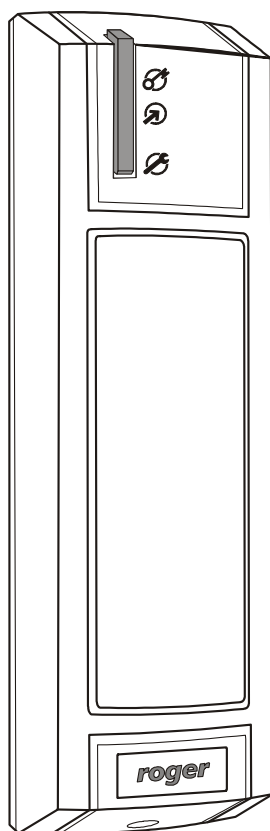


Installation and Programming Guide



PR311-BK
Outdoor Access Controller

Firmware v104.00

roger

1. Table of Contents

1. Table of Contents	2
2. Glossary and Terms	3
3. General	6
3.1. Designed Function	6
3.2. Features.....	6
3.3. Operation in the Integrated Access System.....	7
3.4. Stand-alone Operation	7
4. Functional Description	8
4.1. Users	8
4.2. Managing of Users	9
4.3. Access Groups	9
4.4. User Identification	9
4.5. Armed and Disarmed Modes	10
4.6. Arming and Disarming of the Controller (Rearming).....	10
4.7. Unlocking the Door	11
4.8. Door Modes	12
4.8.1. Normal Mode.....	12
4.8.2. Unlocked Mode	13
4.8.3. Conditional Unlocked Mode.....	13
4.8.4. Locked Mode	13
4.9. Option: Auto-relock	13
4.10. Option: Access When Controller Armed (AWA Privilege)	13
4.11. Facility Code	13
4.12. Option: Controller Timed Lock-out	14
4.13. System Flags	14
4.14. Operation with XM-2 I/O Extension Module.....	15
4.15. Operation with the External PRT Series Reader	15
4.16. Alarms	15
4.17. Function Keys	16
4.18. Inputs.....	16
4.19. Outputs.....	18
5. Programming	20
5.1. Programming Cards	20
5.2. Memory Reset - Programming MASTER Identifier.....	20
5.3. User Programming.....	21
5.3.1. Programming Cards.....	21
5.3.2. User Programming Examples	22
5.4. Installer Programming.....	22
6. Installation and Setup Guidelines	24
7. Acoustic and Optical Signals	25
8. Appendix	26

2. Glossary and Terms

Identifier

The method or meaning used for identifies a person. It can be a proximity card, a PIN code, a finger template etc. In some cases *Identifier* may consist of two or more items required for a single identification procedure. For example when the option *Card and PIN* is active then *Identifier = Card+PIN*.

Stand-alone Mode

This situation when device operate without physical connection to any Host device or when such connection exists but it is used only for uploading/downloading of data to or from a host unit.

Integrated Access Control System (IACS)

The access control system which consists of one or more access controllers connected to a communication medium and managed from a Host device. The Host device plays a special role in such systems while adding some functionality to them. Without the Host device the functionality of the entire access system deteriorates partly or completely.

Networked Access System

It's the same meaning as *Integrated Access System*.

Roger Access Control System (RACS)

The access control system which consists of PR series access controllers developed and manufactured by Roger.

Host Device

The electronic equipment used to expand the access system functionality. In the RACS system the Host unit can be the CPR32-SE host controller or the PC with special software used for *Online* control of the access system.

Door Mode

The method used for control door release device. The PR311-BK offers: *Normal, Unlocked, Locked and Conditional Unlocked* door modes.

Identification Mode

The method used for identification of users. Although the main method of identification which utilizes the PR311-BK is a proximity card but theoretically other identification modes can be used on this controller: *Card and PIN, Card or PIN, Card Only and PIN Only* identification modes. The use of PIN identification has practical sense if the controller operates with additional reader which is equipped with keypad.

Facility Code

The common part of the card code (8 bits) which characterizes all cards used in the particular access system. Usually, the *Facility Code* is factory programmed to a card on a special customer request. Some types of proximity cards may have the *Facility Code* programmed by the end user.

Door Release or Door Lock

The electric device which unlocks a door. Typically it can be a door strike or a magnetic lock.

Communication Bus

The physical medium used for exchanging of data between various devices connected to it. The PR311-BK is equipped with two types of communication buses: the RS485 interface and the *Clock & Data*.

System Flags

Flags are logical registers which exists in controller's memory. Each flag represents a status of relevant situation which may occur in the controller (e.g. TROUBLE flags, DURESS flags).

Timer

The function which automatically clears condition of some item (physical or virtual) after predefined time. The *Timer* function can refer to various elements of controller logic e.g. to outputs, time delays etc.

Latch Mode

Latch Mode refers to situation when some element (e.g. output) changes its condition for unlimited time – till the moment when some other event will restore previous condition of given element.

RS485

The electrical interface which is used by the controller for communication with PC and/or with CPR host controller. Usually, the PC's are not equipped with RS485 communication port, so the special adaptor (UT-2 interface) is required. The RS485 enables communication for up to 1200 meters.

Clock & Data Interface

The electrical interface which is used by the controller for communication with various equipments connected to it. The PR311-BK can operate with second PRT series reader and/or XM-2 extension module. Both device can be connected to the same *Clock* and *Data* lines and must have individual addresses (ID numbers).

XM-2 I/O Extension Module

The remote I/O extension module for RACS system which can be connected to PR311-BK controller via *Clock & Data* lines. The XM-2 provides two NO/NC inputs and two relay type outputs.

PRT Series Readers

The PRT reader's family developed and manufactured by the Roger. Each member of PRT series readers can be connected to PR311-BK access controller via *Clock & Data* interface. Typically the additional remote reader is used for two-way door control.

Identification Point

The electronic equipment (usually reader) used for user identification.

Access Group

The electronic equipment (usually reader) used for user identification.

Programming Cards

The proximity card or tag which has been assigned some programming functions.

Memory Reset

The procedure which clears contents of device's memory and restores default (factory) values.

Restart

The scenario when device goes through initialization procedure, the same as during power up of a unit.

