keypad command: [F31]: Clear INTRUDER and TAMPER</p>	<p>-Flag: INTRUDER</p> <p>- Output line: [65]: TAMPER [68]: INTRUDER</p> <p>- Alarm event: [540]: Tamper Alarm ON [052]: INTRUDER is on</p>
AUX1 flag		
<p>- Input lines: [71]:Set AUX1 [73]:Toggle AUX1</p> <p>- Function keys: [71]:Set AUX1 [73]:Toggle AUX1</p> <p>- Keypad Commands: [F24]:Set AUX1 [F26]:Toggle AUX1</p>	<p>- Automatically when time specified for AUX1 flag elapsed</p> <p>- Input lines: [72]:Clear AUX1 [73]:Toggle AUX1</p> <p>- Function keys: [72]:Clear AUX1 [73]:Toggle AUX1</p> <p>- Keypad Commands: [F25]:Clear AUX1 [F26]:Toggle AUX1</p>	<p>- Output line [66]: AUX1</p>
AUX2 flag		
<p>- Input lines: [74]:Set AUX2 [76]:Toggle AUX2</p> <p>- Function keys: [74]:Set AUX2 [76]:Toggle AUX2</p> <p>- Keypad Commands: [F27]:Set AUX2 [F29]:Toggle AUX2</p>	<p>- Automatically when time specified for AUX2 flag elapsed</p> <p>- Input lines: [75]:Clear AUX2 [76]:Toggle AUX2</p> <p>- Function keys: [75]:Clear AUX2 [76]:Toggle AUX2</p> <p>- Keypad Commands: [F28]:Clear AUX2 [F29]:Toggle AUX2</p>	<p>- Output line [67]: AUX2</p>
INTRUDER flag		
<p>- Input line: [09]:INTRUDER</p> <p>- Function key: [09]:INTRUDER</p>	<p>- Automatically when time specified for INTRUDER flag elapsed</p> <p>- Controller disarming</p> <p>- Function key:</p>	<p>- Output line: [68]: INTRUDER</p> <p>- Alarm event: [052]: INTRUDER is on</p>

- Keypad command: [F30]: INTRUDER	[77]: Clear INTRUDER and TAMPER	
FORCED ENTRY flag		
- Input line [01]: Door contact when controller does not grant access - user entered PIN which, differs by +/-1 in the last digit from correct PIN (see 3.6 Options tab)	- Automatically when time specified for FORCED ENTRY flag elapsed - Use of authorized identifier (proximity card and/or PIN) - Controller arming/disarming	- Output lines: [28]: FORCED ENTRY [256]: Door Alarm - Alarm event: [005]: FORCED ENTRY or [017]: PIN code under duress
PREALARM flag		
- 5 consecutive attempts of identification (proximity card and/or PIN) at particular controller by unknown user	- Automatically when time specified for PREALARM flag elapsed - Use of authorized identifier (proximity card and/or PIN) - Controller arming/ disarming	- Output lines: [29]: PREALARM [256]: Door Alarm - Alarm event: [003]: PREALARM
DOOR AJAR flag		
- Input line: [01]: Door contact when time specified by Door Open Timeout elapsed and the input is still active i.e. door is opened	- Automatically when following input line becomes deactivated: [01]: Door contact - Automatically when time specified FOR DOOR ajar flag elapses - Use of authorized identifier (proximity card and/or PIN) - Controller arming/ disarming Note: The input line [01]: Door contact has the highest priority. DOOR AJAR flag is on as long as this input is active (i.e. door is opened). Once the input line becomes deactivated, the flag is off regardless of its Timer.	- Output lines: [30]: DOOR AJAR [256]: Door Alarm - Alarm event: [004]: DOOR AJAR

Note: Output line **[256]: Door Alarm** can be blocked by other options in PR Master software (see 3.6 Options tab).

2.11 Anti-passback

By activating the APB option the system requires user to identify successively at APB zone entrance and exit (i.e. the sequence of entry-exit...entry-exit must be maintained). PRxx2 controllers monitor the latest identifications of users and store them in APB Register. APB rules can apply either to a

single door or a larger zone called the Anti-passback Zone. APB Zones are defined independently of other zones in RACS 4 (Access Zones, Alarm Zones). In regard of area covered by APB, it can be divided into:

- Local APB
- Global APB

Local APB is defined for a single controller (single door) and both readers corresponding to the entrance and exit of APB zone must be connected to that single controller. By default Terminal ID0 is entry reader while Terminal ID1 is exit reader, but this arrangement can be easily changed by system administrator (see 3.2 Terminal ID1 tab).

Global APB refers to access control area called APB Zone with multiple doors. One APB Zone may incorporate readers connected to various controllers within single network (subsystem). In Global APB, users willing to exit particular APB zone must enter it first. Global APB may be used in systems including at least 2 controllers and a CPR network controller.

In regard of RACS 4 system reaction for violation of APB rules, following types of APB are available:

- Hard APB,
- Soft APB.

In case of Soft APB every violation of APB rules results in the recording of event **[509]: APB Violation** in event log and the controller can grant the access. In case of Hard APB every violation also results in event **[509]: APB Violation** recorded in event log but the controller does not grant access and generates two long acoustic pulses.

RACS 4 also enables configuration of True APB i.e. APB with door contact. Normally, if user is granted access to APB zone then APB Register is updated accordingly but the controller does not monitor if particular user actually enters/leaves the zone. In case of True APB the APB Register is updated when access is granted and controller receives signal from door contact that the door is opened. If only access is granted then APB Register is not updated. True APB requires connection of door contact to controller input line with function **[01]: Door contact**.

Options related to APB are available in controller properties which can be accessed in the main window of PR Master software (see 3.8 APB tab).

Note: After reset of APB Register every user of RACS 4 system can identify at any reader (entry or exit reader) and then follow APB rules i.e. identify interchangeably at entrance and exit.

APB Zones

An APB Zone is an independent area of access control system with multiple doors (controllers). APB Zone incorporates a list of entry and exit readers. The PRxx2 series controller is capable of monitoring single door with read in/out control. Therefore, it needs to be located at a border between two APB Zones. Then one of the readers connected to the controller monitors entry to APB zone while the other monitors exit from that zone (which by the way is the entry to another APB zone). It is forbidden to control entrance to APB zone by means of two readers connected to the same controller.

Note: The PRxx2 series controller located at the APB Zone border is not required to have two connected readers. APB zone entrance and exit can be controlled by two access controllers, each with single reader.

In every RACS 4 system there is built-in, predefined APB Zone called Public zone. Public zone is an area surrounding access control system. For example, if access control system is installed inside the building then user leaving that building enters Public zone and consequently user entering the building exits Public zone.

In RACS 4 systems, single APB zone can incorporate controllers only from single network (subsystem). Controllers from different subsystem cannot be part of single APB Zone.

In case of APB zone it is possible to configure internal door by assigning particular controller (and at the same time its terminals) to particular APB Zone in **APB** tab (see 3.8 APB tab). User can be granted access at such door only if he already is inside the APB Zone i.e. he entered the Zone by one of its entry points/terminals. In practical applications controller responsible for internal door does not have to be located inside room or area controlled by APB. Thus, internal door mechanism can also be used to control user routes in the building.

APB Register

The APB Register is stored in access controller memory and it includes information on users latest entries or exits to/from APB Zone.

As a result of APB Register reset, any user can identify at any reader (entry or exit reader) but then he must follow APB rules and identify successively at entry/exit readers belonging to APB Zone.

The reset of APB Register occurs automatically after connection of power supply to the controller and it can also be done by means of:

- Input line – see 2.13 Inputs,
- Function key - see 2.15 Function keys,
- Remote command from PR Master software – the command **Reset APB Register on controller** can be used by right clicking particular controller in the main window of PR Master software,
- Remote command from PR Master software – the command Reset Global APB Register can be used by right clicking particular Network (subsystem) in the main window of PR Master software,
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands,
- Schedule – **Schedule** option in the main window of PR Master software and **APB** tab (see 3.8 APB tab) within properties of particular controller.

Hierarchy of APB Zones

APB Zone Hierarchy reflects zonal relationships between various APB zones within single access network (subsystem). If the hierarchy is activated then users are allowed to move only from one adjacent APB Zone to another adjacent APB Zone. Zones are adjacent when there is controller on the border of these zones and one of controller's readers enables access to one of the zones while the other reader enables access to the other adjacent zone. The APB Hierarchy can be switched on/off in the window opened by means of **APB Zones** option in the main window of PR Master software.

Procedure for configuration of Local APB

1. In properties of particular controller (PR Master software) open **APB** tab and select the option **Enable Anti-passback**.
2. If necessary, following additional options and settings can be configured in **APB** tab: True APB, Hard/Soft APB Schedule, APB Reset Schedule and max number of users. In case of schedules, both Always/Never schedules and administrator defined schedules (by means of **Schedules** option in the main window of PR Master software) can be applied.
3. In properties of particular controller, open **Terminal ID1** tab and in **Entry/Exit (Local APB)** field select one of the options: **Entrance to the room/area** or **Exit from the room/area**, thus making particular reader the entry or exit terminal.
4. Update the configuration of controller by means of PR Master software.
5. APB Register can be cleared by right clicking particular controller in the main window of PR Master software and selecting of the option **Reset APB Register on controller** from the list. APB Register can be reviewed by means of the option **Read APB Register on controller** from the same list.

Procedure for configuration of Global APB

1. Specify names of APB Zones by means of **APB Zones** option in the main window of PR Master software and if necessary select **Enable APB Hierarchy** option and optionally specify maximum numbers of users in particular zone.
2. In properties of particular controller open **APB** tab and then select the option **Enable Anti-passback**.

3. If necessary, following additional options and settings can be configured in **APB** tab: True APB, Hard/Soft APB Schedule and APB Reset Schedule. In case of schedules, both Always/Never schedules and administrator defined schedules (by means of **Schedules** option in the main window of PR Master software) can be applied.
4. In properties of particular controller open **Terminal ID1** tab and in the field **APB Zone (Global APB)** select one of the available APB Zones from the list. Terminal ID1 will be the entrance to that APB Zone. Open **Terminal ID0** tab and similarly select one of available APB Zones from the list. Terminal ID0 will be the entrance to that APB Zone. You can always use default APB Zone i.e. Public Zone in your configuration. As a result, assigned readers shall be listed in the window opened by means of **APB Zone** option in the main window of PR Master software.
5. Repeat the actions mentioned in point 4 for the remaining controllers of Global APB within single network (subsystem) and then configure remaining APB Zones, if applicable.
6. Verify the settings in the window opened by means of **APB Zones** option in the main window of PR Master software.
7. Update the configuration of controllers and CPR by means of PR Master software.
8. APB Register can be cleared by right clicking particular controller in the main window of PR Master software and selecting the option **Reset APB Register on controller** from the list. APB Register can be reviewed by means of the option **Read Global APB Register** from the same list. Clearing and reading can also be performed globally by right clicking Network (subsystem) in the main window of PR Master software and selecting adequate options from the list.

2.12 Alarm Zones

Alarm Zones are used in the integration of RACS 4 with intruder alarm systems. The Alarm Zone is a group of controllers intended to arm/disarm concurrently. If any controller of particular Alarm Zone arms/disarms (it is not relevant what method for arming/disarming is applied) then the remaining controllers follow. Alarm Zones feature requires installation of CPR network unit which monitors all access controllers within Alarm Zones and switches their Arm/Disarm Modes accordingly.

Note: Alarm Zones do not block other methods of controller arming/disarming.

Note: The maximal number of Alarm Zones in RACS 4 system equals to 32.

If the controller Armed/Disarmed Mode is managed by means of its input line with the function **[03]: Arm/Disarm switch (momentary)**, then the mode cannot be switched by any other method. If the controller with **[03]** input is assigned to Alarm Zone then its Armed/Disarmed Mode still depends only on the **[03]** input and not the status of Alarm Zone.

Hierarchy of Alarm Zones

In RACS 4, the administrator can configure multiple Alarm Zones and they can operate independently or they can be arranged in hierarchy order. In case of independent Alarm Zones they do not affect each other while hierarchic Alarm Zones can operate in master/slave relationship according to following rules:

- Arming the superordinate zone makes all subordinate zones armed
- Disarming the superordinate zone does not affect subordinate zones
- Arming the subordinate zone does not affect the superordinate zone
- Disarming the subordinate zone does not affect the superordinate zone

Alarm Zone hierarchy in RACS 4 system is arranged in tree structure which reflects relationship and dependencies among them. In figure 8, there is shown example of Alarm Zone hierarchy.

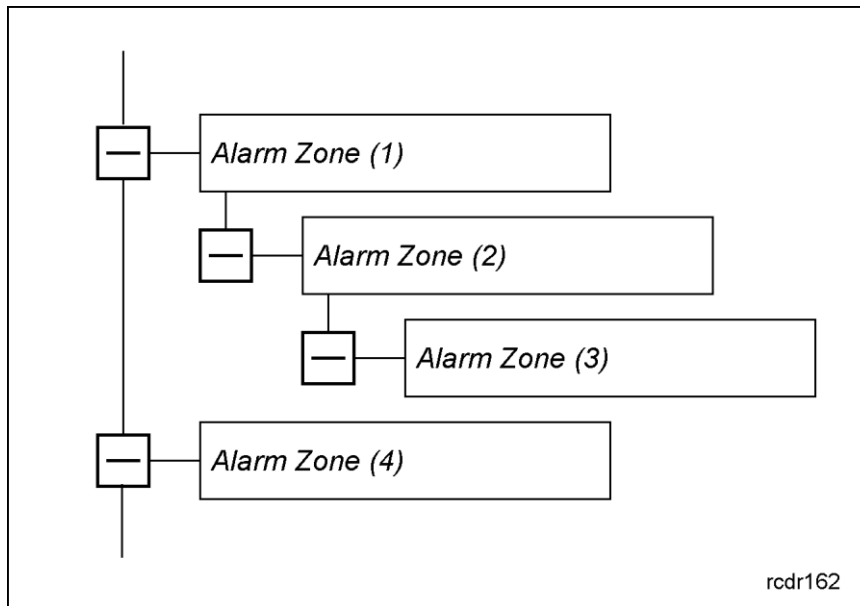


Fig. 8 Hierarchy of Alarm Zones

Based on example shown in fig. 8, following dependencies can be specified: Alarm Zone (4) is independent of other zones; Alarm Zone (2) is dependent on Alarm Zone (1) while Alarm Zone (3) is dependent on Alarm Zone (2); Arming of Alarm Zone 1 results in arming of Alarm Zones (2) and (3) while arming of Alarm Zone (2) results in arming of Alarm Zone (3); Disarming of Alarm Zone (1) does not affect subordinate zones i.e. Alarm Zones (2) and (3).

Procedure for configuration of Alarm Zones

1. Specify names of Alarm Zones by means of the option **Alarm Zones** in the main window of PR Master software, selecting network (subsystem), Schedule and optionally hierarchy of Alarm Zones. Selection of predefined Schedule i.e. Always or Never Schedule actually results in cancelling of automatic arming/disarming of Alarm Zones and determines only default Arm/Disarm Mode of controllers. Administrator defined Schedules can be specified by means of **Schedules** option in the main window of PR Master software.
2. In properties of particular controller open **Arming** tab and then select the option **Enable Arm/Disarm Schedule**.
3. Within the same tab, additional parameters related to arming/disarming can be defined. These parameters generally enable delay of auto-arming and configuration of acoustic warnings (see 3.5 Arming tab).
4. The area of Alarm Zone is defined by assignment of controllers and not their readers (Terminals ID0, ID1). The assignment is done by enabling Arm/Disarm Schedule (see point 3 above).
5. Verify the settings in the window opened by means of **Alarm Zones** option in the main window of PR Master software.
6. Update the configuration of controllers and CPR by means of PR Master software.

For more information on auto-arming and acoustic warnings refer to description of PR Master options – see 3.5 Arming tab.

2.13 Inputs

The number of controller programmable inputs depends on its type – see table 1. Optional XM-2 expander can be connected to PRxx2 series controller in order to increase the number of available inputs by two. In case of PRxx2 series controllers, input lines can be configured in regard of their function, Schedule, Auxiliary Condition, NC/NO triggering and T&A Mode by means of PR Master software within properties of particular controller (see 3.11 Input IN1...IN8 tabs). For NO line (normally open), the triggering is done by closing the circuit while in case of NC line (normally close), the triggering is done by opening the circuit (voltage disconnection).

Additionally all input functions can be divided into ON/OFF monitored and ON monitored. In case of ON/OFF monitored input functions, RACS 4 systems detects the moment of input activation and deactivation. In case of ON monitored input functions, RACS 4 system detects only their activation, thus it is not relevant how long the input is activated and when it is deactivated as only the activation triggers certain actions within the system. For example **[01]: Door contact** function is ON/OFF monitored type and the controller reacts to its activation and deactivation while the function **[02]: Exit button** is ON monitored one and the controller reacts only to its activation.

Table 7 Input functions			
No.	Function	Type	Description
[00]	None	-	Input line is not used.
[01]	Door contact	ON/OFF monitored	The input is dedicated to connection of door detector. Input activation is interpreted by the controller as door opening while input deactivation is interpreted as door closing.
[02]	Exit button	ON monitored	The input is dedicated to connection of exit button or other contact used for door opening. When the input is activated the controller grants access for specified time and door can be opened.
[03]	Arm/Disarm switch (momentary)	ON/OFF monitored	The input is dedicated to control Arm/Disarm Mode of the controller. As long as the input is activated the controller is in Armed Mode. As long as the input is deactivated the controller is in Disarmed Mode. Note: Only single input line of controller can be configured with that function and it has the highest priority among all arming/disarming methods.
[05]	AC lost	ON/OFF monitored	The input is used for 230VAC power supply monitoring. When the input is not activated then it signifies adequate 230VAC power supply to the unit which supplies the controller with 12VDC. When the input is activated then it signifies 230VAC power shortage to the unit which supplies the controller with 12VDC. The input with function [05] can be used for connection to PSAM-1 output or connection to the output of third party power supply unit if it provides 230VAC monitoring. Note: Regardless of the input with function [05] , PR402 controllers can monitor their 18VAC power supply.

[06]	Low battery	ON/OFF monitored	<p>The input is used for monitoring of backup battery connected to power supply unit. When the input is not activated then it signifies adequate operation of backup battery connected to power supply unit with 12VDC output. When the input is activated then backup battery requires charging or replacement. The input with function [06] can be used for connection to PSAM-1 output or connection to output of third party power supply unit if it provides monitoring of its backup battery.</p> <p>Note: Regardless of input with function [06], PR402 controllers can monitor backup battery if it is connected to controller terminals.</p>
[07]	Door bell	ON/OFF monitored	<p>When the input is activated then acoustic signal is generated by controller's internal buzzer and the output with function [15]:Door bell is activated. Both, acoustic signal and output are activated for 4 sec.</p>
[08]	TAMPER	ON monitored	<p>The activation of [08] input is interpreted as tamper alarm and results in activation of TAMPER and INTRUDER flags. Tamper contact is installed inside PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302 controllers and it is connected to separate wires/terminals which can be connected to input with function [08] or any other external devices (e.g. alarm siren).</p>
[09]	INTRUDER	ON monitored	<p>The activation of [09] input is interpreted as activation of connected alarm detector and results in activation of INTRUDER flag.</p>
[11]	Access disabled	ON/OFF monitored	<p>As long as the input is activated, the controller denies access.</p>
[13]	Arming disabled	ON/OFF monitored	<p>As long as the input is activated, the controller cannot be armed with proximity card, PIN, input or function key. Scheduled arming is delayed (see 3.5 Arming tab).</p>
[14]	Door unlock (momentary)	ON/OFF monitored	<p>As long as the input is activated, the controller enables the access at particular door for everyone (as in Unlocked Door Mode).</p>

[44]	Switch temporary access on terminal ID1 on	ON monitored	The assignment of [44] function to any input results in replacement of event related to access granting i.e. instead of typical [001]: Access granted , the event [547]: Access granted-special mode is generated when access is granted by the controller. The event [547] is ignored within Attendance report in PR Master software. When the input with function [44] is activated then Terminal ID1 is emulated for 8 seconds or till the identification of user by means of proximity card and/or PIN. Within this time, standard event [001]:Access granted is generated when access is granted by the controller. Note: The function [44] is not available for PR402 and PR102 controllers.
[45]	Switch temporary terminal ID1 to emulate terminal ID0	ON monitored	When the input is activated, the controller with built-in reader (Terminal ID1) switches to emulation of Terminal ID0. Each Terminal can be configured differently. The emulation lasts 8 seconds or till the identification of user by means of proximity card and/or PIN. The event related to access granting is [001]: Access granted . Note: The function [45] is not available for PR402 and PR102 controllers.
[46]	Random check confirm	ON monitored	When the input is activated, then user inspection is confirmed, controller is unblocked and the next user can identify at the reader by means of proximity card and/or PIN. The input is used only with the option: Random check requires confirmation (see 3.7 Advanced tab).
[47]	Entry button	ON monitored	The input is dedicated to connection of entry button or other contact used for door opening. When the input is activated, the controller grants access for specified time and door can be opened. Function [47] operates similarly as function [02] .
[48]	Keypad selected T&A Mode	ON monitored	The input is used in connection with Time& Attendance (RCP Master software).
[49]	Keypad selected T&A Mode (temporary)	ON monitored	The input is used in connection with Time& Attendance (RCP Master software).
[50]	Next T&A Mode	ON monitored	The input is used in connection with Time& Attendance (RCP Master software). Function [50] is available only in PR602LCD-DT and PR602LCD controllers.
[51]	Next T&A Mode (temporary)	ON monitored	The input is used in connection with Time& Attendance (RCP Master software). Function [50] is available only in PR602LCD-DT and PR602LCD controllers.
[56]	Predefined T&A Mode	ON monitored	The input is used in connection with Time& Attendance (RCP Master software).