3. General

3.1. Designed Function

The PR311-BK access controller has been designed for use in electronic access control installations as an outdoor access control device. The PR311-BK is equipped with built-in proximity reader, three NO/NC type inputs and three outputs (two transistor type outputs and one relay output). The PR311-BK can be configured for operation with external XM-2 I/O extension module and external PRT series reader. The use of XM-2 adds two NO/NC type inputs and two relay outputs to a controller. As a result installer may have up to five programmed inputs and up to five programmed outputs. The system setup utilizing an XM-2 module provides higher level of security for door access control system by separating its logical element (the controller unit) from the activating element controlling the door lock (i.e. the door lock relay). The connection of (with) additional PRT reader enables two-way door control (entry/exit). The PR311-BK unit can work autonomously (*Stand-alone Mode*) or as a part of the *Integrated (Networked) Access Control System*. When controller operates as a stand-alone unit then independently (i.e. autonomously) controls the supervised door access point. In this mode controller doesn't provides event recording no time schedules (time tables).

Important note !

The PR311-BK requires connection to a PC for initial setup. Once configured from PC (*Installer Programming*) unit can continue operation without connection to a PC. The programming of users (*User Programming*) can be carried out remotely from the PC or locally through *Programming Cards*.

Note: Programming of the controller requires RACS v4.2 (or higher) managing software.

3.2. Features

- Built-in EM 125kHz card reader
- Keypad with back light
- 1.000 users with Card and/or PIN
- User indexing (ID indexed user records)
- System settings stored in nonvolatile memory
- Three programmable inputs
- Three programmable outputs (one relay output and two transistor outputs)
- Two-way door control (requires additional PRT reader to form a pair)
- Integration with the alarm system through I/Os
- XM-2 I/O module support (adds two inputs and two relay outputs to the controller)
- User management from a PC or locally through *Programming Cards*
- ABS casing with TAMPER

- CE mark

Additional features when operating in the *Integrated Access Control System*:

- 256 *Access Groups*
- 32 time schedules for access level control
- Time schedules for *Identification Mode* and *Door Mode*
- 128 time periods per schedule
- Events recorded by a Host device (CPR32-SE Network controller or PC with PR Master program in *Online* mode)

3.3. Operation in the Integrated Access System

When controller is a part of the *Integrated Access Control System* which is managed by the Host device, then the PR311-BK extends its functionality significantly and offers the following additional features:

- definition of *Access Groups*
- time schedules which controls access authorization
- time schedule which controls *Identification Mode*
- time schedule which controls *Door Mode*
- recording of the events

Users can be divided into 256 *Access Groups*. Each group may have different access authorization controlled by a time schedule. The PR311-BK allows up to 32 time schedules which are used to control access and two special schedules – one of them controls the *Identification Mode* while the other one controls the *Door Mode*. Events which occur in the access system are stored on the Host device. If the communication with the Host is broken the PR311-BK continues operation with time schedule settings which existed when the communication disappeared. After the communication with the Host resumes all clocks related settings (e.g. time schedules) and events recording are restored.

3.4. Stand-alone Operation

In this case the PR311-BK access controller autonomously supervises door passage and doesn't require any connection to the Host device. In this mode connection to a PC may eventually exist but it is used only for re-programming of a unit. In *Stand-alone Mode* all users registered in the controller belong to the same group of users (this special, predefined group is called: "No Group") and have permanent access authorization regardless of a time. Neither the *Identification Mode* nor *Door Mode* can be controlled by time schedules, events are not registered.

The following features are not available in *Stand-alone Mode*:

- Users can not be divided into a separate groups of users
- Time schedules can not control access authorization
- *Door Mode* can not be controlled by the time schedules

- *Identification Mode* can not be controlled by the time schedules
- Events can not be recorded

Note: All this features listed above are available when the controller operates in *Integrated Access Control System*.

4. Functional Description

4.1. Users

Note: Despite of not having a keypad, the PR311-BK allows to assign PIN code for every user registered in the controller. Programming of a PIN code for a user(s) in PR311-BK can be carried out from PC computer only and have practical sense if:

- the PR311-BK operates with an additional reader equipped with keypad (e.g. PRT12)**
 - the PR311-BK operates in an access system together with other controllers which are equipped with keypads, in this case the same list of users (with cards and PIN's) is used for each controller in a system regardless of a fact that some of them have not a keypad.**
-

The PR311-BK can register up to 1.000 users. Every user has his ID (identification) number from 001 to 999 and may have card and/or PIN. The PIN codes may have from 3 to 6 digits and whenever entered PIN code must be followed by [#] mark which is used to mark the end of a code. The PR311-BK controller precludes assignment of the same cards or PIN's for two different users. Users can be identified by cards, PIN's or both methods simultaneously. The method of user identification depends on the actual *Identification Mode* valid on the controller. The PR311-BK controller supports four types (classes) of the users: MASTER, TOGGLE, TOGGLE LTD and NORMAL. Each of the class has different authorization for programming, unlocking and rearming of a controller.

Table 1. User types (User classes).

User Types	Authorization
MASTER	This user is allowed to unlocking the door and to switching the unit between <i>Armed</i> and <i>Disarmed</i> modes. The MASTER user is defined during <i>Memory Reset</i> and is mainly dedicated for the initial testing of a unit.
TOGGLE	This user is allowed to unlocking the door and to switching the unit between <i>Armed</i> and <i>Disarmed</i> modes.
TOGGLE LTD	This user is only allowed to switching the unit between <i>Armed</i> and <i>Disarmed</i> modes.
NORMAL	This user is only allowed to unlocking the door.

Note: In the PR Master program which is used for programming of a PR311-BK (and other PR series access controllers) the TOGGLE and TOGGLE LTD class of users are called respectively: SWITCHER and SWITCHER LTD.

4.2. Managing of Users

Generally, management of the users in PR311- BK can be provided locally by the *Programming Cards* or remotely from the PC. It is strongly recommended to use only one of the two mentioned methods. The simultaneous use of local and remote method of programming may create confusions. For example, users added to controller manually will not exist in the PC database, as a result every programming from PC it will clear manually added users.

Note: The manual programming of users doesn't allow to specify the ID number of a newly enrolled user. As a result users added to a controller can not be removed later from the controller by indication of theirs ID numbers.

4.3. Access Groups

When the PR311-BK controller is a part of *Integrated Access Control System* supervised by the Host device, users registered in controller can be divided into 256 *Access Groups*. The users which belong to the same *Access Group* have the same access authorization within system. The access level of each group can be controlled by the time schedules. The PR311-BK allows to be defined up to 32 different time schedules for a unit. The time schedules consists of one or more time periods within which users will have access to specified *Access Zone*. The access rights are defined separately for each *Access Groups* and individually for each *Access Zone*.

Note: There is no practical sense to define *Access Zones* in the small installations. Instead of this it should be assume that in the small system every *Access Zone* is equal to a single door.

Note: Users registered in PR311-BK can be divided into the *Access Groups* only when controller operates in the *Integrated Access Control System*.

4.4. User Identification

The PR311-BK recognizes the users by theirs identifiers. In PR311-BK each user programmed in the controller may have card and eventually PIN. The method which controller uses for user's identification depends on the actual *Identification Mode*. The PR311-BK enables following *Identification Modes*:

- *Card Only*, controller accepts only cards
- *PIN Only*, controller accepts only PIN's
- *Card or PIN*, controller requires card or PIN, only one of them is necessary for the successful identification

- *Card and PIN*, controller requires card and PIN, both of them are necessary for the successful identification.

Some of the control commands requiring double use of user identifier (e.g. rearming of a reader by the TOGGLE).

Note: The actual *Identification Mode* specifies user identification method on both: the controller and the additional reader connected to the controller. It is not possible to define *Identification Mode* individually for a controller and for additional reader.

4.5. Armed and Disarmed Modes

The PR311-BK has two working modes: *Armed* and *Disarmed*. The actual working operating mode of the controller is indicated on the dual color LED STATUS, which lights in red for *Armed* and green for *Disarmed*. Generally, the *Armed* and *Disarmed* modes are dedicated to integration of the controller with the alarm system which protects the same room or area supervised by the access controller, nevertheless they can be used for any other control purpose which requires an On/Off control method. The integration with the alarm system (or another device/system) requires one output line to be configured to the function no. 0 (**Disarmed mode**) and optional input line configured to the function no. 13 (**Disable arming**). The controller's output line (function no. 0) indicates current operating mode of the controller, whereas the input line (function no. 13) verifies if the controlled system (or device) can be *Armed* (or set ON) or not. When the installer doesn't define any controller's input to the function no. 13, the controller assumes that the controlled system or device is always ready for arming and switches to *Armed* mode unconditionally.

Note: Although the *Armed* and *Disarmed* modes of the controller were designed for integration with the alarm system they can be used for any other purpose which requires an on/off method of control (light control, heating control etc).

Note: Either upon powering on or Memory Reset reader automatically enters the *Armed* mode. After exit from programming mode reader returns to arming mode (either *Armed* or *Disarmed*) it was before entry to the programming.

4.6. Arming and Disarming of the Controller (Rearming)

The action changing the controller from *Armed* to *Disarmed* and back (i.e. reverse direction) is referred to hereinafter as "**rearming**". The term "arming" should be understood here as the action effecting a switch into the *Armed* mode, whereas the term "disarming" a switch into the *Disarmed* mode.

Controller PR311-BK can be rearmed in few methods listed below:

- by the input line configured to function no. 3: **Disarm steady switch**
- by the input line configured to function no. 61: **Arming/Disarming momentary switch**

- by the input line configured to function no. 78: **Disarmed mode momentary switch**
- by the input line configured to function no. 79: **Armed mode momentary switch**
- by the MASTER user (by using of the MASTER identifier)
- by the TOGGLE user (by using of the TOGGLE identifier)
- by the TOGGLE LTD user (by using of the TOGGLE LTD identifier)
- by an interactive command from PC
- by the *Armed/Disarmed Schedule*

Note: Except first mentioned method, all other methods can be used simultaneously to *Arm/Disarm* the controller – as a result the controller will employ the arming condition which was indicated by the last event (command). When arming mode of a controller is controlled by input: **Arming/Disarming steady switch**, all other methods of rearming are inoperative.

Reader rearming command can be issued by MASTER, TOGGLE or TOGGLE LTD users. To rearm the reader a MASTER and TOGGLE (with or without *AWA Privilege*) users are required to enter their identifier twice, whereas a TOGGLE LTD user must enter his identifier once only.

Note: The manual rearming of the controller through TOGGLE or MASTER users can be carried out either from the controller PR311-BK or from the external reader.

Example1. Rearming of the controller by using a TOGGLE identifier (when the *Card Only* mode is active).

- Read your TOGGLE card, with the first use of the card controller will release a lock and start flashing LED SYSTEM
- When the LED SYSTEM is flashing, read your TOGGLE user card once again
- after the last step controller will changed its arming mode (watch for the LED STATUS which will changed their color)

4.7. Unlocking the Door

In order to unlock the door user is required to use his identifier once. Whenever this happens the reader activates LED SYSTEM (orange) for a moment and generates a short confirmation beep. After successful identification reader unlocks the door for the predefined time specified by: **Door unlock time**. The lock activation is indicated on LED OPEN (green), which remains ON for as long as the door lock is released. When the option: **Auto-relock**, is active the door lock is released till the moment when door become open.

Note: The LED OPEN is activated for the entire time when door lock is released.

When access to the supervised room is denied the reader may generate either the one long beep or two short beeps. The one long acoustic signal indicates that presented identifier is not registered in the controller (identifier is unknown)

whereas two short beeps indicates that presented identifier exists in controller's memory but actually has no authorization for the entry.

The access to a room can be rejected in the following situations:

- When the entered identifier is not valid (unknown)
- When the entered identifier belongs to a TOGGLE LTD class of users
- When controller operates in *Armed* mode and the user which entered identifier has not an *AWA Privilege* assigned
- When the identification doesn't comply with actual identification mode valid on the controller (e.g. user presented only card when *Card and PIN* mode was set on the unit)
- When the input line was configured to the function no. 11: **Access disabled** is triggered
- When access is disabled by the relevant time schedule (this rule refers to scenario when controller operates in *Integrated Access Control System*)

4.8. Door Modes

The *Door Mode* determines method which PR311-BK use to control a door lock.