[57]	Predefined T&A Mode (temporary)	ON monitored	The input is used in connection with Time& Attendance applications (RCP Master software).
[58]	Postponed auto-arming delay ON	ON monitored	When the input is activated then auto-arming is delayed by the time specified with Programmed auto-arming delay option (see 3.5 Arming tab).
[59]	Postponed auto-arming delay OFF	ON monitored	When the input is activated then auto-arming delay resulting from the option Programmed auto-arming delay is cancelled and the controller attempts to arm instantly if required by Arming/Disarming Schedule (see 3.5 Arming tab).
[60]	APB Register reset	ON monitored	When the input is activated then APB Register is reset (cleared) and any user can identify by means of proximity card and/or PIN at any terminal (reader) but in the next steps Anti-pass back rules must be followed.
[61]	Arm/Disarm switch (toggle)	ON monitored	The input is used to toggle between Armed and Disarmed Modes.
[62]	XM-8 outputs OFF	ON monitored	When the input is activated then all relay outputs of XM-8 expanders connected to the controller are switched off.
[63]	XM-8 outputs ON	ON monitored	When the input is activated then all relay outputs of XM-8 expanders connected to the controller are switched on.
[64]	Normal Door Mode	ON monitored	When the input is activated then Normal Door Mode is selected for the controller.
[65]	Unlocked Door Mode	ON monitored	When the input is activated then Unlocked Door Mode is selected for the controller.
[66]	Cond. Unlocked Door Mode	ON monitored	When the input is activated then Conditionally Unlocked Door Mode is selected for the controller.
[67]	Locked Door Mode	ON monitored	When the input is activated then Locked Door Mode is selected for the controller.
[68]	Set LIGHT	ON monitored	When the input is activated then LIGHT Flag (Timer) is on.
[69]	Clear LIGHT	ON monitored	When the input is activated then LIGHT Flag (Timer) is off.
[70]	Toggle LIGHT	ON monitored	When the input is activated then LIGHT Flag (Timer) is switched on/off.
[71]	Set AUX1	ON monitored	When the input is activated then AUX1 Flag (Timer) is on.
[72]	Clear AUX1	ON monitored	When the input is activated then AUX1 Flag (Timer) is off.
[73]	Toggle AUX1	ON monitored	When the input is activated then AUX1 Flag (Timer) is switched on/off.
[74]	Set AUX2	ON monitored	When the input is activated then AUX2 Flag (Timer) is on.

[75]	Clear AUX2	ON monitored	When the input is activated then AUX2 Flag (Timer) is off.
[76]	Toggle AUX2	ON monitored	When the input is activated then AUX2 Flag (Timer) is switched on/off.
[78]	Disarmed Mode	ON monitored	When the input is activated then the controller is switched to Disarmed Mode.
[79]	Armed Mode	ON monitored	When the input is activated then the controller is switched to Armed Mode.
[84]	Card or PIN Mode on term. ID0	ON monitored	When the input is activated then Identification Mode of Terminal ID0 (reader) is switched to Card or PIN.
[85]	Card Only Mode on term. ID0	ON monitored	When the input is activated then Identification Mode of Terminal ID0 (reader) is switched to Card Only.
[86]	PIN Only Mode on term. ID0	ON monitored	When the input is activated then Identification Mode of Terminal ID0 (reader) is switched to PIN Only.
[87]	Card and PIN Mode on term. ID0	ON monitored	When the input is activated then Identification Mode of Terminal ID0 (reader) is switched to Card and PIN.
[88]	Card or PIN Mode on term. ID1	ON monitored	When the input is activated then Identification Mode of Terminal ID1 (reader) is switched to Card or PIN.
[89]	Card Only Mode on term. ID1	ON monitored	When the input is activated then Identification Mode of Terminal ID1 (reader) is switched to Card Only.
[90]	PIN Only Mode on term. ID1	ON monitored	When the input is activated then Identification Mode of Terminal ID1 (reader) is switched to PIN Only.
[91]	Card and PIN Mode on term. ID1	ON monitored	When the input is activated then Identification Mode of Terminal ID1 (reader) is switched to Card and PIN.

Note: Following input functions can be assigned to only single physical input line of the controller: **[01]:Door contact, [03]:Arm/Disarm switch (momentary), [05]:AC lost and [06]:Low battery.**

2.14 Outputs

The number of programmable outputs (relay and transistor type) in the controller depends on its type – see table 1. Optional XM-2 expander can be connected to PRxx2 series controller in order to increase the number of relay outputs by two. In case of PRxx2 series controllers, output lines can be configured in regard of their function, Schedule and Auxiliary Condition by means of PR Master software within properties of particular controller (see 3.12 Output IO1...IO2 tabs and 3.13 Output REL1...REL2 tabs). Relay outputs REL1 and REL2 provide isolated NO, NC and COM terminals (under normal operating conditions NO-COM connectors are open, whereas NC-COM connectors are close). Every transistor output is capable of operating with current up to 1 A (and 15VDC). Transistor outputs are equipped with internal fuses for switching off outputs automatically once a maximum current level is exceeded.

Default function for REL1 relay output is **[99]: Door lock** and it is used for door lock control.

Table 8. Output functions		
No.	Function	Description
[00]	Disarmed Mode	As long as the controller is disarmed then the output is activated and as long as the controller is armed then the output is deactivated. Functions [00] and [35] operate in the opposite way.
[08]	PC command	The output with function [08] can be activated by means of command from PR Master software. In order to activate output [08] , right click particular controller in the main window of PR Master software and select the option Set/clear controller output or select the option Controller output control in the Command menu of Online Monitoring in PR Master software. Both functions [08] and [13] can only be assigned to transistor outputs i.e. IO1 or IO2.
[09]	Access granted	The output is activated when access is granted by means of proximity card and/or PIN for the time specified with parameter Door Unlock Time in the properties of the controller (PR Master software).
[10]	Door status	As long as the door is opened the output [10] is activated. In fact the output represents the signal from controller's input with the function [01]: Door contact .
[11]	Access denied	The output is activated for 2 sec. when controller denies the access.
[12]	Schedule	The output is activated in time periods specified by assigned Schedule, according to From... and To... parameters. The Schedule can be defined by means of the option Schedules in the main window of PR Master software.
[13]	Schedule or PC command	The output operates in the same way as output with function [12] . Additionally, output with the function [13] can be operated by means of commands from PR Master software in the same way as output with the function [08] . Both functions [08] and [13] can only be assigned to transistor outputs i.e. IO1 or IO2.
[14]	User logged on term. ID0	The output is activated upon user identification at Terminal ID0 and remains activated till user identification at Terminal ID1. The function can be used to control turnstile rotation or in case of read in/out controlled door, the output can be used for reporting entry/exit.
[15]	Door bell	The output is activated for 5 sec. when input with the function [07] or function key with the function [255] is activated.
[16]	Room occupied	The output is activated when the first user enters particular room (APB Zone) and remains activated until all users leave the room. The number of users inside the room is calculated based on data stored in APB Register.

[17]	Limit of users reached	The output is activated when the number of users in particular room (APB Zone) reaches the limit. The output is deactivated when the number of users in the room is lower than the limit.
[18]	Normal Door Mode	The output is activated as long as Door Mode of the controller is Normal.
[19]	Unlocked Door Mode	The output is activated as long as Door Mode of the controller is Unlocked.
[20]	Cond. Unlocked Door Mode	The output is activated as long as Door Mode of the controller is Cond. Unlocked.
[21]	Locked Door Mode	The output is activated as long as Door Mode of the controller is Locked.
[22]	Postponed auto-arming delay in progress	The output is activated when auto-arming of the controller is delayed i.e. the output is activated for the time specified by following parameters: Default auto-arming delay and Programmed auto-arming delay (see 3.5 Arming tab) and remains activated till controller arming.
[23]	External buzzer	The output is used for connection of external loudspeaker which can be operated and controlled in the same way as controller/reader internal buzzer.
[24]	Terminal restart	The output is activated for 2 sec. when the controller detects communication failure with any of its external readers. The output line can be used to restart the reader in case of communication failure. Note: The controller can supervise the communication only with terminals operating in RACS CLK/DTA mode (Wiegand and Magstripe readers are excluded).
[25]	Pulse upon disarming	The output is activated for 2 sec. when the controller switches to Disarmed Mode.
[26]	Pulse upon arming	The output is activated for 2 sec. when the controller switches to Armed Mode.
[27]	Request to arm	In general perspective, output with the function [27] operates in the same way as output with the function [0]: Disarmed Mode i.e. as long as the controller is armed then the output [27] is deactivated and as long as the controller is disarmed then the output [27] is activated, but output [27] is also activated in case of unsuccessful arming. For example, if the controller is disarmed and the input with function [13]: Arming disabled is activated then arming attempt shall be unsuccessful but the output with function [27] shall be deactivated despite the fact, that the controller shall still be disarmed.
[28]	FORCED ENTRY	The output represents the state of FORCED ENTRY Flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[29]	PREALARM	The output represents the state of PREALARM Flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.

[30]	DOOR AJAR	The output represents the state of DOOR AJAR Flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[31]	Door chime	The output is activated for 2 sec. when the controller detects door opening. In order to use this output it is necessary to connect door contact to controller input with the function [01]: Door contact . Access granting itself does not activate the output [31] .
[32]	APB violation	The output is activated for 2 sec. when APB rules are violated. The output [32] is not used for signalling that maximal number of users in the room (APB Zone) is exceeded. In such case use the function [17] instead.
[33]	Incoming auto-arming in progress (steady)	The output represents the acoustic warning configured by means of the option Incoming auto-arming in progress signalling time (see 3.5 Arming tab). The output is deactivated when the time configured by the option elapses and the controller arms according to schedule.
[34]	Incoming auto-arming in progress (pulsed)	The output operates in the same way as output with the function [33] but it instead of constant signal, double pulse every 8 sec. is generated.
[35]	Armed Mode	As long as the controller is disarmed then the output is deactivated and as long as the controller is armed then the output is activated. Functions [00] and [35] operate in the opposite way.
[36]	Pulse upon access granting	The output is activated for 1 sec. when access is granted by the controller.
[37]	AC failure	The output is activated approx. 8 minutes after detection of 18VAC power supply failure and is deactivated approx. 40 seconds after detection of 18VAC power supply recovery.
[38]	Low battery	The output is activated approx. 9 minutes after detection of low battery level and is deactivated approx. 9 minutes after detection of adequate battery level.
[39]	Random check request	The output is activated for 2 sec. when particular user is selected by the controller for inspection. But if the option Random check requires confirmation is selected (see 3.7 Advanced tab) then the output [39] is activated until the inspection is confirmed by means of input with the function [46]: Random check confirm or by means of function key with the function [46]: Random check confirm .
[64]	LIGHT	The output represents the state of LIGHT flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[65]	TAMPER	The output represents the state of TAMPER flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[66]	AUX1	The output represents the state of AUX1 flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.

[67]	AUX2	The output represents the state of AUX2 flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[68]	INTRUDER	The output represents the state of INTRUDER flag. When the Flag is on then the output is activated, when the Flag is off then the output is deactivated.
[74]	Antenna switching on term. ID1 and ID0	The output enables alternate switching of antenna coils in controller and external reader. Connection of this output to the input of external reader improves card reading when both devices are installed too close on both sides of door. This output is available only for controllers with built-in reader i.e. PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302.
[84]	Card or PIN Mode on term. ID0	The output is activated as long as Identification Mode at Terminal ID0 (reader) is Card or PIN.
[85]	Card Only Mode on term. ID0	The output is activated as long as Identification Mode at Terminal ID0 (reader) is Card Only.
[86]	PIN Only Mode on term. ID0	The output is activated as long as Identification Mode at Terminal ID0 (reader) is PIN Only.
[87]	Card and PIN Mode on term. ID0	The output is activated as long as Identification Mode at Terminal ID0 (reader) is Card and PIN.
[88]	Card or PIN Mode on term. ID1	The output is activated as long as Identification Mode at Terminal ID1 (reader) is Card or PIN.
[89]	Card Only Mode on term. ID1	The output is activated as long as Identification Mode at Terminal ID1 (reader) is Card Only.
[90]	PIN Only Mode on term. ID1	The output is activated as long as Identification Mode at Terminal ID1 (reader) is PIN Only.
[91]	Card and PIN Mode on term. ID1	The output is activated as long as Identification Mode at Terminal ID1 (reader) is Card and PIN.
[92]	Temporary T&A Mode on	The output is activated for 8 sec. when input or function key with temporary T&A Mode function i.e. [49], [51] or [57] is used. The function [92] can be used for blocking the access for user who did not select any T&A Mode. In such case the output with function [92] should be connected to the input of the same controller with the function [11] and the input should be configured as NC type.
[93]	DOOR AJAR prealert	The output is activated when half of the time required to activate DOOR AJAR Flag elapses i.e. half of time specified by Door Open Timeout parameter. The output becomes deactivated when door is closed or DOOR AJAR flag time elapses. After connection of acoustic device the output with function [93] can be used to warn users about incoming DOOR AJAR alarm.
[97]	Door lock (term. ID0)	The output is activated for the time specified by the parameter Door Unlock Time (see 3.4 Access tab), when the access is granted for user identified at Terminal ID0. The output can be used with turnstiles.

[98]	Door lock (term. ID1)	The output is activated for the time specified by the parameter Door Unlock Time (see 3.4 Access tab), when the access is granted for user identified at Terminal ID1. The output can be used with turnstiles.
[99]	Door lock	The output is activated for the time specified by the parameter Door Unlock Time (see 3.4 Access tab), regardless of terminal, where user identification occurred. The function [99] is default setting of REL1 relay output of the controller and is used for door lock control.
[256]	Door alarm	The output represents Door Alarm (see 2.9 Door Alarm) Note: The function [256] is combined one and it consists of following alarms: DOOR AJAR, PREALARM and FORCED ENTRY. Each of mentioned alarm is signalled by means of different modulation (pulses). If more than one alarm occurs then the one with the highest priority is represented at the output [256] .

2.15 Function keys

The administrator can configure up to four function keys for controller. In case of PRxx2 series controllers, function keys (similarly to input lines) can be configured in regard of their function, Schedule, Auxiliary Condition and T&A Mode by means of PR Master software within properties of particular controller (see 3.16 F1...F4 keys tabs). PR Master software enables the configuration of all four function keys for both Terminal ID0 and Terminal ID1 regardless if these function keys are actually available at controller/reader keypad. Function keys of PRT series readers can be used only if these readers are configured to RACS CLK/DTA mode. In case of Wiegand or Magstripe communication, function keys cannot be used. In general perspective, function key operates in the same way as button connected to controller's input line.

No.	Function	Description
[00]	No function	Function key is not used, no function is assigned.
[02]	Release door	The key enables door opening as in case of standard access granting.
[04]	Key pressed (event only)	Each use of the key with function [04] is registered in event history, and there no other actions/reactions in the system.
[09]	INTRUDER	The key with function [09] works in the same way as input line with function [09] and it activates INTRUDER flag (timer).
[44]	Switch temporary access on terminal ID1 on	The assignment of [44] function to any function key results in replacement of event related to access granting i.e. instead of typical event [001]: Access granted , the event [547]: Access granted-special mode is generated when access is granted by the controller. The event [547] is ignored within Attendance report in PR Master software. When the key with function [44] is pressed then Terminal ID1 is emulated for 8 seconds or till the identification of user by means of proximity card and/or PIN. Within this time, standard event [001]:Access granted is generated when access is granted by the controller. Note: The function [44] is not available for PR402 and PR102 controllers.

[45]	Switch temporary terminal ID1 to emulate terminal ID0	When the key is pressed, the controller with built-in reader (Terminal ID1) switches to emulation of Terminal ID0. Each Terminal can be configured differently. The emulation lasts 8 seconds or till the identification of user by means of proximity card and/or PIN. The event related to access granting is [001]: Access granted . Note: The function [45] is not available for PR402 and PR102 controllers.
[46]	Random check confirm	When the key is pressed, then user inspection is confirmed, controller is unblocked and the next user can identify at the reader by means of proximity card and/or PIN. The input is used only with the option: Random check requires confirmation (see 3.7 Advanced tab).
[48]	Keypad selected T&A Mode	The key is used in connection with Time&Attendance (RCP Master software).
[49]	Keypad selected T&A Mode (temporary)	The key is used in connection with Time&Attendance (RCP Master software).
[50]	Next T&A Mode	The key is used in connection with Time&Attendance (RCP Master software). Function [50] is available only in PR602LCD-DT and PR602LCD controllers.
[51]	Next T&A Mode (temporary)	The key is used in connection with Time&Attendance (RCP Master software). Function [50] is available only in PR602LCD-DT and PR602LCD controllers.
[56]	Predefined T&A Mode	The key is used in connection with Time&Attendance (RCP Master software).
[57]	Predefined T&A Mode (temporary)	The key is used in connection with Time&Attendance (RCP Master software).
[58]	Postponed auto-arming delay ON	When the key is pressed then auto-arming is delayed by the time specified with Programmed auto-arming delay option (see 3.5 Arming tab).
[59]	Postponed auto-arming delay OFF	When the key is pressed then auto-arming delay resulting from the option Programmed auto-arming delay is cancelled and the controller attempts to arm instantly if required by Arming/Disarming Schedule (see 3.5 Arming tab).
[60]	APB register reset	When the key is pressed then APB Register is reset (cleared) and any user can identify by means of proximity card and/or PIN at any terminal (reader) but in the next steps Anti-pass back rules must be followed.
[61]	Arm/Disarm switch (toggle)	The key is used to toggle Armed and Disarmed Modes.
[62]	XM-8 outputs OFF	When the key is pressed then all relay outputs of XM-8 expander connected to the controller are switched off.
[63]	XM-8 outputs ON	When the key is pressed then all relay outputs of XM-8 expander connected to the controller are switched on.
[64]	Normal Door Mode	When the key is pressed then Normal Door Mode is selected for the controller.

[65]	Unlocked Door Mode	When the key is pressed then Unlocked Door Mode is selected for the controller.
[66]	Cond. Unlocked Door Mode	When the key is pressed then Conditionally Unlocked Door Mode is selected for the controller.
[67]	Locked Door Mode	When the key is pressed then Locked Door Mode is selected for the controller.
[68]	Set LIGHT	When the key is pressed then LIGHT Flag (Timer) is on.
[69]	Clear LIGHT	When the key is pressed then LIGHT Flag (Timer) is off.
[70]	Toggle LIGHT	When the key is pressed then LIGHT Flag (Timer) is switched on/off.
[71]	Set AUX1	When the key is pressed then AUX1 Flag (Timer) is on.
[72]	Clear AUX1	When the key is pressed then AUX1 Flag (Timer) is off.
[73]	Toggle AUX1	When the key is pressed then AUX1 Flag (Timer) is switched on/off.
[74]	Set AUX2	When the key is pressed then AUX2 Flag (Timer) is on.
[75]	Clear AUX2	When the key is pressed then AUX2 Flag (Timer) is off.
[76]	Toggle AUX2	When the key is pressed then AUX2 Flag (Timer) is switched on/off.
[77]	Clear INTRUDER and TAMPER	When the key is pressed then INTRUDER and TAMPER Flags (Timers) are off.
[78]	Disarmed Mode	When the key is pressed then the controller is switched to Disarmed Mode.
[79]	Armed Mode	When the key is pressed then the controller is switched to Armed Mode.
[84]	Card or PIN Mode on term. ID0	When the key is pressed then Identification Mode of Terminal ID0 (reader) is switched to Card or PIN.
[85]	Card Only Mode on term. ID0	When the key is pressed then Identification Mode of Terminal ID0 (reader) is switched to Card Only.
[86]	PIN Only Mode on term. ID0	When the key is pressed then Identification Mode of Terminal ID0 (reader) is switched to PIN Only.
[87]	Card and PIN Mode on term. ID0	When the key is pressed then Identification Mode of Terminal ID0 (reader) is switched to Card and PIN.
[88]	Card or PIN Mode on term. ID1	When the key is pressed then Identification Mode of Terminal ID1 (reader) is switched to Card or PIN.
[89]	Card Only Mode on term. ID1	When the key is pressed then Identification Mode of Terminal ID1 (reader) is switched to Card Only.
[90]	PIN Only Mode on term. ID1	When the key is pressed then Identification Mode of Terminal ID1 (reader) is switched to PIN Only.
[91]	Card and PIN Mode on term. ID1	When the key is pressed then Identification Mode of Terminal ID1 (reader) is switched to Card and PIN.
[255]	Door bell	When the key is pressed then acoustic signal is generated by means of internal speaker and the output with function [15]:Door bell is activated. Both, acoustic signal and output are activated for 4 sec.

2.16 Schedules and Auxiliary Conditions

Schedules

Schedule is a weekly calendar (Monday – Sunday) with 4 holidays (H1-H4). The Schedule can be divided into maximum 128 periods defined by From... and To... parameters. Following types of Schedules are available in RACS 4 (PR Master software):

- General Purpose Schedules which can be applied to various functions and options within the controller. They are mainly used when defining access rights for users (see 2.7 Access Rights),
- T&A Mode Schedules which are used for automatic switching of T&A Mode at Terminal ID1. These Schedules are used only if PR Master software is used with RCP Master software (see 2.19.2 Time&Attendance based on RCP Master software),
- Door Mode Schedules which are used for automatic switching of Door Modes (see 2.5 Door Modes)
- APB Reset Schedules which are used for defining moments, when the controller automatically resets its Anti-passback Register (see 2.11 Anti-passback)
- Identification Mode Schedules which are used for automatic switching of Identification Mode (see 2.4 Identification Modes).

For each of mentioned above Schedules the administrator can define not only week days but also holidays. These are days, when usual Schedules of week days are not valid and instead of them some additional mechanisms are applied. Four different daily schemes (H1 – H4) for holidays within particular Schedule can be specified in RACS 4 system and then they can be assigned to particular dates in year. In case of PRxx2 series controllers, the maximum number of holiday dates equals to 120.

Auxiliary conditions

Many functions and options within controller properties (PR Master software) can be enabled for use according to administrator defined Schedules and/or only if certain Auxiliary Conditions are satisfied. It concerns:

- High Security Mode,
- [#] key options,
- Facility Code,
- Two User Mode,
- Use of cards and/or PINs assigned to SWITCHER users,
- Random User Check,
- Conditional Access,
- Keypad Commands,
- Input lines,
- Output lines,
- Function keys,
- Inputs and outputs at XM-2 expander.

Auxiliary Condition indicates additional circumstance or state that must be satisfied in order to enable use of particular function/option (positive logic, e.g. condition **[130]**) or in order to disable use of particular function/option (negative logic, e.g. condition **[131]**).

Example:

*If Auxiliary Conditions **[129]: Enabled when controller armed** is assigned to function key F1 then user will be able to use that key (and function assigned to that key) only if the controller is armed.*

Auxiliary Conditions can also be assigned to input/output lines or function keys. If the Auxiliary Condition is satisfied then particular line or key can be used (positive logic) or cannot be used (negative logic) depending on particular Auxiliary Condition. If particular Auxiliary Condition occurs then already activated line or key can be deactivated and disabled.

Example:

*If input line with function **[07]: Door bell** and Auxiliary Condition **[129]: Enabled when controller armed** is activated then it shall be automatically deactivated and disabled when the controller becomes disarmed.*

Table 10 Auxiliary Conditions	
No.	Condition
[128]	Enabled when controller disarmed
[129]	Enabled when controller armed
[130]	Enabled when IN1 is ON
[131]	Disabled when IN1 is ON
[132]	Enabled when IN2 is ON
[133]	Disabled when IN2 is ON
[134]	Enabled when IN3 is ON
[135]	Disabled when IN3 is ON
[136]	Enabled when IN4 is ON
[137]	Disabled when IN4 is ON
[138]	Enabled when last login on term.ID0
[139]	Enabled when last login on term.ID1
[140]	Enabled when room is occupied
[141]	Disabled when room is occupied
[142]	Enabled when limit of users in room is reached
[143]	Disabled when limit of users in room is reached
[144]	Enabled when controller in Normal Door Mode
[145]	Disabled when controller in Normal Door Mode
[146]	Enabled when controller in Unlocked Door Mode
[147]	Disabled when controller in Unlocked Door Mode
[148]	Enabled when controller in Cond. Unlocked Door Mode
[149]	Disabled when controller in Cond. Unlocked Door Mode
[150]	Enabled when controller in Locked Door Mode
[151]	Disabled when controller in Locked Door Mode
[152]	Enabled when LIGHT is ON
[153]	Disabled when LIGHT is ON
[154]	Enabled when TAMPER is ON
[155]	Disabled when TAMPER is ON
[156]	Enabled when AUX1 is ON
[157]	Disabled when AUX1 is ON
[158]	Enabled when AUX2 is ON
[159]	Disabled when AUX2 is ON

[160]	Enabled when INTRUDER is ON
[161]	Disabled when INTRUDER is ON
[162]	Enabled when FORCED ENTRY is ON
[163]	Disabled when FORCED ENTRY is ON
[164]	Enabled when PREALARM is ON
[165]	Disabled when PREALARM is ON
[166]	Enabled when DOOR AJAR is ON
[167]	Disabled when DOOR AJAR is ON
[255]	None

2.17 Special options

2.17.1 Two User Mode

In this mode, the controller grants access if two users (with different cards and/or PINs) undergo the authentication procedure in any order. Both users should carry out the authentication procedure according to the current Identification Mode (see 2.4 Identification Modes) in particular controller and both users are required to have access rights at the controller. The second authentication can be done at any reader connected to the controller (Terminal ID0 or ID1), thus allowing also such situation that both users are located at opposite sides of the door. Two User Mode cannot be activated separately for each side of the door. The mode is activated by selection of Schedule and it can be controlled by Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions).

Procedure for configuration of Two User Mode:

1. Within controller properties (PR Master software) select **Access** tab (see 3.4 Access tab) and in the area **Two User Mode** select Always Schedule or any other General Purpose Schedule previously defined by administrator. The General Purpose Schedule can be specified by means of the option **Schedules** in the main window of PR Master software.
2. Upload the configuration to the controller.

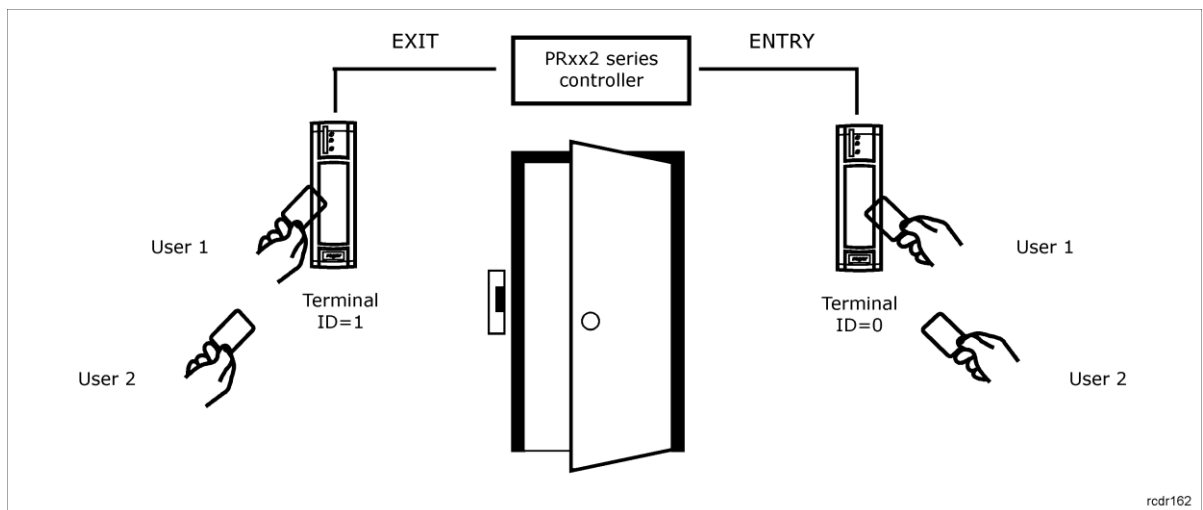


Fig. 9 Two User Mode

2.17.2 Conditional Access

In this mode, the controller grants access not only to users with access rights but also to all other users of RACS 4 system if any user with access rights is present in controlled room. Users (cards and/or PINs) unknown to RACS 4 system cannot get access at all. When there is no user in controlled room then only users with access rights can enter such room. In case of Conditional Access Mode all user of RACS 4 system can exit controlled room regardless of their access rights and number of users in the room.

Conditional Access Mode is based on Local Anti-passback (see 2.11 Anti-passback). The mode is activated by selection of Schedule and it can be controlled by Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions).

Note: Conditional Access Mode is based on Local Anti-passback therefore after reset of APB Register only user with access rights can enter the room. Further on, standard rules for Conditional Access Mode apply.

Procedure for configuration of Conditional Access

1. Specify Access Zone, where some users have access rights and some users do not have access rights (see 2.7 Access Rights).
2. In the properties of controller intended for Conditional Access Mode select **Advanced** tab (see 3.7 Advanced tab) and in the area **Conditional Access** select Always Schedule or any other General Purpose Schedule previously defined by administrator. The General Purpose Schedule can be specified by means of the option **Schedules** in the main window of PR Master software.
3. In the **APB** tab (see 3.8 APB tab) select the option **Enable Anti-passback**.
4. Assuming that Terminal ID0 is the entry reader to the room, select the tab **Terminal ID0** within controller properties (see 3.3 Terminal ID0) and then verify if in the field **Entry/exit (Local APB)** there is selected the option **Entrance to the room/area**. If not, then select that option. If Terminal ID1 is to be entry reader then enter analogical settings in **Terminal ID1** tab.
5. Upload the configuration to the controller.

2.17.3 High Security Mode

In this mode, the controller grants access if users undergoes two-stage authentication procedure. First, the user needs to authenticate at primary reader and then at secondary reader, both installed at the same side of the door. When this procedure is completed, the controller can grants access to the user. The mode can be defined separately for both sides of the door. The mode is activated by selection of Schedule and it can be controlled by Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). In practical applications the secondary reader could be biometric reader but any type of reader can be used as well. The secondary reader is always connected to RACS CLK/DTA terminals (see 2.2.3 RACS CLK/DTA interface) except for PR402DR controller, where Wiegand and Magstripe readers are connected to its input lines. In case of secondary readers which communicate with controller by means of RACS CLK/DTA protocol, the addresses ID2 or ID3 can be configured within Memory Reset procedure or by means of RARC software. The reader which is built in the controller (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302) has always address ID=1. Default address of new external reader is ID=0.

Procedure for configuration of High Security Mode:

1. Within controller properties (PR Master software) select **Terminal ID1** tab (see 3.2 Terminal ID1 tab) and in the area **High Security Mode** select method of communication with the secondary reader and Always Schedule or any other General Purpose Schedule defined by administrator. The General Purpose Schedule can be specified by means of the option **Schedules** in the main window of PR Master software.
2. If it is required to provide High Security Mode at both sides of the door then conduct the same steps in **Terminal ID0** tab within controller properties (see 3.3 Terminal ID0)
3. Upload the configuration to the controller.

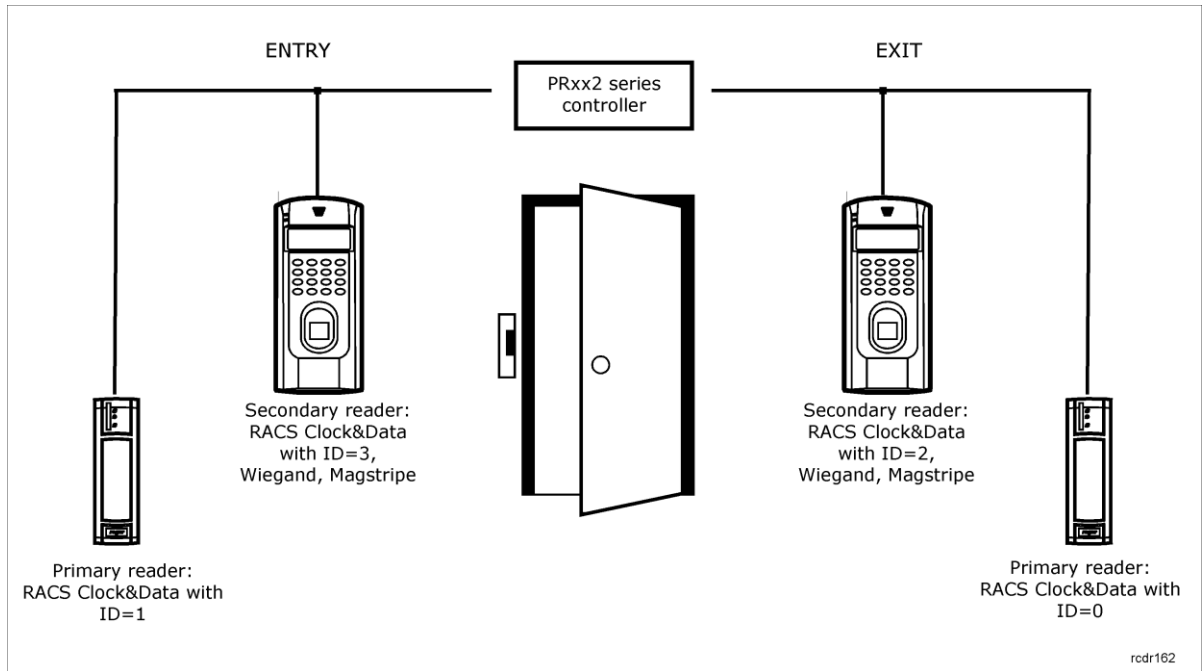


Fig. 10 High Security Mode

2.18 Keypad Commands

PRxx2 series controllers as opposed to PRxx1 series controller cannot be entirely configured by means of commands entered with controller keypad or external PRT series reader keypad. However there are some Keypad Commands available which are listed in table 11 and also within PR Master software (see 3.10 Keypad commands tab).

Commands may require authorization after entering by means of adequate identifier (card and/or PIN). The administrator can assign Schedule and Auxiliary Conditions for each Keypad Command (see 2.16 Schedules and Auxiliary Conditions). By default the controller accepts commands from both Terminals ID0 and ID1 but the administrator can limit commands to selected reader. The authorization, Schedule and Auxiliary Condition can be configured by means of the option

Properties.

In the table 11, the term [Authorisation] signifies use of authorised proximity card and/or PIN. The authorization requirement can be disabled for each Keypad Command individually.

Note: In systems with controllers connected to the same RS485 bus it is recommended not to use Keypad Commands for controller address modification as it shall result in discrepancy between actual controller settings and controller settings in PR Master software.

Table 11 Keypad Commands	
Command	Description
F00: Set controller ID	[*][0][0][#][Authorisation][new ID address][#] The command sets a new ID for the controller in range of ID=00-99.

F01: Set date	[*][0][1][#][Authorisation][DD][MM][YY][W][#] The command sets new date and a weekday according to following format: DD: Day (0-31) MM: Month (00-12) YY: Year (00-99) W: Day of week (0-6), where "0" refers to Sunday, "1" denotes Monday, etc.
F02: Set clock	[*][0][2][#][Authorisation][HH][MM][#] The command sets new time according to following format: HH: Hour (00-23) MM: Minute (00-59)
F07: Normal Door Mode	[*][0][7][#][Authorisation] The command activates the Normal Door Mode.
F08: Locked Door Mode	[*][0][8][#][Authorisation] The command sets the Locked Door Mode.
F09: Unlocked Door Mode	[*][0][9][#][Authorisation] The command activates the Unlocked Door Mode.
F10: Cond. Unlocked Door Mode	[*][1][0][#][Authorisation] The command activates the Conditionally Unlocked Door Mode.
F11: Disarmed Mode	[*][1][1][#][Authorisation] The command sets a controller in the Disarmed Mode.
F12: Armed Mode	[*][1][2][#][Authorisation] The command sets a controller in the Armed Mode.
F13: Arm/Disarm switch (toggle)	[*][1][3][#][Authorisation] The command toggles Armed/Disarmed Mode.
F14: Restart controller	[*][1][4][#][Authorisation] The command restarts the controller.
F15: APB Register reset	[*][1][5][#][Authorisation] The command clears/initializes the APB Register in the controller.
F16: Keypad selected T&A Mode	[*][1][6][#][Authorisation][NNN][#] The command sets the T&A Mode on ID1 terminal. The T&A Mode code is NNN(=000-255), The T&A Mode change is permanent.
F17: Keypad selected T&A Mode (temporary)	[*][1][6][#][Authorisation][NNN][#][Login] The command sets the T&A Mode on ID1 terminal. The T&A Mode code is NNN(=000-255). The T&A Mode change is temporary (approx. 8 sec.).

F18: Postponed auto-arming delay ON (default delay)	[*][1][8][#][Authorisation] The command postpones the auto-arming according to parameter: Programmed auto-arming delay (see 3.5 Arming tab).
F19: Postponed auto-arming delay ON (delay 1-255 min.)	[*][1][9][#][Authorisation][NNN][#] The command delays the auto-arming by NNN minutes, other auto-arming delays are deactivated.
F20: Postponed auto-arming delay OFF	[*][2][0][#][Authorisation] The command resets the auto-arming delay (if previously activated).
F21: Set LIGHT	[*][2][1][#][Authorisation] The command switches the LIGHT flag on.
F22: Clear LIGHT	[*][2][2][#][Authorisation] The command switches the LIGHT flag off.
F23: Toggle LIGHT	[*][2][3][#][Authorisation] The command toggles the LIGHT flag state.
F24: Set AUX1	[*][2][4][#][Authorisation] The command switches the AUX1 flag on.
F25: Clear AUX1	[*][2][5][#][Authorisation] The command switches the AUX1 flag off.
F26: Toggle AUX1	[*][2][6][#][Authorisation] The command toggles the AUX1 flag state.
F27: Set AUX2	[*][2][7][#][Authorisation] The command switches the AUX2 flag on.
F28: Clear AUX2	[*][2][8][#][Authorisation] The command switches the AUX2 flag off.
F29: Toggle AUX2	[*][2][9][#][Authorisation] The command toggles the AUX2 flag state.
F30: INTRUDER	[*][3][0][#][Authorisation] The command switches the INTRUDER flag on.
F31: Clear INTRUDER and TAMPER	[*][3][1][#][Authorisation] The command switches off both INTRUDER and TAMPER flags.
F32: Change Identification Mode for term.ID1	[*][3][3][#][Authorisation][N][#] The command switches the Identification Mode at Terminal ID1 according to N= 0..3, where: N=0: Card or PIN Mode N=1: Card Only Mode N=2: PIN Only Mode N=3: Card and PIN Mode

F33: Change Identification Mode for term.ID0	[*][3][3][#][Authorisation][N][#] The command is used in the same way as F32 with the only difference that this command pertains to Terminal ID0.
--	--

2.19 Time and Attendance (T&A)

In RACS 4 system there are two solutions for Time&Attendance. Both require use of PR Master software and access control system for events recording.

2.19.1 Time&Attendance based on Attendance Areas within PR Master software

This is very simple Time&Attendance solution which consists in counting the time of users presence in designated areas of RACS 4 access control system. This solution requires only proper configuration of PR Master software. T&A Modes are not used at all in case of Attendance Areas.

Procedure for configuration of Attendance Areas

1. Configure the access control system by means of the options: Access Zones, User Groups and Schedules in the main window of PR Master software (see 2.7 Access Rights).
2. In the main window of PR Master software select the option **Attendance Areas**.
3. In the opened window configure new area by entering its name as well as selecting entry and exit readers (Terminals ID0 and ID1). In practice, entrances and exits are usually readers located at the entrances and exits from/to the building/office. The administrator can assign multiple entry and exit readers within particular Attendance Area.
4. In case of Attendance Areas there is no need to select any options within the properties of any controller. Attendance Areas operate regardless of Access Zones, APB Zones or Alarm Zones. No settings are uploaded to controllers. In case of Attendance Areas, PR Master just interprets events recorded by access control system.
5. The summary of Time&Attendance can be accessed by means of the option **Reports** and then **Attendance**. The summary in the report is up to date if all events are downloaded from controllers and/or CPR to PR Master software. The command **Read event buffers now** in the main window or PR Master software can be used for that purpose.

Note: Attendance Reports are described in detail within PR Master manual.

2.19.2 Time&Attendance based on RCP Master software

PR Master software can record events which can be further exported to other program for detailed Time&Attendance summary in accordance with local laws or requirements. RCP Master is such external software for PR Master.

Note: RCP Master 2 can download events from PR Master as described below or alternatively operate as standalone software with dedicated PR602LCD-DT and PR602LCD controllers.

The PR602LCD-DT controller is recommended for Time&Attendance based on RCP Master as it is equipped with built-in reader, LCD and function keys but any terminal (reader) in RACS 4 system can be the terminal for registration of events for RCP Master. PRxx2 series controller can operate with two readers (Terminal ID0 and ID1) which can be used for registration of **[001] Access granted** events with different T&A Modes. In general perspective T&A Mode for events at Terminal ID0 is static and cannot be changed dynamically while T&A Mode for events at Terminal ID1 can be changed dynamically as given below.

In RACS 4 system the administrator can specify up to 255 T&A Modes which can be used to differentiate **[001] Access granted** events. Every T&A Mode has its code (0..255) and name. Additional text information can be assigned to T&A Mode by selection of the option **Tools** in the top bar of PR Master main window and then the option **T&A Modes**.

T&A Modes in almost whole range can be freely defined by administrator. Following T&A Modes are predefined within RACS 4 system:

- ENTRY (Code 000),
- EXIT (Code 016),
- ON-DUTY EXIT (Code 017),
- Breakfast break (Code 018)
- Lunch break (Code 019),
- Overtime1..5 (Codes 020..024),
- Exit on Request (Code 025),
- On duty (Code 026),
- NO T&A (Code 032),
- Starting work at pos.1..3 (Codes 033..035),
- Smoking brake (Code 036)
- Break (Code 037)
- Breastfeeding brake (Code 038)
- Custom 1..5 (Codes 101..105)
- On duty exit with day closing (Code 115)

Access granted events with NO T&A Mode (code 032) are ignored in Time&Attendance summaries. In order to prepare data for Time&Attendance it is necessary to export events with T&A Modes from PR Master software. For that purpose select the option **Event history** in the main window of PR Master software and then after selection of filter parameters select the option **T&A Report** and finally select the **OK** button. In the newly opened window select the format of output file. In the next step the exported file must be imported into RCP Master software.

T&A Mode switching

Default T&A Mode for particular reader (Terminal ID0 or ID1) can be assigned by means of PR Master software. For that purpose, open the properties of particular controller by clicking the controller in the main window of PR Master software and select the tab **Terminal ID0** and/or **Terminal ID1** (see 3.2 Terminal ID1 tab). In the field **Default T&A Mode** select desired mode. If the administrator selects **Entry** T&A Mode then all **[001]: Access granted** events at that reader shall be treated by system as work starting moments for users. The current T&A Mode can be switched manually by user or automatically by T&A Schedule. The T&A Mode can be switched permanently or temporary (approx. 8 sec.). Following methods can be used to switch T&A Mode of the reader:

- Input line – see 2.13 Inputs,
- Function key (at reader/controller keypad) – see 2.15 Function keys,
- Schedule – configured by means of the option **Schedules** and the tab **Options** in controller properties,
- Keypad Command from controller keypad or PRT reader keypad – see 2.18 Keypad Commands.