There are four *Door Modes* available in the controller:

- *Normal*
- *Unlocked*
- *Conditional Unlocked*
- *Locked*

A *Door Mode* can be controlled in a few listed below methods:

- By use of *Programming Cards*
- From the input line
- From the interactive commands send from the PC
- Automatically, according to the time schedule (*Door Mode Schedule*)

Note: The *Door Mode* can be controlled by the time schedule only when the PR311-BK operates in *Integrated Access Control System*.

All methods of *Door Mode* control listed above can be used simultaneously and equally – as a result controller will always employ that *Door Mode* which results from last event (cause or command).

4.8.1. Normal Mode

This is the standard and most commonly used *Door Mode*. In *Normal* door mode controller unlocks the door for limited time (**Door unlocks time**). Each time the access to a door is granted. The *Normal* door mode is automatically set after power up of a unit.

4.8.2. Unlocked Mode

In this mode door are permanently unlocked and every user may open a door without use of any identifier.

4.8.3. Conditional Unlocked Mode

Initially door is locked but with the first use of the authorized identifier controller unlocks the door. Since this moment door will remain unlocked till the moment when new *Door Mode* will be set.

4.8.4. Locked Mode

In this mode door is permanently locked, even when authorized identifier is used the door will be still kept locked and access will be denied.

4.9. Option: Auto-relock

Normally when this option is not set controller activates a door release device and keep it energized by entire predefined time. When this option is set on door release device is triggered till the moment the controller recognized that the door became open but not longer that time defined by parameter: **Door unlock time**.

4.10. Option: Access When Controller Armed (AWA Privilege)

Normally when the controller is *Armed* access to the controlled door is disabled for all types of users except the MASTER. This rule can be changed by an option: **Access when controller Armed (AWA Privilege)**. When this option is set on user may enter the room when the controller operates either in the *Armed* or in the *Disarmed* mode. The AWA Privilege can be set individually for each user programmed in the controller. The PR311-BK controller offers separate sets of programming commands, one for the users which are allowed for AWA Privilege and another for the users which are not granted with this privilege.

4.11. Facility Code

The *Facility Code* is a part of the entire card code and can be a number from 000 to 255. When *Facility Code* option is set the controller accepts not only cards which are programmed to its memory but also all other cards which are characterized with the same *Facility Code*. As a result of the *Facility Code* option access can be granted to large number of users which are not programmed into a device. Typically, the *Facility Code* option is used when controller is dedicated for the installation where number of users exceeds one thousand. During configuration process installer can assign an AWA Privilege to the group of *Facility* cards so the every card with *Facility Codes* will be able to open a door even when controller is *Armed* (Default: Option Disabled).

4.12. Option: Controller Timed Lock-out

If the controller recognizes three consecutive attempts of entry of a non-valid identifier it will ignore all attempts to enter any identifier within next three minutes. During this three minutes of penalty time controller will continue its operation with all other functionalities.

Note: Every use of authorized identifier clear counter for this option.

4.13. System Flags

System Flags are the logical registers which exist in controller's memory. Each flag represent a status of relevant situation which may occur on a controller and have a set of cause which may set or clear it. Every *System Flag* has assigned a separate *Timer*. The *Timer* specifies for what time the relevant *System Flag* will remain active after it is set ON. The *Timers* for AUX1 and LIGHT flags can be optionally programmed for unlimited time (*Latch mode*) in this case once the *System Flag* is set it will remain ON till the moment when adequate command or adequate event will clear it. The condition of each *Flag* can be signaled on the output line.

The PR311-BK utilizes the following *System Flags*:

- AUX1
- LIGHT
- TAMPER
- DURESS

Table 2. System Flags in the PR311-BK.

Flag	Latch Mode	Setting methods	Clearing methods
AUX1	YES	<ol style="list-style-type: none"> 1. <i>Programming Card</i> (PC-F12). 2. <i>Programming Card</i> (PC-F14). 3. Input line (Function no. 71). 4. Input line (Function no. 73). 	<ol style="list-style-type: none"> 1. <i>Programming Card</i> (PC-F13). 2. <i>Programming Card</i> (PC-F14). 3. Input line (Function no. 72). 4. Input line (Function no. 73). 5. Controller restart.
LIGHT	YES	<ol style="list-style-type: none"> 1. <i>Programming Card</i> (PC-F15). 2. <i>Programming Card</i> (PC- F17). 3. Input line (Function no. 68). 4. Input line (Function no. 70). 5. [F2] function key. 	<ol style="list-style-type: none"> 1. <i>Programming Card</i> (PC-F16). 2. <i>Programming Card</i> (PC- F17). 3. Input line (Function no. 69). 4. Input line (Function no. 70). 5. [F2] function key. 6. Controller restart.
TAMPER	NO	<ol style="list-style-type: none"> 1. Input line (Function no. 8). 	<ol style="list-style-type: none"> 1. <i>Arm/Disarm</i> of the controller. 2. Controller restart.

TROUBLE	NO	<ol style="list-style-type: none"> 1. Lost of communication with XM-2 module. 2. Input line (Function no. 5). 3. Input line (Function no. 6). 	<ol style="list-style-type: none"> 1. <i>Arm/Disarm</i> of the controller. 2. Controller restart.
DURESS	NO	<ol style="list-style-type: none"> 1. Duress code entered. 	<ol style="list-style-type: none"> 1. <i>Arm/Disarm</i> of the controller. 2. Any valid identifier 3. Controller restart.

4.14. Operation with XM-2 I/O Extension Module

The PR311-BK is capable to operate with an external XM-2 I/O extension module. If employed the XM-2 ads two inputs and two relay outputs to a controller each input and output of the XM-2 can be programmed on the same basis as internal inputs and outputs of a controller. The XM-2 should be connected to controller's CLK and DTA lines and should have address set to ID=5. The maximum distance between a controller and the XM-2 extension module is limited to 150 m.