All mentioned above methods can be used interchangeably. The T&A Mode can be switched on Terminal ID1 i.e. the reader which is built in the controller (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302) or on the external reader connected to the controller (PR402, PR102DR). The Terminal ID0 for all controllers is always the external reader and it can have only default T&A Mode.

Note: If the option **Term. ID0 follows T&A Mode of Term. ID1** within controller properties (see 3.6 Options tab) is selected then it is possible to control dynamically and indirectly the T&A Mode at Terminal ID0 as it follows T&A Mode at Terminal ID1.

Method	Function	Description
Input line	[48]: Keypad selected T&A Mode	When the input is activated then the reader awaits for entering 3-digit code [NNN] which correspond to particular T&A Mode. After pressing the [#] key the reader switches to desired T&A Mode. The switching is permanent and concerns events from Terminal ID1,

		(NNN=000-255).
	[49]: Keypad selected T&A Mode (temporary)	When the input is activated then the reader awaits for entering 3-digit code [NNN] which correspond to particular T&A Mode. After pressing the [#] key the reader switches to desired T&A Mode. The switching is temporary (8 sec.) and concerns events from Terminal ID1, (NNN=000-255).
	[50]: Next T&A Mode	When the input is activated then the reader switches to the next available T&A Mode. The switching is permanent and concerns events from Terminal ID1. The function is available only for PR602LCD-DT and PR602LCD controllers.
	[51]: Next T&A Mode (temporary)	When the input is activated then the reader switches to the next available T&A Mode. The switching is temporary (8 sec.) and concerns events from Terminal ID1. The function is available only for PR602LCD-DT and PR602LCD controllers.
	[56]: Predefined T&A Mode	When the input is activated then the reader switches to T&A Mode which is predefined for that input. Predefined T&A Mode can be set in the controller properties (PR Master software) in the tab of particular input. The switching is permanent and concern events from Terminal ID1.
	[57]: Predefined T&A Mode (temporary)	When the input is activated then the reader switches to T&A Mode which is predefined for that input. Predefined T&A Mode can be set in the controller properties (PR Master software) in the tab of particular input. The switching is temporary (8 sec.) and concern events from Terminal ID1.
Functions keys	[48]: Keypad selected T&A Mode	See function [48] of input line.
	[49]: Keypad selected T&A Mode (temporary)	See function [49] of input line.
	[50]: Next T&A Mode	See function [50] of input line. The function is available only for PR602LCD-DT and PR602LCD controllers.
	[51]: Next T&A Mode (temporary)	See function [51] of input line. The function is available only for PR602LCD-DT and PR602LCD controllers.
	[56]: Predefined T&A Mode	See function [56] of input line.
	[57]: Predefined T&A Mode (temporary)	See function [57] of input line.
Keypad Commands	F16: Keypad selected T&A Mode	See table 11.
	F17: Keypad selected T&A Mode (temporary)	See table 11.

Other	T&A Mode Schedules	T&A Mode Schedule can be used for automatic switching of T&A Mode at Terminal ID1. The schedule defines periods for particular T&A Mode. The procedure for configuration of T&A Schedules is given below.
-------	--------------------	---

Procedure for configuration of T&A Mode Schedules

1. In the main window of PR Master software select the option **Schedules** and then select the tab **T&A Mode Schedules**.
2. In the newly opened window use the button **Add** and then enter the name of your schedule and specify periods for particular T&A Modes in week days.
3. In the main window of PR Master software click particular controller and enter its properties.
4. In the tab **Options**, in the area **T&A Mode** select the option **Enable T&A Schedule** and in the field **T&A Schedule** select previously defined schedule.
5. If necessary, in the tabs **Terminal ID1** and/or **Terminal ID0**, in the field **Default T&A Mode** select desired T&A mode. The administrator can define own T&A Modes selecting the option **Tools** in the top bar of PR Master main window and then selecting the option **T&A Modes**.
6. Besides T&A Modes it is necessary to assign T&A IDs. For that purpose select the option **Users** in the main window of PR Master software, then **Add** or **Edit** button and in the tab **General** enter the number in **T&A ID** field.

Note: More information on RCP Master software is given in its manual.

2.20 Login limits

In case of PRxx2 controller it is possible to specify how many times particular user can be granted access at particular controller (i.e. door). This feature is called login limits and in case of PR Master 4.5.6 or newer and PRxx2 firmware x.18.4.x or newer it is possible to configure not only manually renewed login limit but also automatically renewed login limit. The first one is configured for indefinite time and it requires manual renewal when depleted while the second one can be automatically refreshed in administrator defined periods.

Procedure for configuration of manually renewed login limit

1. Configure users in access control system (more information in PR Master manual).
2. Right click particular controller in the main window of PR Master software and then select **Login limit** option.
3. In the newly opened window select the button **Add**.
4. In the next window select any user from the list and specify his login limit.
5. Close all windows and return to the main window of PR Master software. New settings shall be updated automatically

or

1. During configuration of user by means of the option **Users** in the main window of PR Master software, in the properties of particular user select the tab **Login limits** and then press the button **Read user login limits from all controllers**. Login limit can be configured both for new and existing user.
2. Select the controller from the list and press the button **Modify**.
3. Select the number from the list for the parameter **Login limit**
4. Close the window and update new settings by pressing the button **Update** or **Update all**.

Procedure for configuration of automatically renewed login limit

1. Select the controller in the main window of PR Master software and open the tab **Options**.
2. In the area **Automatic login limit refresh** (see 3.6 Options tab) specify such parameters as **Refresh period** and **Start refresh at**
3. Configure users in access control system (more information in PR Master manual).

4. Right click particular controller in the main window of PR Master software and then select **Login limit** option.
5. In the newly opened window select the button **Add**.
6. In the next window select any user from the list, specify his login limit and select the option **Periodic refresh**.
7. Close all windows and return to the main window of PR Master software. New settings shall be updated automatically

or

1. Select the controller in the main window of PR Master software and open the tab **Options**.
2. In the area **Automatic login limit refresh** (see 3.6 Options tab) specify such parameters as **Refresh period** and **Start refresh at**
3. During configuration of user by means of the option **Users** in the main window of PR Master software, in the properties of particular user select the tab **Login limits** and then press the button **Read user login limits from all controllers**. Login limit can be configured both for new and existing user.
4. Select the controller from the list and press the button **Modify**.
5. Select the number from the list for the parameter **Login limit** and select the option **Periodic refresh**.
6. Close the window and update new settings by pressing the button **Update** or **Update all**.

III. PROGRAMMING

PRxx2 series controllers are programmed by means of PR Master management and monitoring software which can be downloaded from www.roger.pl. In the present section, all options available in the controller properties are described. Controller properties can be accessed by clicking particular controller in the main window of PR Master software. The options are used not only for configuration of the controllers but also for configuration of the access control system. The remaining options are described PR Master manual.

PRxx2 series controllers as opposed to PRxx1 series controller cannot be entirely configured by means of commands entered with controller keypad or external PRT series reader keypad. However there are some Keypad Commands available (see 2.18 Keypad Commands).

Note: Hints are provided for all options in the PR Master software. In order to display particular hint just point your mouse to the option and wait approx. 1 sec.

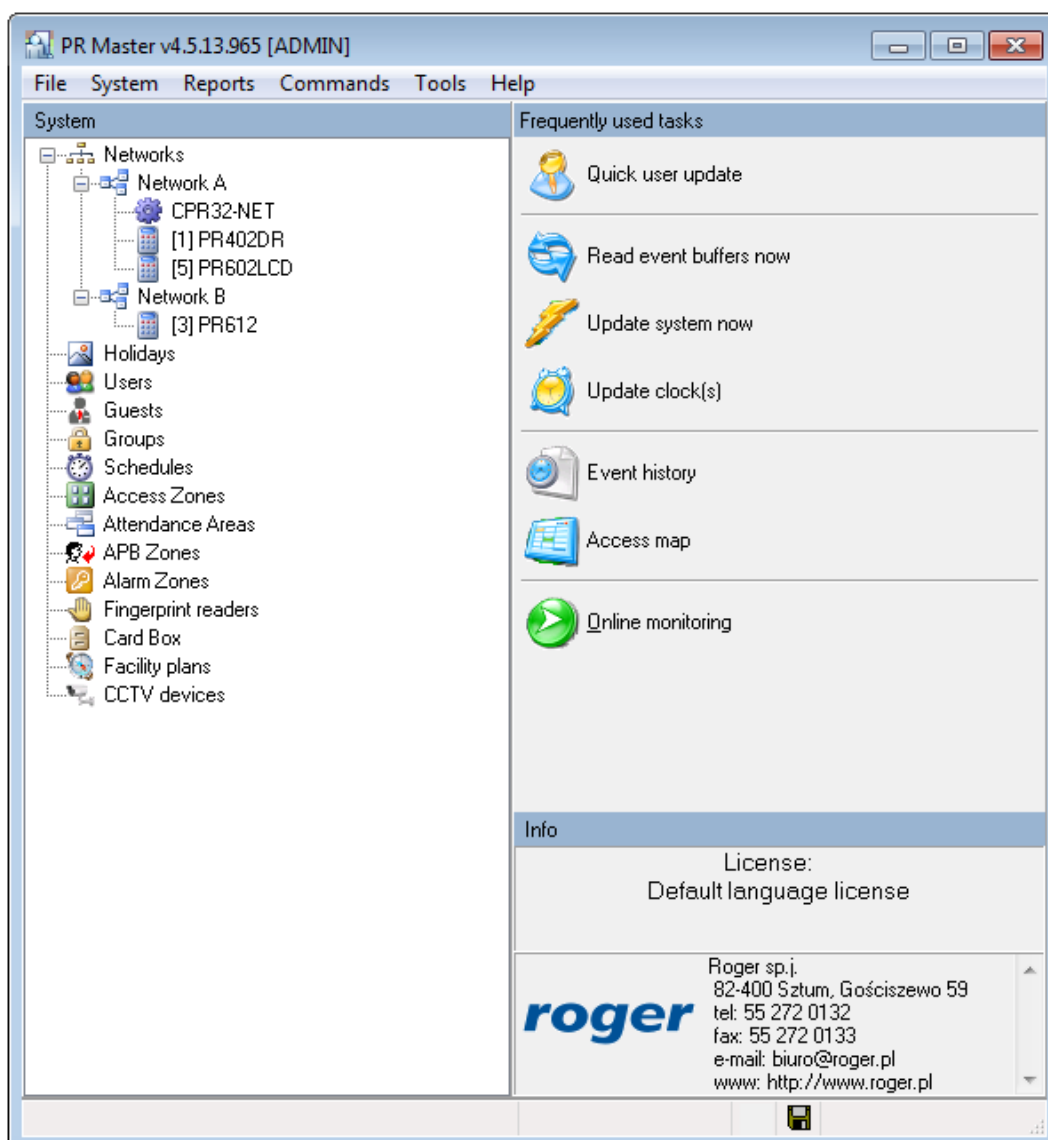


Fig. 11 The main window of PR Master software

3.1 General tab

In the **General** tab, the administrator can activate or deactivate the controller, change the name of controller and acquire some general information i.e.:

- Controller type,
- Controller address (ID),
- Firmware version,
- Controller name,
- Name of the subsystem (network).

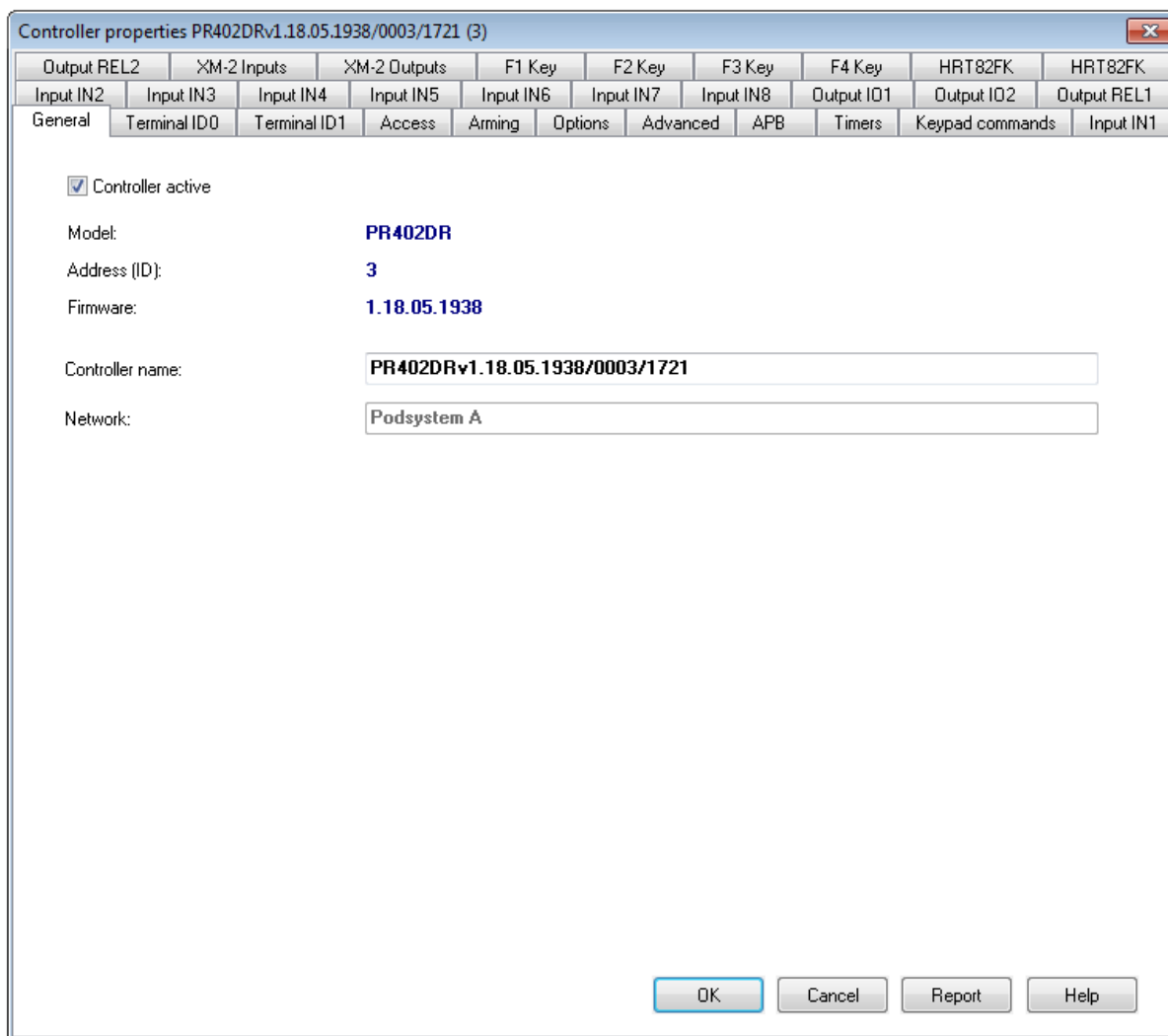


Fig. 12 General tab

3.2 Terminal ID1 tab

Terminal ID1 is the reader built into the controller (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302) or the external reader connected to the controller (PR102DR, PR402) (see 1.2 Design and architecture).

Fig. 13 Terminal ID1 tab

Area: Terminal ID1

In this area, the administrator can modify the name of reader, enter comments and select communication method with the reader (see 2.2.3 RACS CLK/DTA and 2.2.8 Wiegand/Magstripe interface readers). Proper functioning of controller and reader sometimes requires also configuration of reader including mode, address, etc. New PRT series readers are by default configured to RACS CLK/DTA mode with ID=0 address.

Option: Default T&A Mode – the option enables selection of predefined or administrator defined T&A Mode for the reader. The option is not used if Time&Attendance based on Attendance Areas is applied. For more information – see 2.19.2 Time&Attendance based on RCP Master software.

Option: Access Zone – the option is used for selection of the reader as the entrance to particular Access Zone. The Access Zone can be created by means of the option **Access Zones** in the main window of PR Master software. For more information – see 2.7 Access Rights.

Option: APB Zone (Global APB) – the option is used for selection of the reader as the entrance to APB Zone. The Anti-passback Zone can be defined by means of the option **APB Zones** in the main window of PR Master software. The option is used in Global APB and it is active if the option **Enable Anti-passback** is activated in the **APB** tab. For more information - see 2.11 Anti-passback

Option: Entry/exit (Local APB) – the option is used for selection of the reader as the entry or the exit reader for Local APB. The option is activated if the option **Enable Anti-passback** is activated in the **APB** tab. For more information - see 2.11 Anti-passback.

Area: High Security Mode

In this area, the administrator can select the secondary reader for parallel operation with Terminal ID1 in High Security Mode (see 2.17.3 High Security Mode). The Schedule and Auxiliary Conditions can be assigned to High Security Mode (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when High Security Mode is activated. If Always Schedule is selected then High Security Mode is active all the time.

Area: [#] key options

In this area, the administrator can activate the option **Enable [#] key to operate alternatively as Door Bell/Exit Button**. The Schedule and Auxiliary Conditions can be assigned to the option (see 2.16 Schedules and Auxiliary Conditions). If predefined Never Schedule is selected then [#] key at controller keypad or connected PRT series reader keypad operates in the same way as function key with the function **[255]: Door bell** (see 2.15 Function keys). If the function **[15]: Door bell** is assigned to one of output lines of the controller then external buzzer or any other acoustic device can be connected to that line. If predefined Always Schedule is selected then [#] key at controller keypad or connected PRT series keypad operates as function key with the function **[02]: Release door**. The administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. Then, in periods specified by parameters From... and To... the [#] key shall operate as exit button and in the remaining time as door bell button.

Area: Identification Mode

In this area, the administrator can select default Identification Mode (see 2.4 Identification Modes). The administrator can also assign Identification Mode Schedule after defining such Schedule by means of the option **Schedules** in the main window of PR Master software.

3.3 Terminal ID0 tab

In the tab **Terminal ID0** all options are the same as in the tab **Terminal ID1**. Terminal ID0 is always the external reader connected to PRxx2 series controller (see 1.2 Design and architecture).

3.4 Access tab

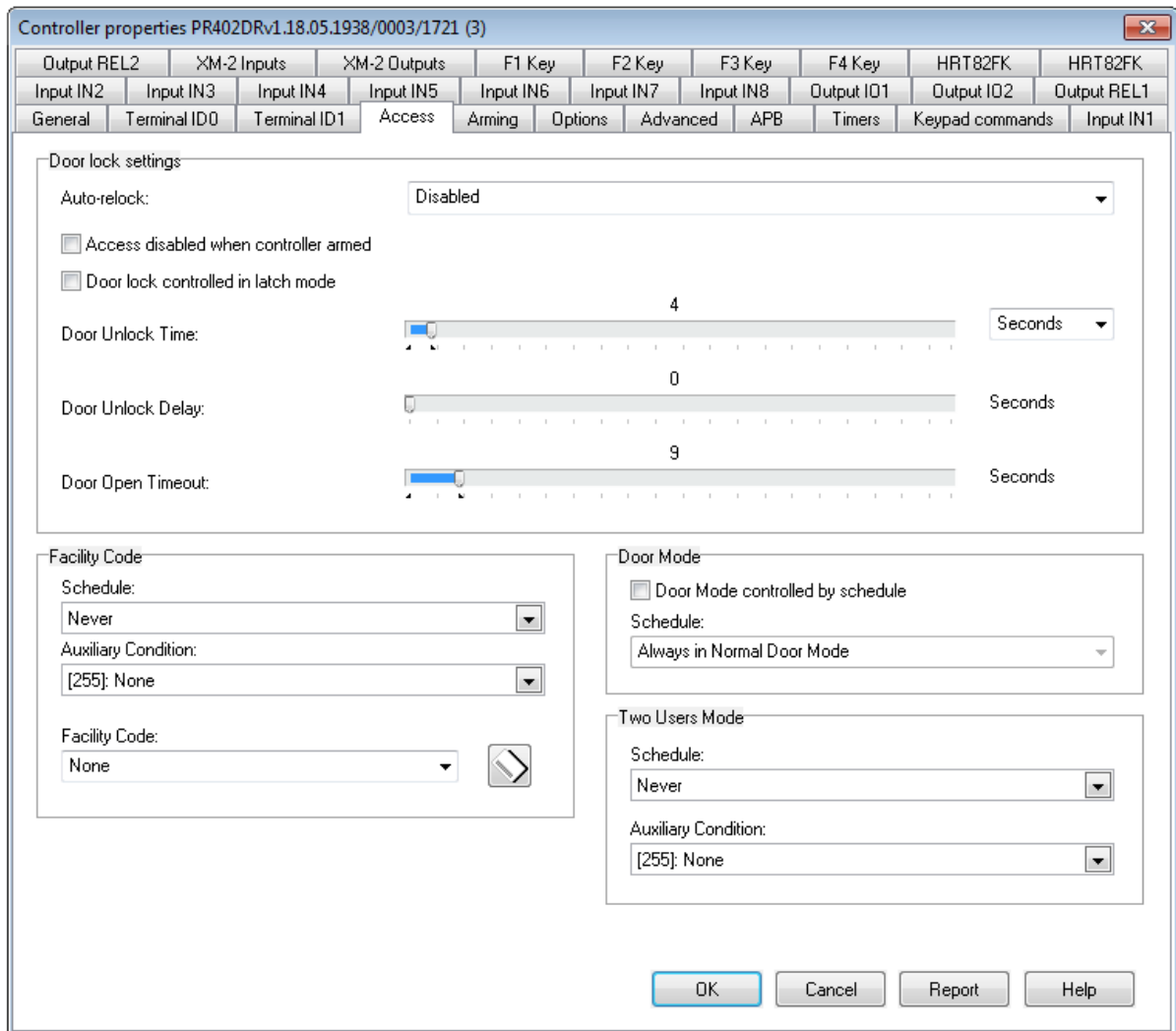


Fig. 14 Access tab

Area: Door lock settings

In this area, the administrator can configure options and parameters related to door lock which is connected to the controller (see 2.7 Access Rights).

Option: Auto-relock – the option is useful only if door contact is connected to controller input (see 2.13 Inputs). Based on this option the controller can block door lock earlier than it would result from the parameter **Door Unlock Time**. The option can be disabled or one of following settings can be selected:

- Block the door lock upon door opening detection,
- Block the door lock upon door closing detection

Based on the first setting, the controller deactivates its relay output connected to the door lock when door opening is detected. In other words, the lock is blocked immediately when door opening is detected and not after time specified by parameter **Door Unlock Time** elapses. Based on the second setting, the controller blocks the lock immediately when door closing is detected.

Option: Access disabled when controller armed – when this option is selected then access can be granted only when the controller is disarmed (see 2.6 Armed/Disarmed Modes). If the controller is armed then the access is denied for all users, regardless of their access rights.

Based on that option, users who can arm/disarm the controller (e.g. SWITCHER type users) can also block and unblock the access to other users regardless of their access rights.

Option: Door lock controlled in latch mode – when this option is selected then access granting switches the output relay (which is connected to the door lock) to the opposite state. The output remains in such state as long as the next access granting occurs. In other words, door lock can be closed or opened all the time. If the option is not selected then relay output is activated for the time specified by the parameter **Door Unlock Time** and then it automatically returns to the previous state.

Parameter: Door Unlock Time – this parameter is used for specifying how long the door lock must be opened. The range of possible settings is from 1 sec. to 99 minutes.

Parameter: Door Unlock Delay – this parameter is used for specifying delay for door opening after access granting. The range of possible settings is from 1 sec. to 99 sec.

Parameter: Door Open Timeout – this parameter is used for specifying time required for door closing after access granting. In order to make this parameter useful it is necessary to connect door contact to controller input (see 2.13 Inputs). If the time specified by parameter **Door Open Timeout** elapses and the door is still opened then the Door Alarm called DOOR AJAR is raised (see 2.9 Door Alarm and 2.10 System Flags (Timers)). The range of possible settings is from 1 sec. to 99 sec.

Area: Facility Code

In this area, the administrator can configure Facility Code (see 2.8 Facility Code) as well as assign Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when Facility Code is activated. By means of the button with card icon, the administrator can read his proximity card by means of connected reader in order to determine its Facility Code (specified part of card number).

Area: Door Mode

In this area, the administrator can select the option **Door Mode controlled by schedule** (see 2.5 Door Modes) and assign predefined Schedule i.e. Always in Normal Door Mode or assign own Schedule which can be defined by means of the option **Schedules** in the main window of PR Master software.

Area: Two User Mode

In this area, the administrator can activate Two User Mode (see 2.17.1 Two User Mode) by selection of predefined Schedule i.e. Always or by selection of own Schedule specified by means of the option **Schedules** in the main window of PR Master software. The activation of Two User Mode can also depend on Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions).

3.5 Arming tab

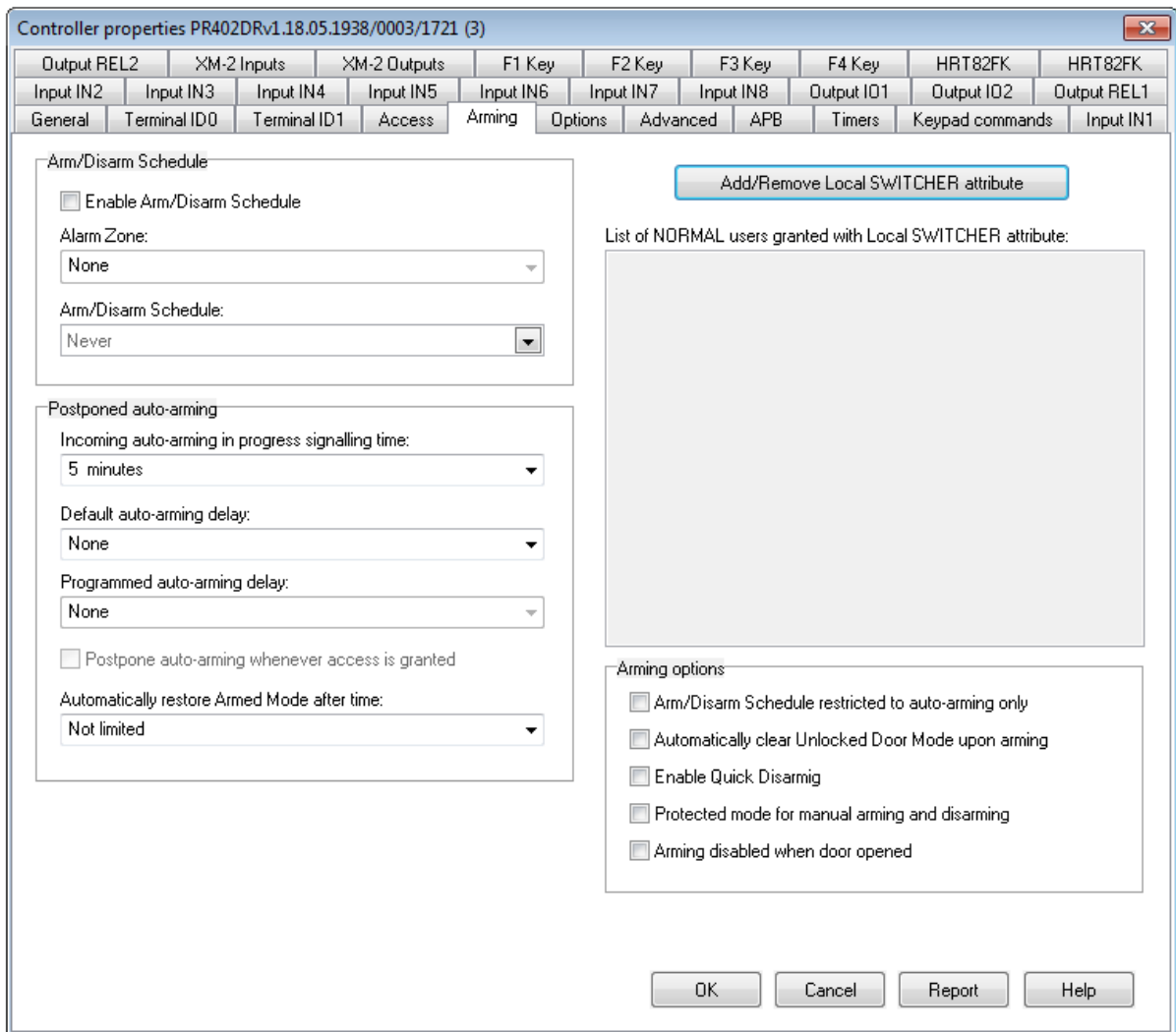


Fig. 15 Arming tab

Area: Arm/Disarm Schedule

Option: Enable Arm/Disarm Schedule – this option is used for switching Arm/Disarm Schedule on/off (see 2.6 Armed/Disarmed Modes). Arm/Disarm Schedule can be used in the integration of RACS 4 system with intruder alarm systems.

Option: Alarm Zone – the option is used for assigning the controller to particular Alarm Zone (see 2.12 Alarm Zones). Alarm Zones are created by means of the option **Alarm Zones** in the main window of PR Master software. The controller assigned to particular Alarm Zone switches to Armed/Disarmed Mode concurrently with other controllers belonging to the same Alarm Zone (see 2.6 Armed/Disarmed Modes) and in accordance with the Schedule assigned to that Alarm Zone. Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The Schedule can be assigned to particular Alarm Zone by means of the option **Alarm Zones** in the main window of PR Master software.

Option: Arm/Disarm Schedule – the option is used for assigning Arm/Disarm Schedule directly to the controller and not to Alarm Zone with group of controllers (see 2.6 Armed/Disarmed Modes). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main

window of PR Master software. The schedule is configured by means of From... and To... parameters and the first parameter signifies the moment when controller becomes disarmed while the second parameter signifies the moment when the controller becomes armed. When predefined Always Schedule is selected then the controller by default is in Disarmed Mode and when predefined Never Schedule is selected then the controller by default is in Armed Mode but the controller does not monitor its arming mode regularly. It switches to default mode when restarted or after configuration upload.

Area: Auto-arming

Parameter: Incoming auto-arming in progress signalling time – the parameter is used for specifying how many minutes prior to controller arming based on Arm/Disarm Schedule, the controller shall signal such incoming auto-arming (see 2.6 Armed/Disarmed Modes). The signalling can be acoustic one at reader/controller buzzer or it can be electric one at the output line of controller with the function **[33]: Incoming auto-arming in progress (steady)** and/or **[34]: Incoming auto-arming in progress (pulsed)** (see 2.14 Outputs). The purpose of such signalling is to warn in advance all persons inside the premises that scheduled arming of controller shall occur soon. The range of possible settings is from 1 to 99 minutes.

Parameter: Default auto-arming delay – this parameter is used for specifying the delay (in minutes) for controller which attempts to arm in accordance with Arm/Disarm Schedule (see 2.6 Armed/Disarmed Modes). The delay is activated if in the moment of scheduled arming, the controller input line with the function **[13]: Arming disabled** (see 2.13 Inputs) is activated. The delay is repeated till the input line with function **[13]** is deactivated or the arming is no longer required by the Schedule. The purpose of the delay is to enable automatic postpone of controller arming by external device/system. The range of possible settings is from 5 to 99 minutes.

Parameter: Programmed auto-arming delay – this parameter is used for specifying the delay (in minutes) for controller which attempts to arm in accordance with Arm/Disarm Schedule (see 2.6 Armed/Disarmed Modes). The functioning of this delay is the same as in case of parameter **Default auto-arming delay** but this delay is activated not by the input line of the controller with the function **[13]: Arming disabled** (see 2.13 Inputs) but by the input line with the function **[58]: Postponed auto-arming delay ON**, by the function key with the function **[58]: Postponed auto-arming delay ON** or by the Keypad command **F18: Postponed auto-arming delay ON (default delay)**. The delay is repeated as long as the user activates it by means of one the mentioned above methods or the arming is no longer required by the Schedule. The purpose of the delay is to enable manual postpone of controller arming by the user. The range of possible settings is from 5 to 99 minutes.

Option: Postpone auto-arming whenever access granted – when this option is selected then **Programmed auto-arming delay** (see above) can be activated not only by three mentioned above methods (input line, function key and Keypad Command) but also by access granting (use of card and/or PIN by user with access rights).

Parameter: Automatically restore Armed Mode after time – the parameter is used for specifying the delay (in minutes) for automatic rearming of the controller according to Arm/Disarm Schedule. The purpose of the delay is to arm the controller automatically if the user disarmed the controller manually (see 2.6 Armed/Disarmed Modes) and according to the Schedule the controller should be armed at that moment. Such rearming can be delayed by the user based on the parameter **Programmed auto-arming delay** (see above). The range of possible settings is from 5 to 99 minutes.

Area: Local SWITCHER


In this area, the administrator can assign Local Switcher attribute to NORMAL users (with ID in range of 1000 – 3999) in order to allow them to arm and disarm the controller (see 2.6 Armed/Disarmed Modes). As opposed to MASTER user, SWITCHER Full user and SWITCHER Limited user (see 2.3 Users), the NORMAL user with Local SWITCHER attribute can only arm and disarm these controllers, where the attribute is assigned and not all controllers in RACS 4 system.

Area: Arming options

Option: Arm/Disarm Schedule restricted to auto-arming only – when this option is selected then Arm/Disarm Schedule can only arm the controller (see 2.6 Armed/Disarmed Modes) while disarming must be conducted manually or remotely.

Option: Automatically clear Unlocked Door Mode upon arming – when the option is selected then the Unlocked Door Mode is switched to Normal Door Mode (see 2.5 Door Modes) when the controller becomes armed (see 2.6 Armed/Disarmed Modes). The purpose of this option is to prevent such situation that controller is armed and at the same time door lock is released because of the Unlocked Door Mode.

Option: Enable quick disarming – when this option is selected then MASTER and SWITCHER Full users as well as NORMAL users with Local Switcher attribute (see 2.6 Armed/Disarmed Modes) can disarm the controller with single card swipe and/or PIN entering. Arming still requires double card swipe and/or PIN entering. Switcher Limited user always arms and disarms with single card swipe and/or PIN entering regardless of that option.

Option: Protected mode for manual arming and disarming – when this option is selected then SWITCHER Limited user (see 2.3 Users) must use his identifier (card and/or PIN) five times in order to arm/disarm the controller (see 2.6 Armed/Disarmed Modes). MASTER and SWITCHER Full users as well as NORMAL users with Local SWITCHER attribute must actually use their identifiers six times in order to arm/disarm the controller as the first use is related to door lock opening. Identifier must be swiped without unnecessary delays when the orange LED SYSTEM  is on.

Note: If the Card and PIN Identification Mode is selected for the terminal (see 2.4 Identification Modes) then the PIN must be entered once and then the card must be swiped five times in order to arm/disarm the controller.

Option: Arming disabled when door opened – when the option is selected then arming of controller is blocked if the door contact connected to the controller signals that the door is opened. Door contact must be connected to controller input. The option can block manual arming (by means of card/PIN, function key, Keypad Command) but cannot block Arm/Disarm Schedule and if automatic arming is configured then it works in the same way as input line of the controller with the function **[13]: Arming disabled** which affects the parameter **Default auto-arming delay** (i.e. auto-arming is repeatedly delayed till the door is closed or the arming is no longer required by the Schedule).

3.6 Options tab

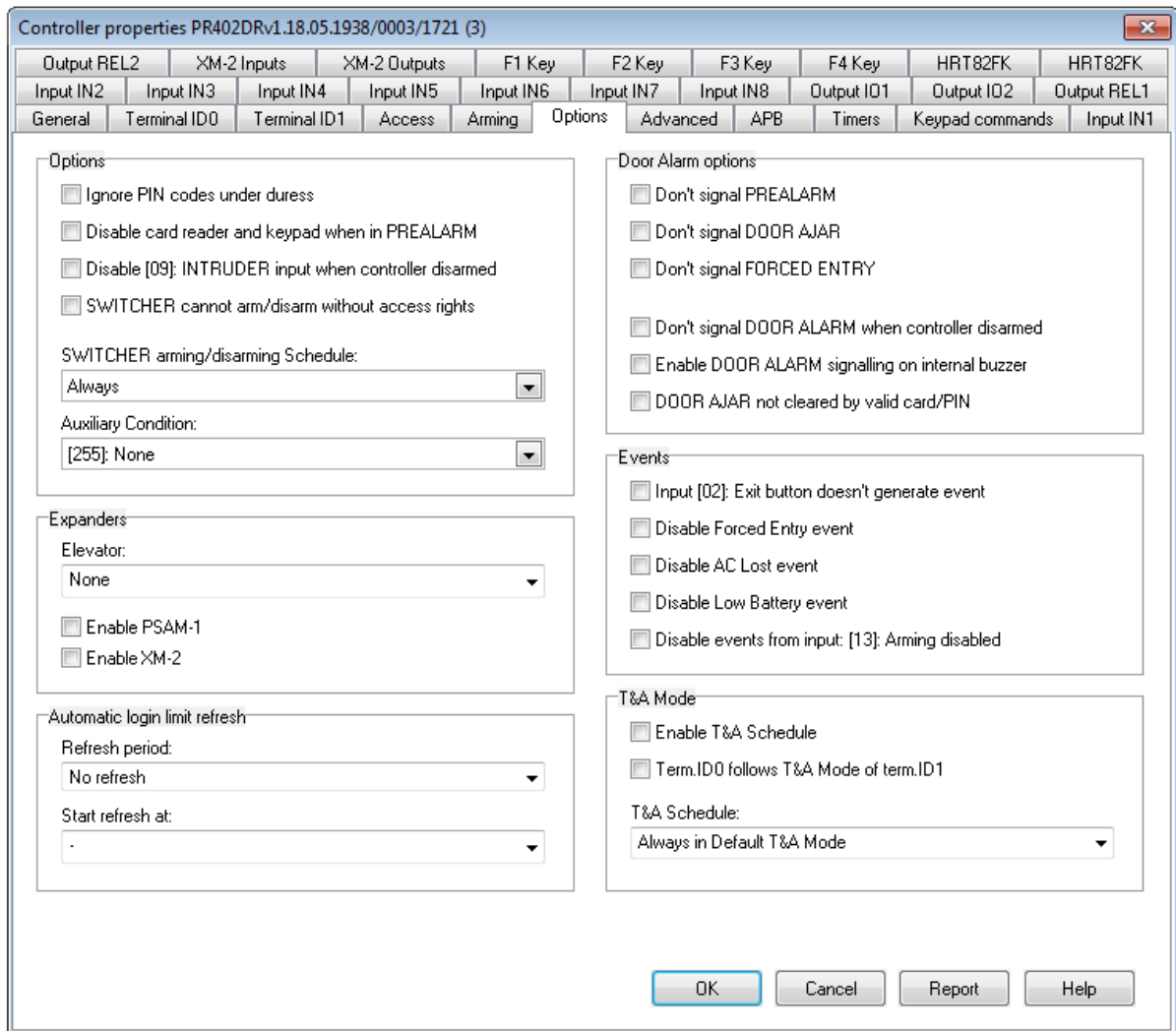


Fig. 16 Options tab

Area: Options

Option: Ignore PIN codes under duress – when this option is selected then entering of PIN that differs +/-1 from correct (authorized) PIN is interpreted by the controller as wrong PIN and access is denied. When the option is not selected then entering of PIN which differs +/-1 from correct (authorized) PIN results in granting the access by the controller but the alarm called FORCED ENTRY is also raised (see 2.9 Door Alarm and 2.10 System Flags (Timers)).

Example:

*When the option **Ignore PIN codes under duress** is selected and the correct PIN is [4569][#] then entering of [4568][#] or [4570][#] is interpreted as wrong PIN. When the option is not selected then entering of [4568][#] or [4570][#] results in the access granting by the controller and Door Alarm called FORCED ENTRY is raised.*

Option: Disable card reader and keypad when in PREALARM– when the option is selected then the controller rejects card reading and PIN entering as long as the Door Alarm called PREALARM is activated (see 2.9 Door Alarm) i.e. as long as flag PREALARM is on (see 2.10 System Flags (Timers)). PREALARM is raised when the unknown identifier (card or PIN) is used 5 times in a row at the controller.

Option: Disable [09]: INTRUDER input when controller disarmed – when the option is selected then the controller ignores the activation of its input line with the function **[09]: INTRUDER** (see 2.13 Inputs) and consequently the system flag INTRUDER is not activated (see 2.10 System Flags (Timers) when the controller is disarmed (see 2.6 Armed/Disarmed Modes).

Option: SWITCHER cannot arm/disarm without access rights – when the option is selected then SWITCHER Full and SWITCHER Limited users as well as NORMAL users with Local SWITCHER attribute (see 2.3 Users) cannot arm/disarm controller if they are not assigned with access rights at that controller. The option does not affect MASTER user.

Option: SWITCHER arming/disarming Schedule – the option is used for assigning Schedule for SWITCHER full and SWITCHER Limited users as well as for NORMAL users with Local SWITCHER attribute (see 2.3 Users) in order to enable or disable their arming/disarming rights. Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software.

Option: Auxiliary Condition – the option is used for assigning Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions) for SWITCHER full and SWITCHER Limited users as well as for NORMAL users with Local SWITCHER attribute (see 2.3 Users) in order to make their arming/disarming rights dependant on that condition.

Area: Expanders

Option: Elevator – this option is used for assigning elevator to the controller. The option is used in configuration of access control in elevators based on XM-8 expander(s). More information on such application is provided in 2.2.5 XM-8 I/O expander and in XM-8 Installation Guide which is available at www.roger.pl

Option: Enable PSAM-1 – when this option is selected then operation of the controller with PSAM-1 module is enabled. More information on power supply supervision is provided in 2.2.6 PSAM-1 and in PSAM-1 Installation Guide which is available at www.roger.pl

Option: Enable XM-2 – when the option is selected then operation of the controller with XM-2 expander is enabled and functions to XM-2 inputs and outputs in respective tabs (see 3.14 XM-2 Inputs tab and 3.15 XM-2 Outputs tab) can be assigned. More information on XM-2 expander is provided in 2.2.4 XM-2 I/O expander and in XM-2 Installation Guide which is available at www.roger.pl

Area: Automatic login limit refresh

Parameter: Refresh period: – the parameter is used for configuration of refreshing period for renewable login limit (see 2.20 Login limits). Following settings are available: No refresh, 1h, 2h, 3h, 4h, 6h, 12h and 24h.

Parameter: Start refresh at: – the parameter is used for configuration of starting moment for renewable login limit (see 2.20 Login limits). The starting moment is selected from the list e.g. 01:00 o'clock. Minutes cannot be specified.

Area: Door Alarm options

Option: Don't signal PREALARM – when the option is selected then the controller does not signal the alarm called PREALARM at its output line with the function **[256]: Door alarm** (see 2.9 Door Alarm and 2.14 Outputs). The option does not block other methods for raising the PREALARM, in particular, it does not block the output line of controller with the function **[29]: PREALARM** and PREALARM System Flag (see 2.10 System Flags (Timers)). The option does not block also other Door Alarms associated with the function **[256]** i.e. DOOR AJAR and FORCED ENTRY. The event related to PREALARM is recorded in event history and it is displayed in Online Monitoring of PR Master software.

Option: Don't signal DOOR AJAR – when the option is selected then the controller does not signal the alarm called DOOR AJAR at its output line with the function **[256]: Door alarm** (see 2.9 Door Alarm and 2.14 Outputs). The option does not block other methods for raising the DOOR AJAR alarm in particular, it does not block the output line of controller with the function **[30]: DOOR AJAR** and DOOR AJAR System Flag (see 2.10 System Flags (Timers)). The option does not block also other Door Alarms associated with the function **[256]** i.e. PREALARM and FORCED ENTRY. The event related to DOOR AJAR is recorded in event history and it is displayed in Online Monitoring of PR Master software.