4.15. Operation with the External PRT Series Reader

The PR311-BK is capable to operate with external PRT series reader. If used the PRT reader enables two-way door control, the PRT reader should be connected to the controller's CLK and DTA lines and must have an address set to ID=0. The maximum distance between controller and the PRT reader is limited to 150 m.

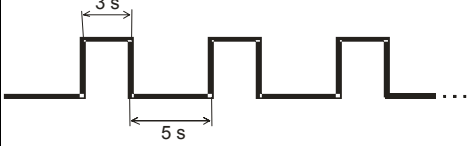
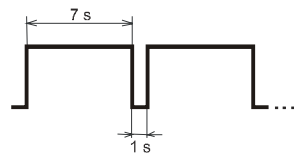
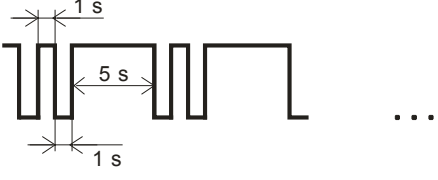
4.16. Alarms

The PR311-BK controller has been designed to detect and indicate the following alarm types:

- *Forced Door*
- *Prealarm*
- *Door Ajar*

Forced Entry and *Door Ajar* alarms will occur only if the reader operates with a **Door contact**. The alarm signaling is carried out over the dedicated output line. Each alarm can be indicated on the separate output or alternatively the one output line can be configured to signal two or even three alarms simultaneously. For each type of alarm the PR311-BK uses different signal modulation of an output, which depends on the alarm type (see Table 3). Alarm duration is always ~3 minutes, regardless of the alarm type. Each alarm can be stopped manually within 3 minutes from its start by using any valid identifier. Additionally, a *Door Ajar* alarm is stopped as soon as the door became closed. If more than one alarm is triggered, the output indicates the alarm with the highest priority.

Table 3. Alarm signaling methods.

Alarm type	Priority	Signaling method	Alarm situation (event)
<i>Forced Door</i>	High	By cycles with the following sequence: Active – 3 sec., Pause – 5 sec. 	Door opened without use of the valid identifier.
<i>Prealarm</i>	Medium	By cycles with the following sequence: Active - 7 sec., Pause - 1 sec. 	Three consecutive attempts to enter with an unregistered (unknown) identifier.
<i>Door Ajar</i>	Low	By cycles with the following sequence: Active - 1 sec., Pause - 1 sec., Active - 1 sec., Pause - 5 sec. 	After access has been granted and the door left open for the time exceeding the maximum door open time.

4.17. Function Keys

Although the PR311-BK is not equipped with any function key, it may serve [F1] and [F2] function keys, if they are available on remote reader (e.g. PRT12) connected to the controller. Pressing [F1] on the remote reader triggers **Door bell** output (if programmed), pressing [F2] toggles on/off the LIGHT flag along with LIGHT output (when programmed).

4.18. Inputs

The PR311-BK provides five logical inputs (IN1, IN2, IN3, IN4, IN5). Three of them are physically located on the PR311-BK itself and two on the remote XM-2 I/O extension module. Each input can be configured as NO or NC type and may have assigned function from the list below:

Table 4. Input line functions.

Function	Number	Description
Input off	0	Selecting this function will disable decoding of this input. This function can be used for temporary input deactivation without disconnecting it physically from the triggering source.

Door contact	1	Input is dedicated for a contact used to indicate that the corresponding door is open.
Exit button - momentary switch	2	Input is dedicated for the operation with a button which will be used to open the corresponding door without using any identifier. Activation of this input will activate the door lock for the same time period as defined by Door unlock time . This function is usually used to enable connection of a <i>Request To Exit</i> (REX) button.
Arm/Disarm steady switch	3	When input is triggered controller switches unconditionally to <i>Disarmed</i> mode. Note: Only one input on the controller can be configured to this function. When this function is selected any other methods of <i>Arming/Disarming</i> are disabled.
AUX	4	Whenever this input goes on or off the adequate event is registered in history (when controller operates in <i>Integrated Access Control System</i>)– no other effects.
AC lost	5	Input is dedicated for connection to an output line or a contact which is used to indicate a loss of AC power supply. Each time this input is triggered it sets the TROUBLE flag on.
Low battery	6	Input is dedicated for connection to an output line or a contact which is used to indicate the low level of reserve battery. Each time this input is triggered it sets the TROUBLE flag on.
Bell button	7	Each time this input is triggered controller activates the Door bell output (function no. 15). Input is dedicated for connection to a button used to indicate that somebody wants to enter the premises.
Tamper	8	Tamper loop input. Each time this input is triggered it activates the TAMPER flag timer which can further activate (if programmed) the Tamper output (Function no. 65).
Access disabled	11	When triggered disables access to a room or area.
Arming disabled	13	When input is triggered controller can't be armed. Note: This input does not affect arming when it is carried out by input Disarm steady switch (function no. 3).
Exit button steady switch	14	Triggering of this input unlocks the door. Door remains unlocked as long as input is triggered.
Arm/Disarm momentary switch	61	Each time this input is triggered the controller reverses its arming condition (goes from Armed to Disarmed or vice versa).
Normal door mode	64	Triggering of this input sets <i>Normal</i> door mode.
Unlocked door mode	65	Triggering of this input sets <i>Unlocked</i> door mode.
Conditional Unlocked door mode	66	Triggering of this input sets <i>Conditional Unlocked</i> door mode.
Locked door mode	67	Triggering of this input sets <i>Locked</i> door mode.
LIGHT flag on	68	Triggering of this input sets LIGHT flag on.

LIGHT flag off	69	Triggering of this input sets LIGHT flag off.
Toggle LIGHT flag on/off	70	Triggering of this input toggles LIGHT flag on/off.
AUX1 flag on	71	Triggering of this input sets AUX1 flag on.
Set AUX1 flag off	72	Triggering of this input sets AUX1 flag off.
Toggle AUX1 flag on/off	73	Triggering of this input toggles AUX1 flag on/off.
Disarmed mode	78	Triggering of this input switches controller to <i>Disarmed</i> mode.
Armed mode	79	Triggering of this input switches controller to <i>Armed</i> mode.
Card or PIN mode	80	Triggering of this input sets <i>Card or PIN</i> identification mode for terminal ID1.
Card only mode	81	Triggering of this input sets <i>Card only</i> identification mode for terminal ID1.
PIN only mode	82	Triggering of this input sets <i>PIN only</i> identification mode for terminal ID1.
Card and PIN mode	83	Triggering of this input sets <i>Card and PIN</i> identification mode for terminal ID1.