Option: Don't signal FORCED ENTRY – when the option is selected then the controller does not signal alarm called FORCED ENTRY at its output line with the function **[256]: Door alarm** (see 2.9 Door Alarm and 2.14 Outputs). The option does not block other methods for raising the DOOR AJAR alarm in particular, it does not block the output line of controller with the function **[28]: FORCED ENTRY** and FORCED ENTRY System Flag (see 2.10 System Flags (Timers)). The option does not block also other Door Alarms associated with the function **[256]** i.e. PREALARM and DOOR AJAR. The event related to FORCED ENTRY is recorded in event history and it is displayed in Online Monitoring of PR Master software.

Option: Don't signal DOOR ALARM when controller disarmed – when the option is selected then the controller blocks all possible Door Alarms at its output line with the function **[256]: Door alarm** (see 2.9 Door Alarm and 2.14 Outputs) if the controller is disarmed (see 2.6 Armed/Disarmed Modes). In such case, Door Alarms are also not signalled at output lines with functions **[29]: PREALARM**, **[30]: DOOR AJAR**, **[28]: FORCED ENTRY** and respective System Flags are not activated (see 2.10 System Flags (Timers)), but events related to Door Alarms are recorded in event history and they are displayed in Online Monitoring of PR Master software.

Option: Enable DOOR ALARM signalling on internal buzzer – when the option is selected then Door Alarms (see 2.9 Door Alarm) can be additionally signalled acoustically by internal buzzer of controller (PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302) or by the buzzer of reader (only with ID=1 address) connected to the controller (PR102DR, PR402).

Option: DOOR AJAR not cleared by valid card/PIN – when the option is selected then Door Alarm called DOOR AJAR (see 2.9 Door Alarm) and respective DOOR AJAR System Flag (see 2.10 System Flags (Timers)) cannot be cleared by use of authorized card and/or PIN.

Area: Events

Option: Input [02]: Exit button doesn't generate event – when this option is selected then the event **[001]: Access granted** is not recorded in log and is not displayed in Online Monitoring of PR Master software when the access is granted based on function key with the function **[02]: Release door**, input line with the function **[02]: Exit button** or input line with the function **[47]: Entry button**. For all other methods (card and/or PIN), **[001]** event is recorded in the Event history.

Option: Disable Forced Entry event – when this option is selected then the event **[005] Forced Entry** related to Door Alarm called FORCED ENTRY (see 2.9 Door Alarm) is not recorded in log and is not displayed in Online Monitoring of PR Master software. The methods for raising this alarm are listed in 2.10 System Flags (Timers). The option does not block activation of FORCED ENTRY flag or activation of output lines with functions **[256]:Door alarm** or **[28]: FORCED ENTRY**.

Option: Disable AC Lost event – when this option is selected then the alarm related to power supply failure is not recorded in log and is not displayed in Online Monitoring of PR Master software but output line of the controller with the function **[37]: AC failure** can be activated. The option concerns both the power supply connected to the controller via 230VAC/18VAC transformer (PR402) and operation with PSAM-1 module (see 2.2.6 PSAM-1).

Option: Disable Low Battery event – when this option is selected then the alarm related to low voltage of battery connected to the controller is not recorded in the log and is not displayed in Online Monitoring of PR Master software but output line of the controller with the function **[38]: Low battery** can be activated. The option concerns the battery connected directly to the controller (PR402) and operation with PSAM-1 module (see 2.2.6 PSAM-1).

Option: Disable events from input: [13]: Arming disabled – when the option is selected then both events **[13]: Arming disabled -ON** and **[13]: Arming disabled -OFF** are not recorded in the log and are not displayed in Online Monitoring of PR Master software. The option does not affect the operation of input line with the function **[13]: Arming disabled** i.e. the option blocks only events and not input lines.

Area: T&A Mode

Option: Enable T&A Schedule – when the option is selected then T&A Mode at Terminal ID1 (see 1.2 Design and architecture) can be switched by T&A Schedule. In case of PR602LCD-DT, PR602LCD, PR612, PR622, PR312EM, PR312MF and PR302 controllers, built-in reader is Terminal ID1. In case of PR402 and PR102DR controllers, Terminal ID1 is an external reader. The procedure for configuration of T&A Schedule is provided in 2.19.2 Time&Attendance based on RCP Master software.

Option: Term. ID0 follows T&A Mode of term. ID1 – when this option is selected then T&A Mode at Terminal ID0 (see 1.2 Design and architecture) is the same as T&A Mode at Terminal ID1. Generally, T&A Mode at Terminal ID0 is static while T&A Mode at Terminal ID1 can be switched dynamically. The option enables indirect control of T&A Mode at Terminal ID0. The methods for switching T&A Mode at Terminal ID1 are listed in 2.19.2 Time&Attendance based on RCP Master software.

Option: T&A Schedule – this option is used for assigning T&A Schedule to Terminal ID1 of the controller. The procedure for configuration of T&A Schedules is described in 2.19.2 Time&Attendance based on RCP Master software.

3.7 Advanced tab

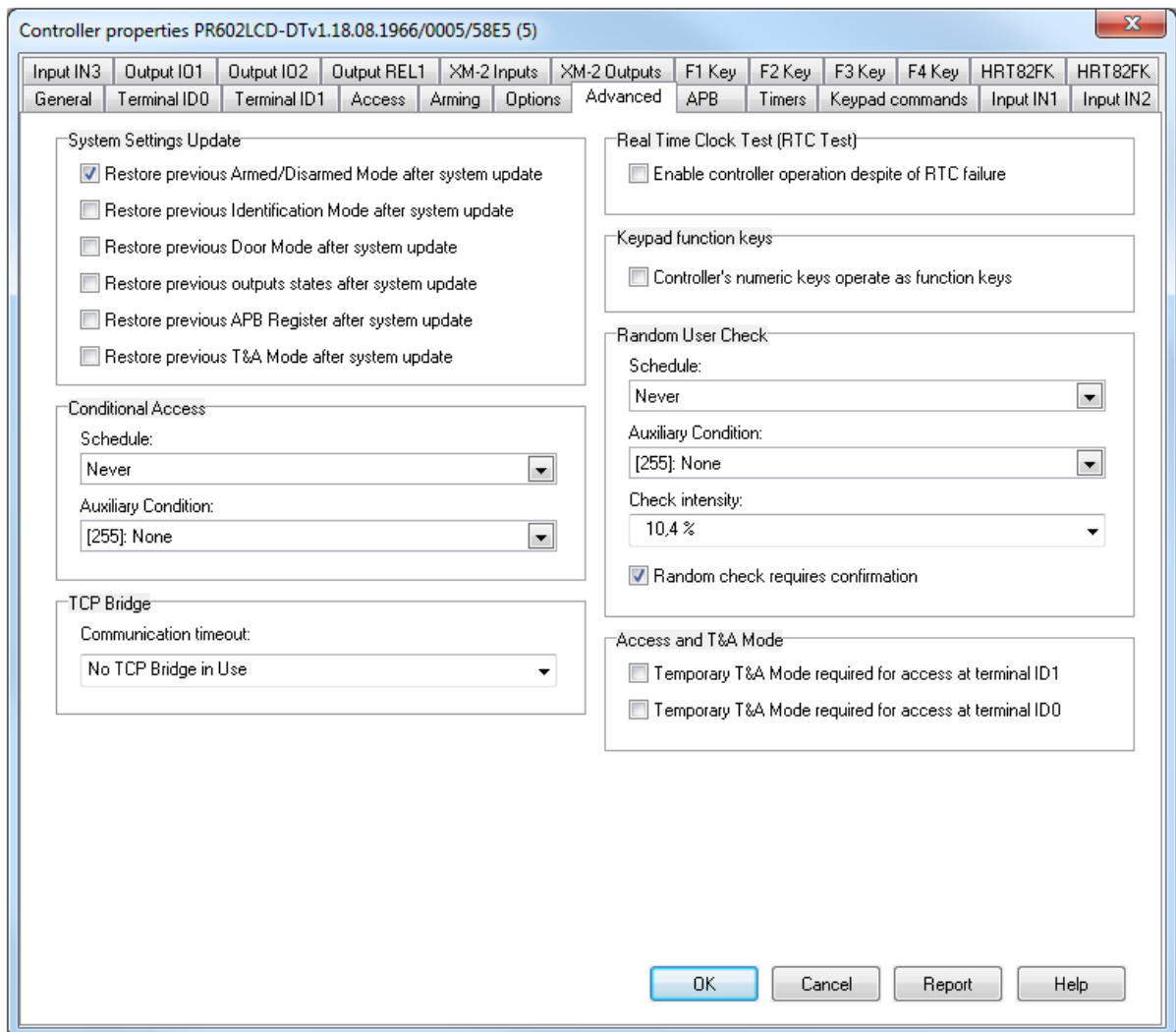


Fig. 17 Advanced tab

Area: System Settings Update

Option: Restore previous Armed/Disarmed Mode after system update – when this option is selected then after configuration update, the controller shall restore the same Armed/Disarmed Mode (see 2.6 Armed/Disarmed Modes) as it was before configuration update. If the option is not selected then the controller by default switches to Armed Mode after configuration upload unless it is against Arm/Disarm Schedule which has higher priority.

Option: Restore previous Identification Mode after system update – when this option is selected then after configuration update, the controller shall restore the same Identification Mode (see 2.4 Identification Modes) as it was before configuration update. The option has higher priority than scheduled Identification Mode and default Identification Mode (see 3.2 Terminal ID1 tab).

Option: Restore previous Door Mode after system update – when this option is selected then after configuration update, the controller shall restore the same Door Mode (see 2.5 Door Modes) as it was before configuration update. The option has higher priority than scheduled Door Mode and default Door Mode (see 3.4 Access tab).

Option: Restore previous output states after system update – when this option is selected then after configuration update, the controller shall restore ON/OFF states of its output lines as they were before the configuration update. The controller restores its output lines with following functions:

- **[08]: PC Command** if the line was activated remotely from PR Master software
- **[13]: Schedule or PR Command** if the line was activated remotely from PR Master software
- **[64]: LIGHT**
- **[66]: AUX1**
- **[67]: AUX2**

Option: Restore previous APB Register after system update – when this option is selected then after configuration update, the controller shall restore APB Register (see 2.11 Anti-passback) as it was before the configuration update.

Option: Restore previous T&A Mode after system update – when this option is selected then after configuration update, the controller shall restore T&A Mode (see 2.19.2 Time&Attendance based on RCP Master software) as it was before configuration update. The option has higher priority than scheduled T&A Mode (see 3.6 Options tab) or default T&A Mode (see 3.2 Terminal ID1 tab).

Area: Conditional Access

In this area, the administrator can configure Conditional Access Mode (see 2.17.2 Conditional Access) by assigning Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when Conditional Access Mode is activated, in the remaining time the mode is disabled. Activation of the mode (its Schedule) can also depend on Auxiliary Condition. In order to use Conditional Access Mode it is necessary to select the option **Enable Anti-passback** in **APB** tab.

Area: TCP Bridge

In this area, the administrator can select communication timeout for the controller connected to RS485 bus via TCP bridge consisting of two UT-4 interface in LAN/WAN network. The range of possible settings is from 20ms to 5 sec. with 20ms resolution.

Area: Real Time Clock Test (RTC Test)

Option: Enable controller operation despite of RTC failure – when this option is selected then the controller shall operate even if its own RTC is not operating correctly.

Area: Keypad function keys

This area is available only in case of PR602LCD, PR612, PR312EM, PR312MF and PR302 controllers as they are equipped with keypad. By means of the option **Allow controller's keypad to operate as function key input**, the administrator enables use of numeric keys as function keys. Numeric keys from 1 to 4 correspond to function keys from F1 to F4 at Terminal ID1 while numeric keys from 5 to 8 correspond to function keys from F1 to F4 at Terminal ID0 (see 1.2 Design and architecture and 2.15 Function keys).

Area: Random User Check

In this area, the administrator can configure random selection of users for inspection. When it is activated then the controller randomly denies the access for users with access rights. These users can then be inspected by guardsmen. Such access denial is signalled acoustically on the at reader/controller buzzer or by means of message displayed at controller LCD (only PR602LCD type). Additionally it can also be signalled at controller output line with the function **[39]: Random**

check request (see 2.14 Outputs). The signalling lasts for 2 sec. and the controller denies the access for such time. Random User Check concerns only NORMAL user types (see 2.3 Users). The function is activated by selection of Schedule. Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when Random User Check is activated, in the remaining time the function is disabled. Activation of the function (its Schedule) can also depend on Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions).

Parameter: Check intensity – this option is used for specifying average number of users (in percents) subject to inspection. The range of possible settings is from 0,4% to 99,6% with 0,4% resolution. The higher the value of parameter the more frequently the inspection is signalled. For example, if the intensity equals to 10% then statistically every tenth person shall be indicated for inspection.

Option: Random check requires confirmation – when this option is selected then the controller based on Random User Check denies the access until its input line with the function **[46]: Random check confirm** is activated (see 2.13 Inputs) or function key with the function **[46]: Random check confirm** is pressed (see 2.15 Function keys).

Area: Access and T&A Mode

Option: Temporary T&A Mode required for access at terminal ID1 – when this option is selected then user is denied access regardless of his access rights until temporary T&A Mode is selected. Such T&A Mode is activated for 8 sec. using input or function key with such functions as **[49]: Keypad selected T&A Mode (temporary)**, **[51]: Next T&A Mode (temporary)**, **[57]: Predefined T&A Mode (temporary)** (see 2.13 Inputs and 2.15 Function keys).

Option: Temporary T&A Mode required for access at terminal ID0 – as above but it concerns terminal ID0.

3.8 APB tab

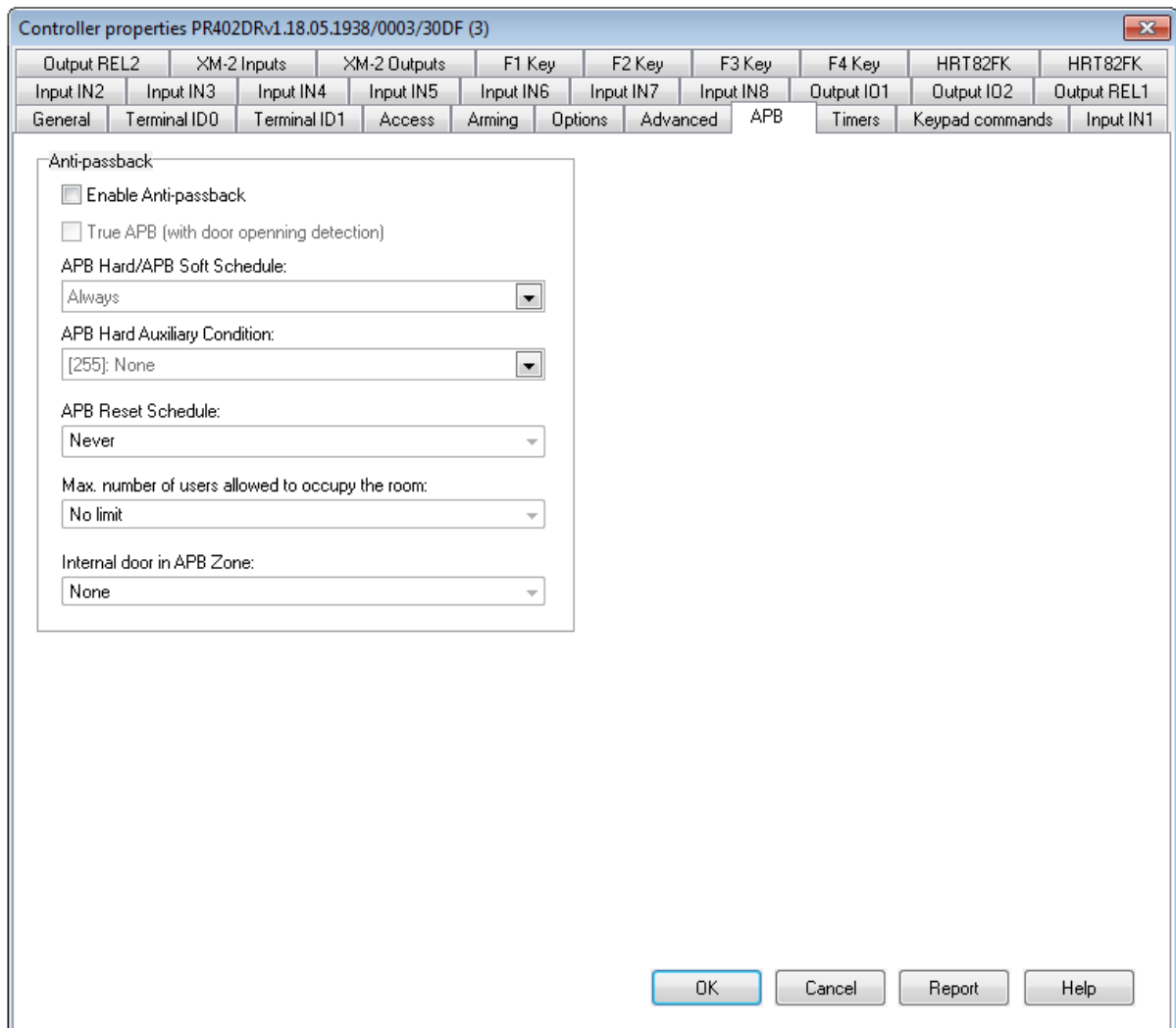


Fig. 18 APB tab

Area: Anti-passback

Option: Enable APB – it is necessary to select this option in order to enable Local or Global Anti-passback and proceed with further APB settings (see 2.11 Anti-passback).

Option: True APB (with door opening detection) – this option is available if the option **Enable APB** (see above) is selected. This option activates so called True APB (see 2.11 Anti-passback) which requires connection of door contact to controller's input line with the function **[01]: Door contact**

Option: APB Hard/APB Soft Schedule – this option is used for assigning the Schedule for Soft and Hard APB (see 2.11 Anti-passback). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. Within the periods defined by the Schedule, Hard APB is applied and for the rest of time Soft APB is applied. Therefore selection of Always Schedule results in permanent Hard APB while selection of Never Schedule results in permanent Soft APB.

Option: APB Hard Auxiliary Condition – this option is used for assigning Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions) to APB Hard/APB Soft Schedule. If the

condition is not satisfied then Soft APB is applied and if the condition is satisfied then APB Hard/APB Soft Schedule is applied.

Option: APB Reset Schedule – this option is used for assigning Schedule to Anti-pass back Register reset (see 2.11 Anti-passback). Predefined Never Schedule is already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software.

Parameter: Max. number of users allowed to occupy the room – this option is used for limiting the maximum number of users in particular room with single door. The option concerns Local Anti-passback (see 2.11 Anti-passback). In case of Global APB, the maximum number of users in the room is defined when APB Zone is created by means of the option **APB Zones** in the main window of PR Master software. The range of possible settings is from 1 to 3999 users.

Option: Internal door in APB Zone – this options is used to assign particular controller (and its terminals) to APB Zone in order to configure internal door within this APB Zone. User can be granted access at such door only if he entered APB Zone through one of entry points/terminals to the APB Zone. For more information see 2.11 Anti-passback.

3.9 Timers tab

In this tab, the administrator can configure Timers (see 2.10 System Flags (Timers)). Timer can be set in latch mode and then it triggers infinitely to opposite state (on/off) or it can be assigned with time parameter which denotes how long the Timer is activated. The last possible setting is None which means complete turning off the Timer.

Example:

Activation of LIGHT Timer in latch mode, by means of controller input line with the function [68]: Set LIGTH results in activation of controller output line with the function [64]: LIGHT. As the Timer was in latch mode then the output line with the function [64] shall be activated till the controller input line with the function [69]: Clear LIGTH is activated

If time is assigned to Timer then respective System Flag is activated for that time. The range of possible settings is from 1 second to 120 minutes.