Note: It is not allowed to program two or more inputs to the same function.

4.19. Outputs

The PR311-BK provides five logical outputs. Three of them (called OUT1, OUT2 and OUT3) are located on the controller's electronic module while two others (OUT4, OUT5) are located on the optional XM-2 extension module. The OUT1 is a relay output with one NO/NC/COM contact. The OUT2 and OUT3 are transistor types capable to sink up to 1A DC current. Regardless of the output type and its location (internal on the controller or external on the extension module) they can be configured to one from the following list of functions:

Table 5. Output lines functions.

Function	Number	Description
Disarmed mode	0	Whenever controller switches to <i>Disarmed</i> mode this output goes on and remains on as far as controller is disarmed.
Prealarm	1	The output is dedicated to indicate one or more alarm situation which occurred on the controller. Depending on programmed function (01-07) the output can signal one or more type of alarms. If more then one alarm exists, the output signals alarm with highest priority. Each alarm is signaled through different modulation of an output line.
Door Ajar	2	
Prealarm + Door Ajar	3	
Forced Entry	4	
Prealarm + Forced Entry	5	

Door Ajar + Forced Entry	6	
Prealarm + Door Ajar + Forced Entry	7	
Access granted	9	Whenever controller grants access, this output goes on and remains in this state till the moment when door contact indicates that the door became closed or the Door unlock time has passed by.
Access denied	11	Each time the access is denied, this output goes on for app. two seconds.
Identification on reader ID0	14	Each time a successful identification occurs on the reader ID0, this output turns on and remains in this state till the nearest user identification on terminal ID1. Typically, this function is used to control a direction of a rotary gate.
Door bell	15	Whenever Door bell input is triggered or Door bell key is pressed this output goes on for approx. 3 seconds.
Normal door mode	18	Output goes on and remains in this condition as long as the controller operates in <i>Normal</i> door mode.
Unlocked door mode	19	Output goes on and remains in this condition as long as the controller operates in <i>Unlocked</i> door mode.
Conditional Unlocked door mode	20	Output goes on and remains in this condition as long as the controller operates in <i>Conditional Unlocked</i> door mode.
Locked door mode	21	Output goes on and remains in this condition as long as the controller operates in <i>Locked</i> door mode.
Pulse on disarming	25	Whenever controller switches to <i>Disarmed</i> mode this output goes on for approx. two seconds.
Pulse on arming	26	Whenever controller switches to <i>Armed</i> mode this output goes on for two seconds.
LIGHT flag	64	Output follows the condition of the LIGHT flag.
TAMPER flag	65	Output follows the condition of the TAMPER flag.
AUX1 flag	66	Output follows the condition of the AUX1 flag.
DURESS flag	69	Output follows the condition of the DURESS flag.
TROUBLE flag	70	Output follows the condition of the TROUBLE flag.
Card or PIN mode	80	Output goes on and remains in this condition as long as the controller operates in <i>Card or PIN</i> identification mode.
Card only mode	81	Output goes on and remains in this condition as long as the controller operates in <i>Card only</i> identification mode.
PIN only mode	82	Output goes on and remains in this condition as long as the controller operates in <i>PIN only</i> identification mode.
Card and PIN mode	83	Output goes on and remains in this condition as long as the controller operates in <i>Card and PIN only</i> identification mode.
Door lock	99	Output to a door lock.

5. Programming

The programming of a PR311-BK is divided into two separate parts:

- *User Programming*
- *Installer Programming*

The *Installer Programming* is intended to configure the unit for specific installation environment and can be carried out from PC computer only.

The *User Programming* is mainly dedicated to maintain Cards and PIN's but it is also designed to provide some other user commands. The *User Programming* can be carried out remotely from PC or locally by means of *Programming Cards*.

5.1. Programming Cards

The *Programming Card* is an ordinary proximity card or tag which was assigned for specific user function. Up to 32 *Programming Cards* can be defined in PR311-BK, each *Programming Card* may have assigned only one programming function but many *Programming Cards* may be assigned to a single user programming function. The *Programming Cards* are defined during the initial installer's setup and can be carried out from PC only.

Note: The use of *Programming Cards* is restricted to controller only, it is not possible to use the *Programming Cards* from the external reader connected to the controller.

5.2. Memory Reset - Programming MASTER Identifier

The *Memory Reset* Procedure clears entire contents of the PR311-BK memory and restores default factory settings. During this procedure the new MASTER identifier and the new controller ID number (address) can be programmed.

The *Memory Reset* consists of the following steps:

- Power down the unit
- Remove all connections from CLK and DTA lines
- Make connection between CLK to DTA lines
- Restore power, the unit will generate a continuous beep
- Wait until the LED OPEN (green) starts flashing
- Disconnect CLK from DTA
- Present any a proximity card or tag to a unit, it will be a new MASTER identifier
- Once the previous step is completed controller will generate signal OK and then will enter the *Armed* mode

If the *Memory Reset* is not accomplished successfully or the content of controller's memory is corrupted then after power up the unit will signal memory error (LED

SYSTEM is ON and the controller generates acoustic signal in sequence: sound 2s/pause 2s).

Note: With the *Memory Reset* completed controller is automatically set for address ID=00. This address can be later changed from PC to any other value from 00-99 range. Every unit connected to RS485 *Communication Bus* must have individual ID address.

5.3. User Programming

The *User Programming* can be carried out from the managing computer as well as locally using *Programming Cards*. The *User Programming* provides following programming functions:

- Management of users (adding, removing)
- AUX1 and LIGHT control commands
- *Identification Mode* control commands
- *Door Mode* control commands

Note: Programming through *Programming Cards* doesn't offer entire set of programming functions which are available in the programming from the PC.