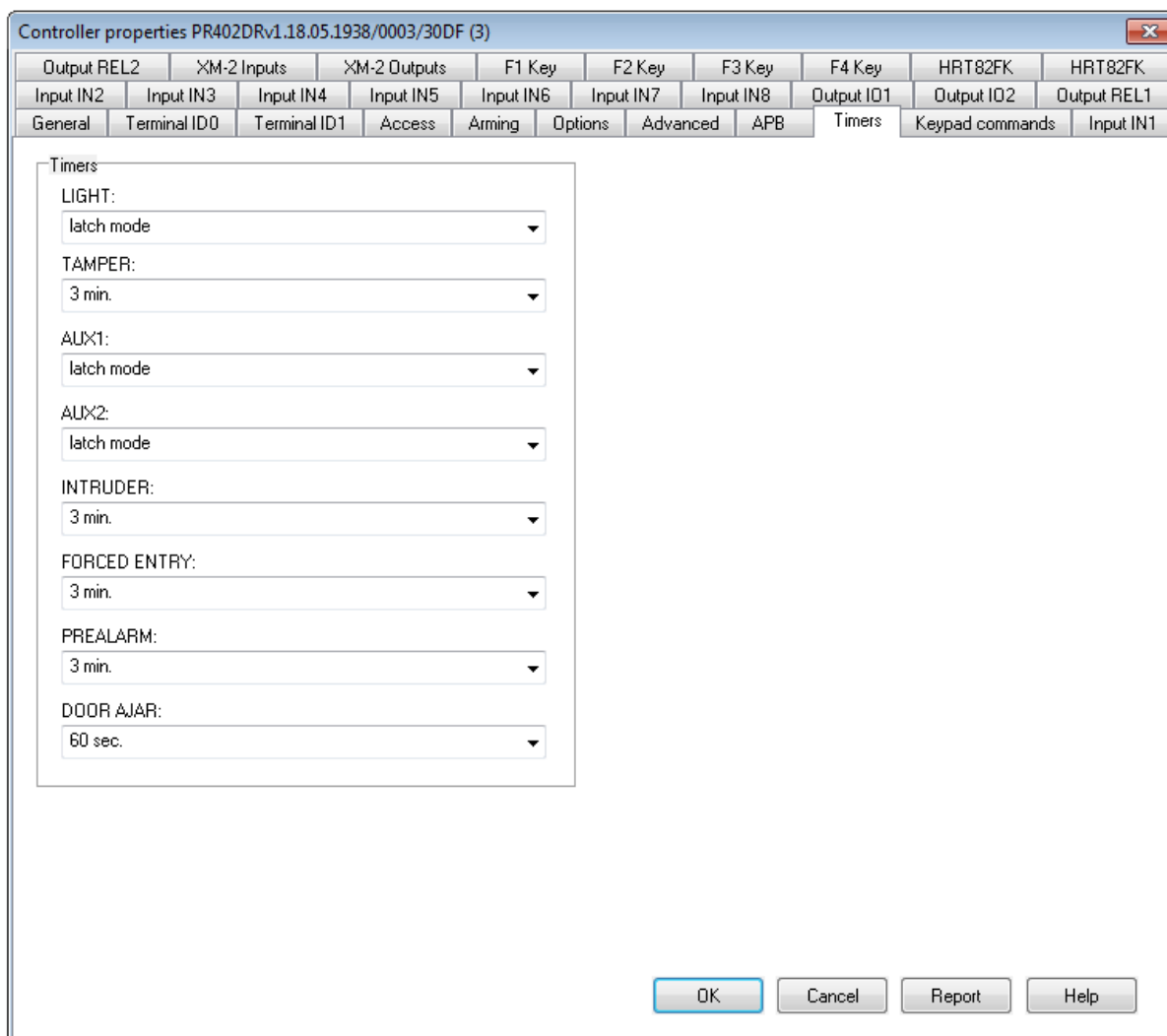


Fig. 19 Timers tab

3.10 Keypad commands tab

In this tab, the administrator can configure rules regarding use of Keypad Commands at controller/reader (see 2.18 Keypad Commands and 1.2 Design and architecture). It is possible to get the information on command syntax by selection of the button **Properties**. In the newly opened window, the administrator can assign Schedule and Auxiliary Condition to Keypad Commands (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when Keypad Command can be used but it still may require authorization. When the Never Schedule is selected then the command is disabled. In the same window, the administrator can select the option **Authorization required**. When the option is activated then every use of particular Keypad Command requires authorization by means of proximity card and/or PIN. The list of authorized users is configured by means of the option **Users allowed to use keypad commands** in the main window of tab.

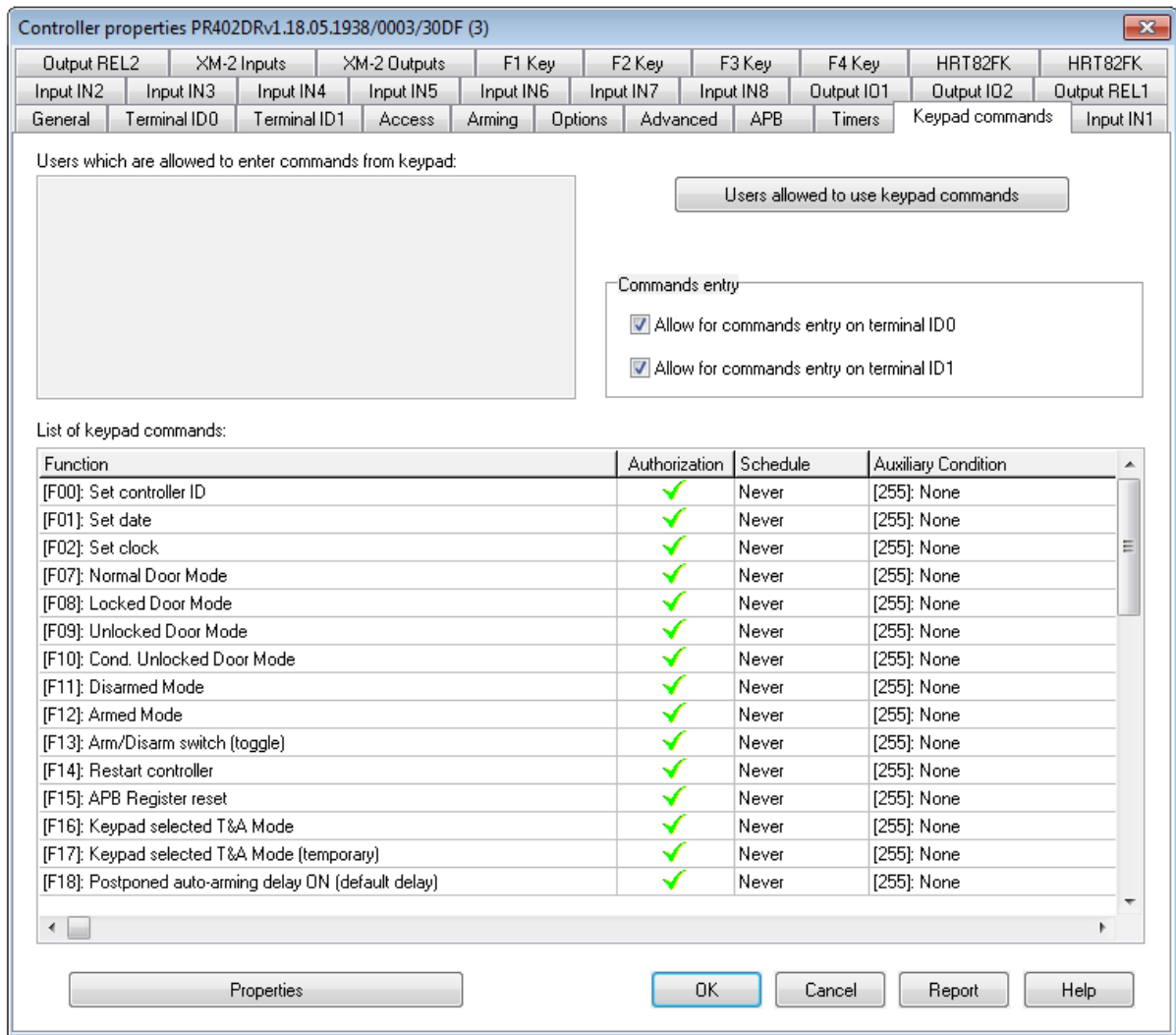


Fig. 20 Keypad command tab

Option: Users allowed to use keypad commands – this option is used for selecting users who can use Keypad Commands when authorization is enabled.

Option: Allow for commands entry on Terminal ID0 – when this option is selected then Keypad Commands (see 2.18 Keypad Commands) can be entered by means of keypad at Terminal ID0 (see 1.2 Design and architecture).

Option: Allow for commands entry on Terminal ID1 – when this option is selected then Keypad Commands (see 2.18 Keypad Commands) can be entered by means of keypad at Terminal ID1 (see 1.2 Design and architecture).

3.11 Input IN1...IN8 tabs

Depending on the number of input lines available in particular controller (see Table 1), respectively 2 to 8 tabs are displayed in controller properties. In the tab **Input IN1** and the remaining tabs, the administrator can assign function (see 2.13 Inputs) to particular input line. Moreover, type of the line i.e. NC or NO can be selected and in case of T&A functions (see 2.19.2 Time&Attendance based on RCP Master software) default T&A Mode can be specified. Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions) can also be assigned to the input line. Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the

input line can be used. In case of Always Schedule, the input line can be used all the time. The Schedule does not signify the time when the input is activated but only the time when the line can be activated.

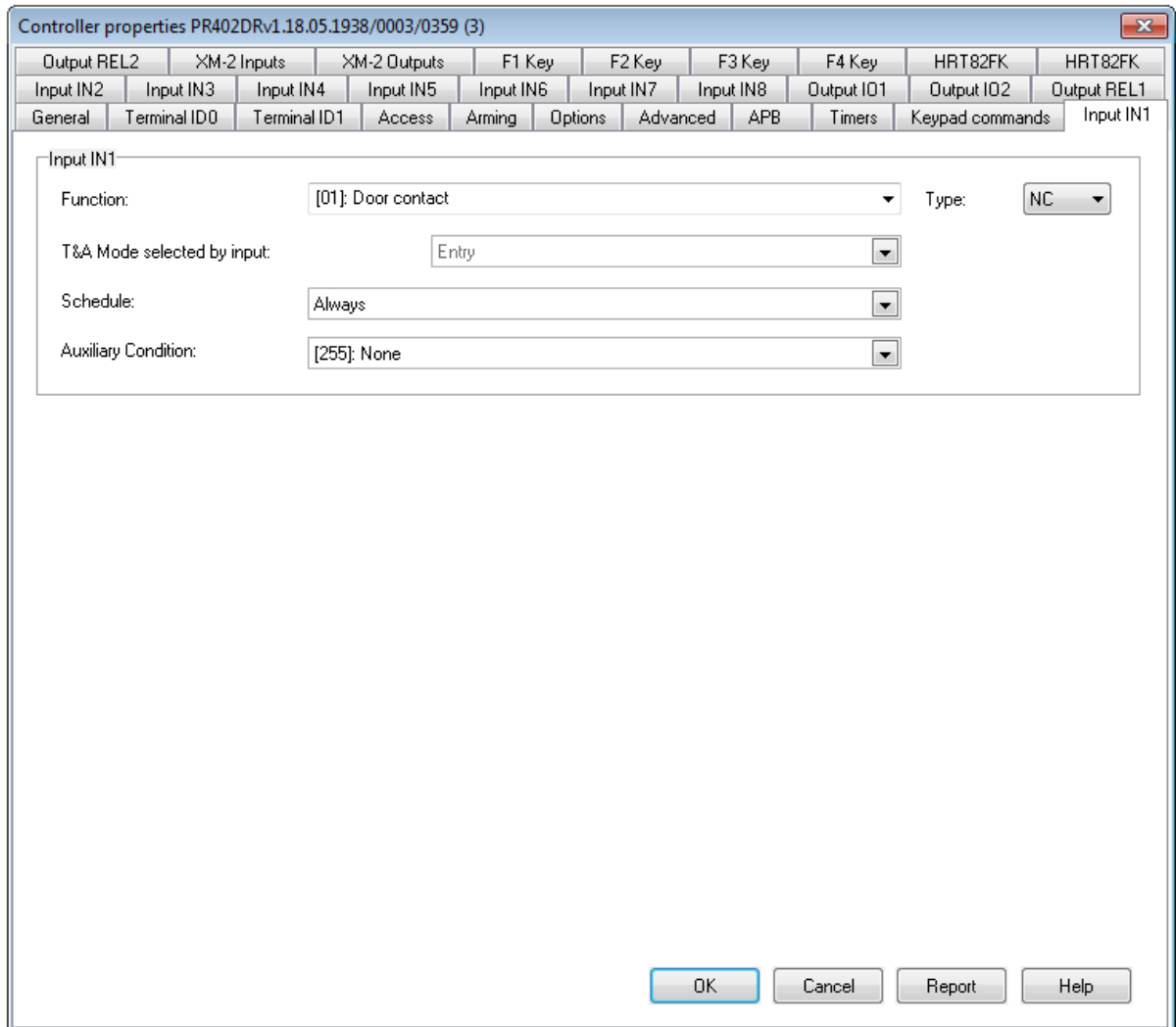


Fig. 21 Input IN1 tab

3.12 Output IO1...IO2 tabs

Depending on the number of transistor output lines available in particular controller (see Table 1), respectively 1 or 2 tabs are displayed in controller properties. In the tab **IO1 Output** or **IO2 Output**, the administrator can assign function (see 2.14 Outputs) to particular output line as well as Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the output line can be used. In case of Always Schedule, the output line can be used all the time. In general, the Schedule does not signify the time when the output is activated but only the time when the line can be activated. The only exceptions are functions **[12]: Schedule** and **[13]: Schedule or PC commands** which actually are activated by assigned Schedule.

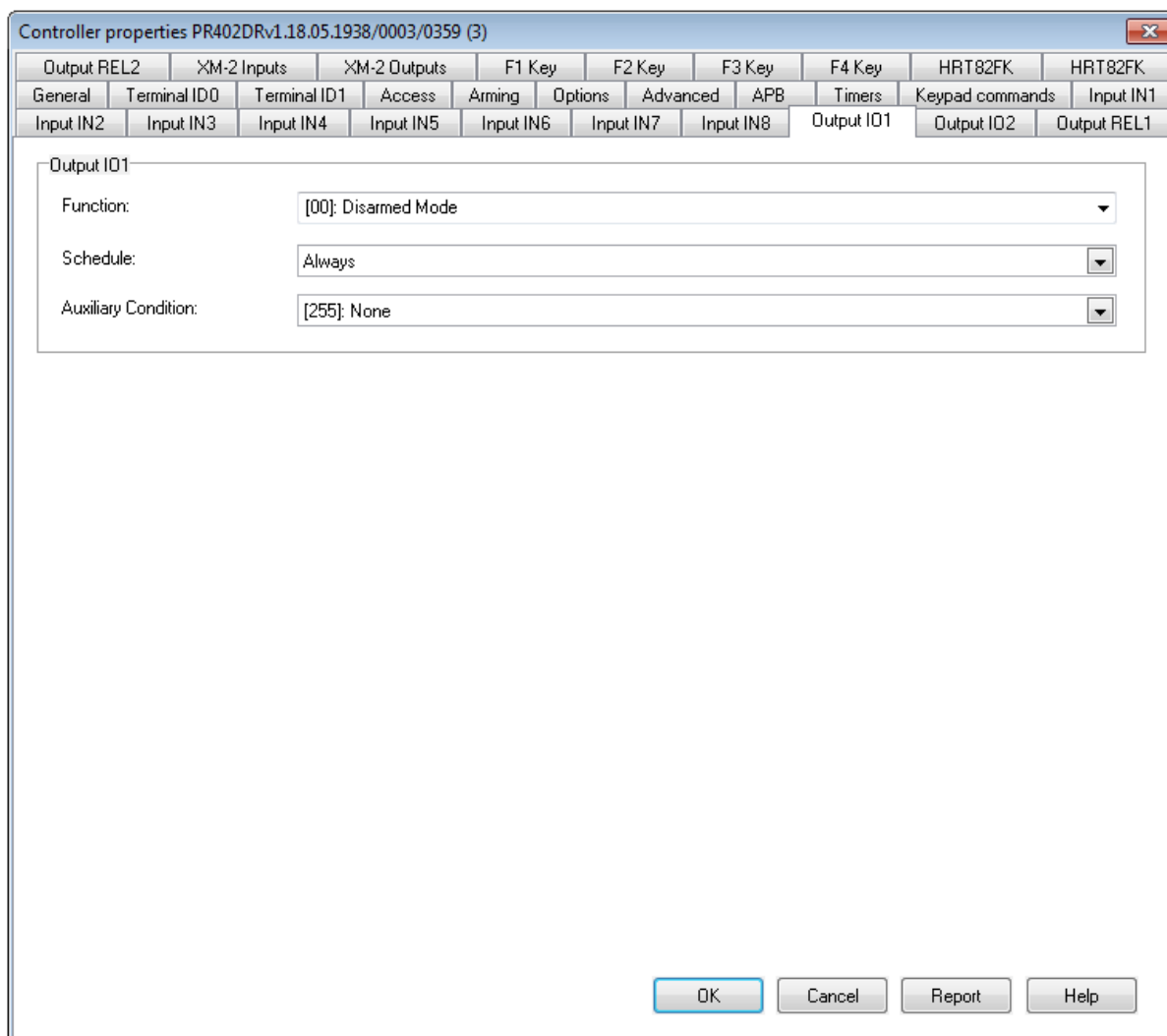


Fig. 22 IO1 Output tab

3.13 Output REL1...REL2 tabs

Depending on the number of relays available in particular controller (see Table 1), respectively 1 or 2 tabs are displayed in controller properties. In the tab **REL1 Output** or **REL2 Output**, the administrator can assign function (see 2.14 Outputs) to particular relay output line as well as Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the relay output line can be used. In case of Always Schedule, the relay output line can be used all the time. The Schedule does not signify the time when the relay output is activated but only the time when the line can be activated. Default function for relay output REL 1 is **[99]: Door lock** and it is used for door opening.

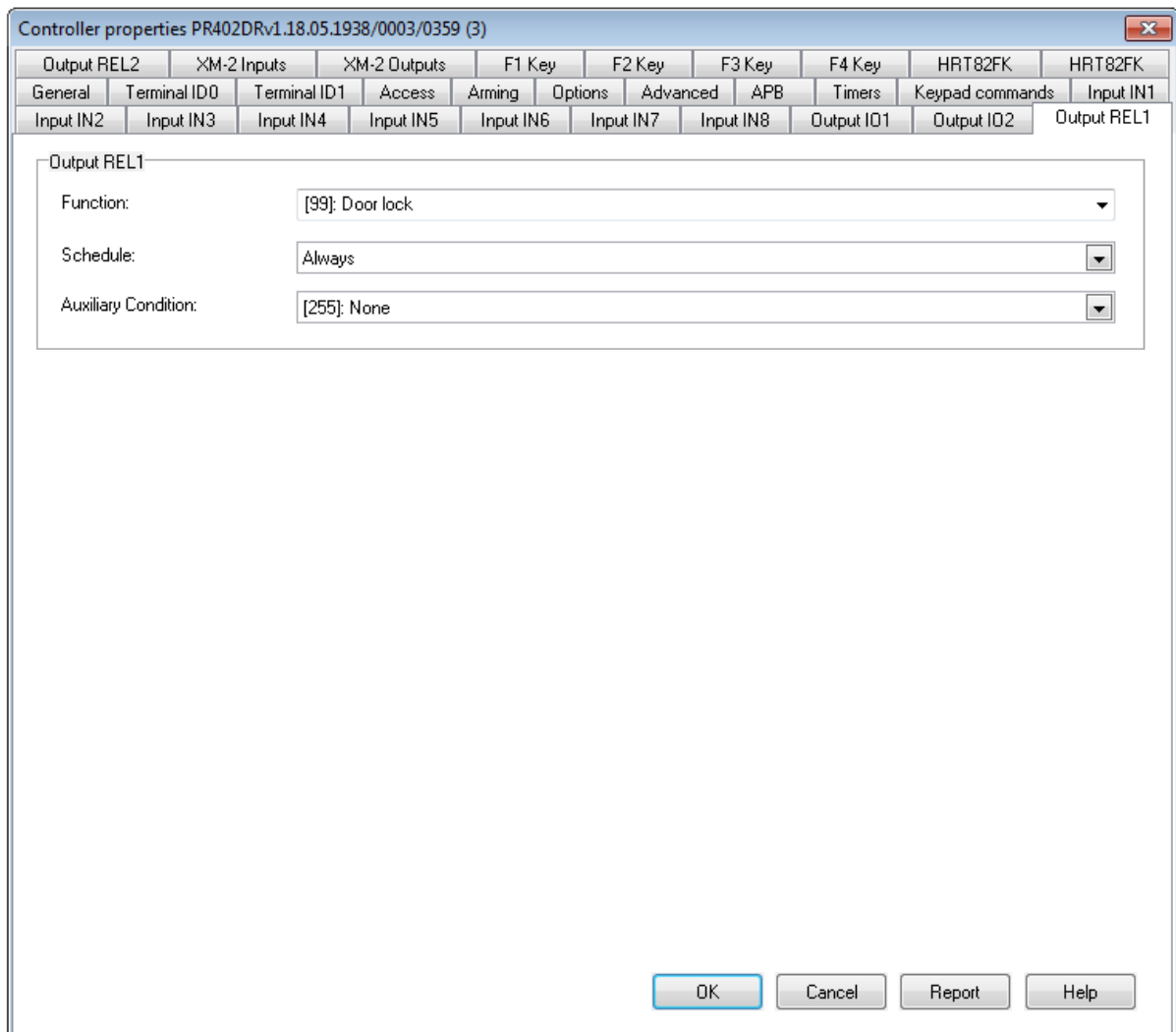


Fig. 23 REL1 Output tab

3.14 XM-2 Inputs tab

The XM-2 expander can be connected to PRxx2 series controller (see 2.2.4 XM-2 I/O expander) in order to increase the number of available inputs by two. The XM-2 expander must be connected to the controller by means of RACS CLK/DTA bus (see 2.2.3 RACS CLK/DTA) and the option **Enable XM-2** in the **Options** tab must be selected. Inputs at XM-2 expander are configured in the same way as inputs of controller which are available in **Input IN1...IN8** tabs (see 3.11 Input IN1...IN8)

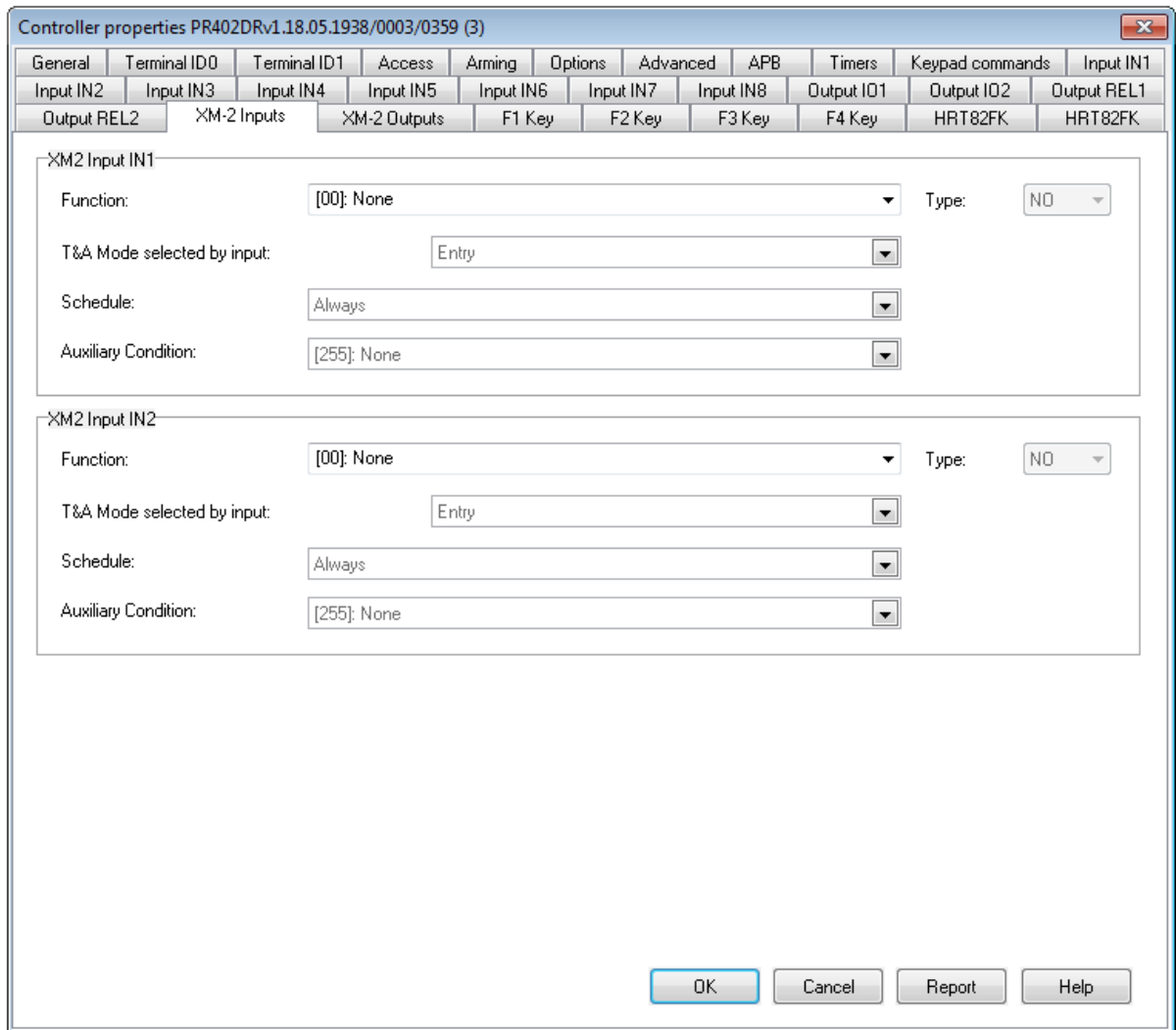


Fig. 24 XM-2 Inputs tab

3.15 XM-2 Outputs tab

The XM-2 expander can be connected to PRxx2 series controller (see 2.2.4 XM-2 I/O expander) in order to increase the number of available relay outputs by two. The XM-2 expander must be connected to the controller by means of RACS CLK/DTA bus (see 2.2.3 RACS CLK/DTA) and the option **Enable XM-2** in the **Options** tab must be selected. Relay outputs at XM-2 expander are configured in the same way as relay outputs of controller which are available in **REL1 ...REL2 Outputs** tabs (see 3.13 Output REL1...REL2 tabs)

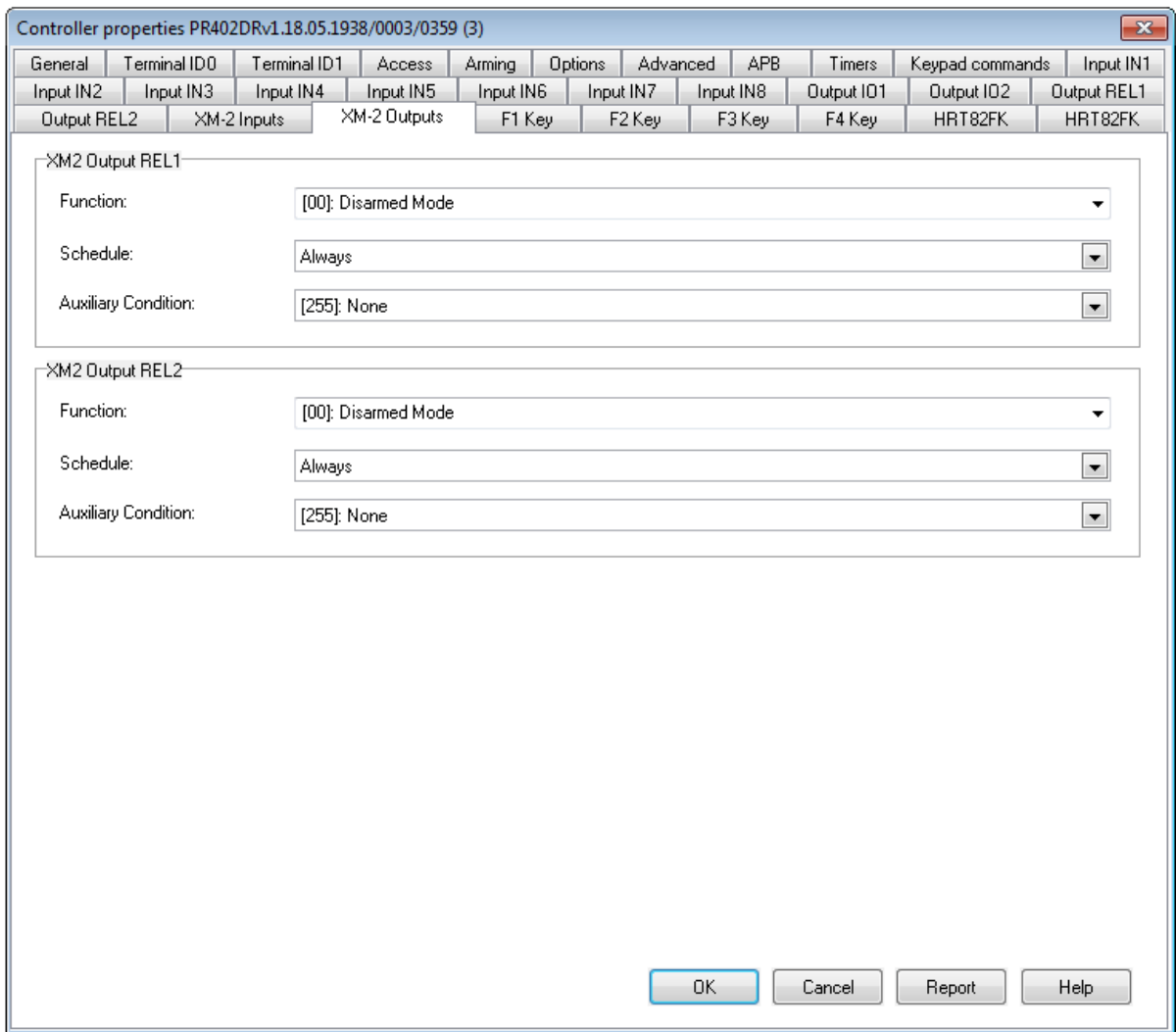


Fig. 25 XM-2 Outputs tab

3.16 F1...F4 keys tabs

Up to four function key tabs are displayed for controller. Physically, the keypad with 4 function keys is available only in PR602LCD type controllers, but external readers with two function keys (PRT12LT) can be connected to all Roger controllers. In **F1...F4 key** tabs, the administrator can configure function keys at Terminal ID0 and ID1 (see 1.2 Design and architecture) selecting the function (see 2.15 Function keys) and assigning Schedule as well as Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the function key can be used. In case of Always Schedule, the key can be used all the time. In general, the Schedule does not signify the time when the function key is activated but only the time when the key can be activated. In case of T&A functions (see 2.19.2 Time&Attendance based on RCP Master software) default T&A Mode can also be assigned to the function key.

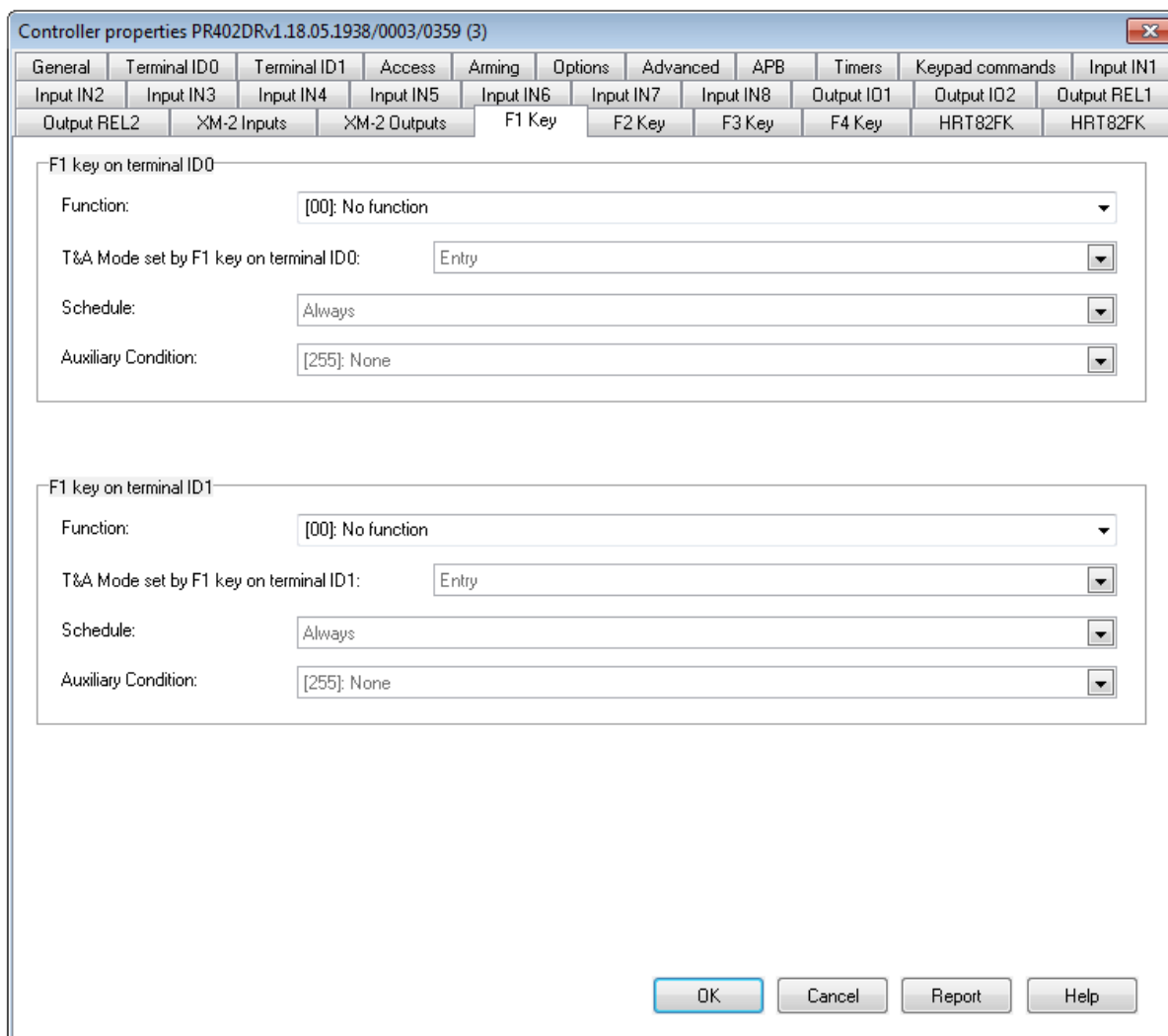


Fig. 26 F1 key tab

3.17 HRT82FK tabs

The HRT82FK function key panel can be connected to PRxx2 series controller (see 2.2.7 HRT82FK function key panel) in order to increase the number of available function keys by four. Each key can be assigned with two different functions (primary and secondary) which are activated respectively by short and long pressing. The HRT82FK panel must be connected to the controller by means of RACS CLK/DTA bus (see 2.2.3 RACS CLK/DTA).

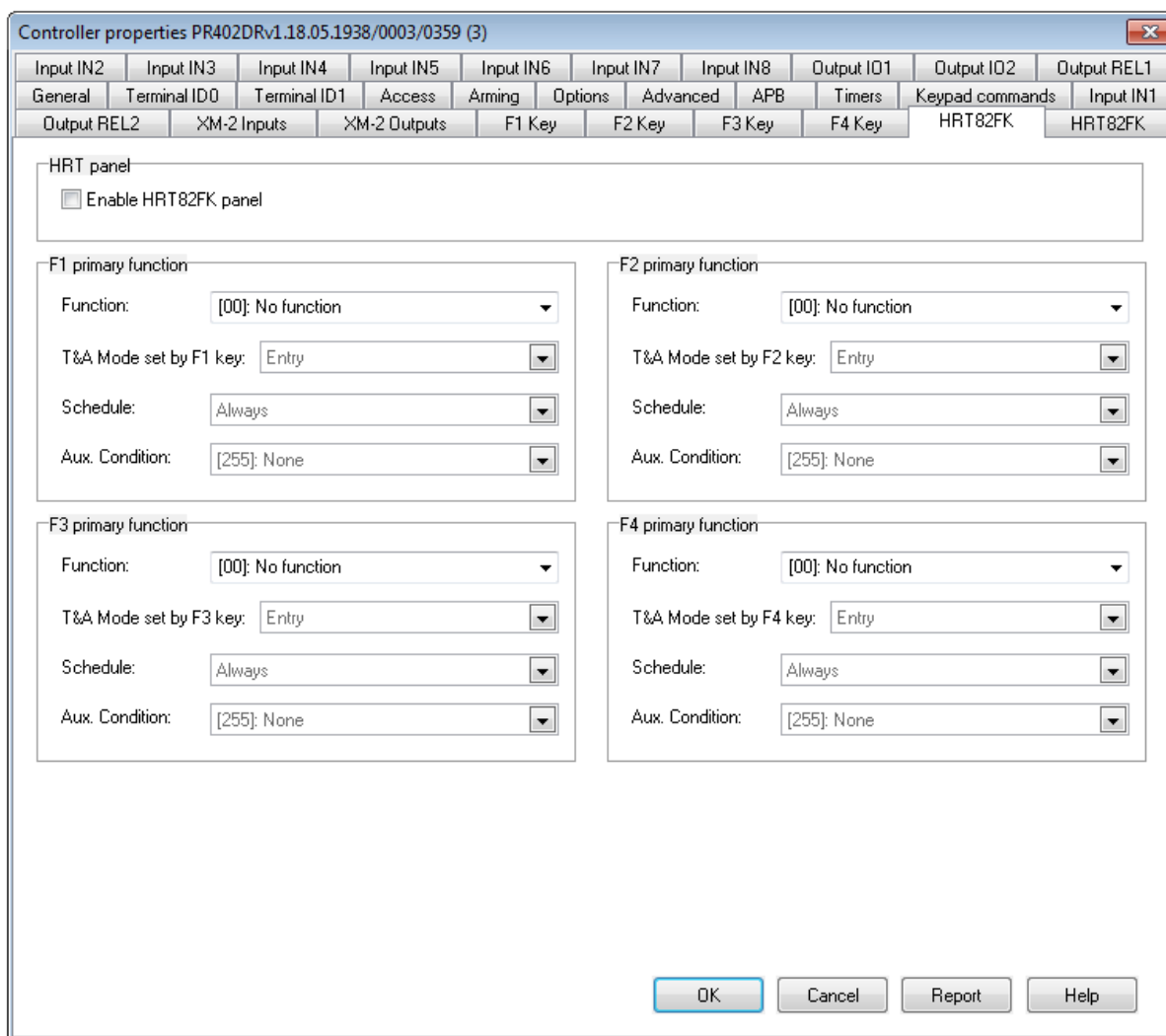


Fig. 27 HRT82FK tab

Area: HRT panel

Option: Enable HRT82FK panel - when the option is selected then operation of the controller with HRT82FK panel is enabled and both primary and secondary functions can be assigned to the panel buttons. More information on HRT82FK panel is provided in 2.2.7 HRT82FK function key panel and in HRT82FK Installation Guide which is available at www.roger.pl

Area: F1 primary function

There are four primary functions areas, each corresponding to respective function key. For each button the administrator can assign primary function (see 2.15 Function keys) which is activated by short pressing of the button as well as Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the function key can be used. In case of Always Schedule, the key can be used all the time. In general, the Schedule does not signify the time when the function key is activated but only the time when the key can be activated. In case of T&A functions (see 2.19.2 Time&Attendance based on RCP Master software) default T&A Mode can also be assigned to the function key.

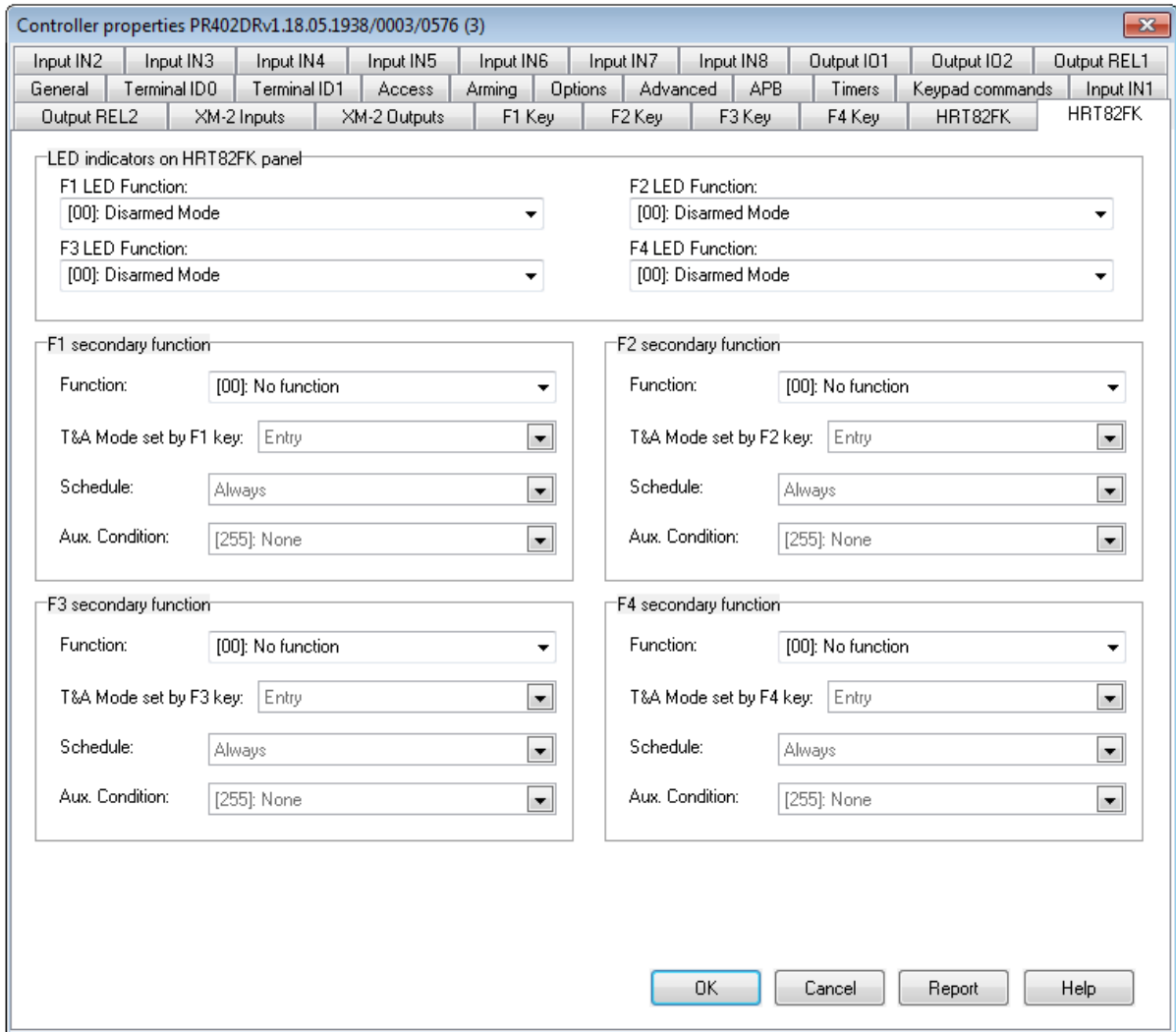


Fig. 28 HRT82FK tab

Area: LED indicators on HRT82FK panel

Each LED indicator can be assigned with function (see 2.14 Outputs). In practical applications, indicator is assigned the function associated with the key function in order to signal that the key was used and adequate function or state was activated.

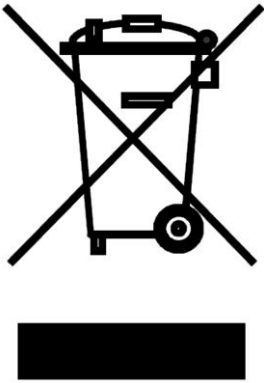
Example:

If the function [70]: Toggle LIGHT is assigned to F1 key and the function [64]: LIGHT is assigned to associated LED indicator then each activation of LIGHT System Flag shall be confirmed by switching F1 LED indicator on.

Area: F1 secondary function

There are four secondary functions areas, each corresponding to respective function key. For each button the administrator can assign secondary function (see 2.15 Function keys) which is activated by long (default 3 sec.) pressing of the button as well as Schedule and Auxiliary Condition (see 2.16 Schedules and Auxiliary Conditions). Two predefined Schedules i.e. Always and Never are already available and the administrator can also specify own Schedule by means of the option **Schedules** in the main window of PR Master software. The period defined by means of parameters From... and To... signifies the time, when the function key can be used. In case of Always Schedule, the key can be used all the time. In general, the Schedule does not signify the time when the function key is activated but only the time when the key can be activated. In case of T&A functions (see 2.19.2

Time&Attendance based on RCP Master software) default T&A Mode can also be assigned to the function key.

	<p>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.</p>
--	---

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