5.3.1. Programming Cards

The following programming functions can be assigned to *Programming Cards*:

- Function No. 0 (PC-F1): **Add NORMAL user without AWA Privilege**
- Function No. 1 (PC-F2): **Add NORMAL user with AWA Privilege**
- Function No. 2 (PC-F3): **Add TOGGLE user without AWA Privilege**
- Function No. 3 (PC-F4): **Add TOGGLE user with AWA Privilege**
- Function No. 4 (PC-F5): **Add TOGGLE LTD user**
- Function No. 6 (PC-F6): **Delete a user**
- Function No. 7 (PC-F7): **Delete all users**
- Function No. 8 (PC-F8): **Set Normal door mode**
- Function No. 9 (PC-F9): **Set Unlocked door mode**
- Function No. 10 (PC-F10): **Set Conditional Unlocked door mode**
- Function No. 11 (PC-F11): **Set Locked door mode**
- Function No. 12 (PC-F12): **Set AUX1 output on**
- Function No. 13 (PC-F13): **Set AUX1 output off**
- Function No. 14 (PC-F14): **Toggle AUX1 output on/off**
- Function No. 15 (PC-F15): **Set LIGHT output on**
- Function No. 16 (PC-F16): **Set LIGHT output off**
- Function No. 17 (PC-F17): **Toggle LIGHT output on/off**

Where abbreviation **PC-Fx** is used to indicate a *Programming Card* programmed to function No. **x**.

Note: Functions No. 6 and 7 are dedicated to delete both user identifiers (card and/or PIN) and have no influence on *Programming Cards*.

5.3.2. User Programming Examples

Example No. 1: Add new NORMAL user without AWA Privilege

- Present PC-F0 *Programming Card* to the reader, the unit will generate the encourage signal (two beeps) and then will enter programming mode (LED STATUS is green, LED SYSTEM is flashing)
- As the LED STATUS is flashing present a proximity card to a reader, this card will be assigned to newly programmed NORMAL user, the ID number of a new user will be unknown
- Once the new user is programmed, the controller will generate OK signal (three beeps) and will leave programming mode and will return to operating mode it was before

Controller will not program the new NORMAL user if:

- No card is presented during time when LED SYSTEM is flashing
- The presented card is already programmed to another user

Example No. 2: Set controller to *Unlocked door mode*

- Present **PC-F10** *Programming Card* to the reader, the unit will enter programming mode (LED STATUS is green, LED SYSTEM is flashing) for a short while
- Once in the programming mode controller will set *Unlocked door mode* and then will automatically return to operating mode it was before

Example No. 3: Delete card

- Present **PC-F6** *Programming Card* to the reader, the unit will generate OK signal and enter programming mode (LED STATUS is green, LED SYSTEM is flashing)
- As the LED STATUS is flashing present a proximity card to a reader, this card will be removed from the memory of the controller
- Once the card is removed, controller generates OK signal (three beeps) and then leaves programming mode

5.4. Installer Programming

As mentioned earlier the *Installer Programming* is dedicated to configure a unit for the specific installation environment. In PR311-BK the *Installer Programming* can be carried out from PC only – it is not possible to configure the controller locally.

The following elements can be setup during the *Installer Programming*:

- Controller address (ID number)
- Function for IN1 input
- Function for IN2 input
- Function for IN3 input
- Function for IN4 input
- Function for IN5 input

Note: The IN4 and IN5 inputs are located on optional XM-2 extension module.

- Function for OUT1 output
- Function for OUT2 output
- Function for OUT3 output
- Function for OUT4 output
- Function for OUT5 output

Note: The OUT4 and OUT5 outputs are located on optional XM-2 extension module.

- **Door unlock time**
- **Door open timeout**
- **XM-2 extension module on/off**
- Option: **Timed lock-out**
- Option: **Auto-relock**
- Option: **Facility Code**
- *Timer* value for AUX1 flag
- *Timer* value for LIGHT flag
- *Timer* value for TAMPER flag
- *Timer* value for DURESS flag
- *Timer* value for TROUBLE flag

6. Installation and Setup Guidelines

- The PR311-BK reader should be mounted near the supervised door on a vertical piece of supporting structure.
- Assure that the surface beneath of the controller's rear panel is flat and smooth, especially in the area where tamper sensor will contact a surface of the wall.
- Disconnect power supply before making any electrical connections.
- For installations on a metal surface, place a non-metallic min. 10 mm thick spacer (a plastic/plaster plate etc.) between the reader and the supporting structure.
- For installations with two readers to be mounted on opposite sides of the same wall and aligned along the same geometrical axis, place a metal plate (2-4 time bigger is size then a reader) between them and make sure none of them has direct contact with it (allow min. 10 mm space between reader and metal plate). This measure is intended to isolate magnetic fields generate by both readers. If the readers are not adequate separated it may occur that card presented for a first reader will be read on the second one.
- For best results mount the proximity readers at least 0.5 m apart.
- When using separate power supply sources, connect all power supply negative (-) leads together. This rule is not valid for power sources used for supply of a door lock. Always assure that supplies used to power electronics and door locks are electrically separated.
- Roger recommends grinding the negative (-) lead of a power supply. Connection to the earth should be arranged in one arbitrary selected point.
- With its relatively weak electromagnetic field generation, the terminal should not cause any harmful interference to operation of other equipment. However, its card reading performance can be affected by other interference generating devices, esp. radio waves emitting equipment or CRT computer monitors.
- If card reading performance of the controller deteriorates (e.g. reduced reading range or incorrect readings) consider reinstallation in a new location.
- Once installed and electrically connected, the reader has to be properly configured. The programming can be carried out either through manual method or from PC. A new factory unit is delivered with preprogrammed MASTER card and with address set to ID=00.
- When lost, MASTER cards can be reprogrammed to a reader anew, any EM 125 kHz card can be programmed as a MASTER.
- It is strongly recommended to program the controller form one source only: from PC program or manually. When both methods are used to the same unit it may result in some confusion (e.g. new user added manually will not exist in PC program).
- When controller is intended to be managed from PC only you don't have to program any MASTER card, just program ID address of the unit and connect it to the computer.
- When controller operates in an *Integrated Access Control System* it must be connected to RS485 *Communication Bus*.

- The *Communication Bus* can be laid down using free topology – bus, star, three or any combination of them. It is forbidden to use topology of a ring.
- Generally the twisted, unshielded cables are recommended for *Communication Bus* (popular UTP cables). The shielded cables should be used only in installation when strong electromagnetic interferences exist.
- No terminating resistors on the ends of *Communication Bus* are required.
- The maximum cable run between any controller on the *Communication Bus* and a host PC must not exceed 1200 m.
- The maximum cable run between controller and external unit(s) connected to *Clock* and *Data* lines (e.g. external reader or I/O extension module) can be maximum 150 m long.
- The controller must be supplied form reliable power supply, calculate the adequate wire gauge to guarantee that the voltage dropout between the power supply and the supplied unit doesn't exceed 1V in the worst case.
- It is recommended to supply door release device (e.g. door strike or magnet lock) from separate power supply. When both controller and door release device are supplied from the same power source you must use separate cable pairs for both of them.
- Always add the silicon diode (e.g. 1N400x series) in parallel to door release device – locate diode as close as possible to door release and as far as possible from the controller.
- Do not supply the door release from the supply terminals of a controller.




7. Acoustic and Optical Signals

Table 6. Acoustic signals.

Signal	Symbol	Description
One long signal	♪	Programming error or unknown identifier (card or PIN not registered in the controller).
Two long signals	♪ ♪	Access denied, identifier is registered in controller's memory but actually has not access authorization. Alternatively this signal will occur when controller operate in Card and PIN mode but user entered only one from two required form of identification.
Three short beeps	♪♪♪	Command or procedure successfully completed (OK signal).
Two burst of three beeps	♪♪♪ ♪♪♪	Signal OK. repeated two times is generated each time the controller restarts.
Two beeps	♪♪	Prompt signal, the reader is waiting for the next part of the command. This signal is intended to encourage the programmer to proceed with next programming step.

One long signal continuously repeated	♪ ♪ ♪ ♪ ... and so on	Memory contents corrupted or MASTER card not programmed - memory reset necessary. This signal is accompanied by the steady lit LED SYSTEM.
Legend: ♪ - one long audible signal ♪ - one short audible signal (beep).		

Table 7. LED indication.

LED STATUS	LED OPEN	LED SYSTEM	Meanings
			
Steady (green)	—	—	Controller is <i>Disarmed</i> .
Steady (red)	—	—	Controller is <i>Armed</i> .
Steady (green)	—	Steady	Controller is in the <i>User Programming</i> mode.
Flashing (green)	—	Flashing	Controller is waiting for next step during the <i>User Programming</i> mode.
—	—	Flashing	Controller is waiting for an identifier.
—	Steady	—	The door lock is activated; this LED remains ON as long as the door lock is energized.
—	—	Steady	The memory contents corrupted or MASTER identifier not programmed. This situation is accompanied by acoustic signal repeated in sequence: sound 2s/pause 2s.
Blinking	Blinking	Steady	The controller is being programmed from PC, the LED STATUS and OPEN are blinking along with data send/received by a device.

8. Appendix

Table 8. Connection cable assignments.

Wire Color	Label	Description
Red	+12V	Supply input plus.
Black	GND	Supply input minus.
Pink	IN1	Input line, internally pulled up to the supply plus through a 5,6K resistor.
Blue	IN2	Input line, internally pulled up to the supply plus through a 5,6K resistor.
White-Yellow	IN3	Input line, internally pulled up to the supply plus through a 5,6K resistor.
Red-Blue	COM	Relay output contacts, 1A/24V DC/AC rated:
Grey-Pink	NC	COM – common

Violet	NO	NO – normally open NC – normally closed Note: The relay contacts are protected with the MOV varistors, any attempt to apply higher voltages than specified to the relay contacts will cause damage.
Yellow-Brown	OUT2	Transistor output, open collector type, 16V/1A, normally in high resistance, when triggered it switches to GND (supply minus).
Green-Brown	OUT3	Transistor output, open collector type, 16V/1A, normally in high resistance, when triggered it switches to GND (supply minus).
Brown	A	RS485 communication bus: A: Wire A B: Wire B
Green-White	B	
White	CLK	Clock communication line, internally pulled up to supply plus through 5,6K resistor.
Green	DTA	Data communication line, internally pulled up to supply plus through 5,6K resistor.
Grey	TMP A	Tamper contacts, 50mA/24V rated, NC and dry: TMP A: Wire A TMP B: Wire B
Yellow	TMP B	

Table 9. Technical specification.

Technical Specification	
DC Supply	10...16 VDC
Current Consumption	Avg. 60 mA
Anti-sabotage Protection (Tamper)	NC contact, 50mA/24V, IP67
Reading Distance	Up to 12 cm for ISO cards (depends on cards).
Proximity Cards	EM UNIQUE 125 kHz, ASK modulation, 64 bits (compatible with EM4100/4102).
Communication Distance	Between controller and PC (UT-2 interface): max. 1200 m. Between controller and Host (CPR32SE): max. 1200 m. Between controller and external reader: max. 150m. Between controller and XM-2 extension module: 150m.
Environmental Class (according to EN 50131-1)	Class IV, Outdoor-General, temperature: -25°C- +60°C, relative humidity: 10 to 95% (non-condensing)
Ingress Protection	IP 65
Dimensions	100 X 40 X 25 mm
Weight	~130 g
Approvals	CE

Table 10. Ordering codes

Ordering Codes	
PR311-BK Grey	RFID Access Controller, grey.
PR311-BK Light Grey	RFID Access Controller, light grey.
RM-2	Relay module, the RM-2 offers two relays with one NO/NC contact 1.5A/24V rated, relay contacts are protected with over-voltage elements.
XM-2	I/O extension module, digital communication with host reader, two NO/NC inputs and two relay outputs, each relay offers one NO/NC contact 1.5A/24V rated. Relay contacts are protected with the over-voltage elements. Module is delivered with ABC installation box.

Table 11. Product history



Hardware	Firmware	Date	Description
PR311-BK v1.0	102.00	24/09/05	Initial product version.

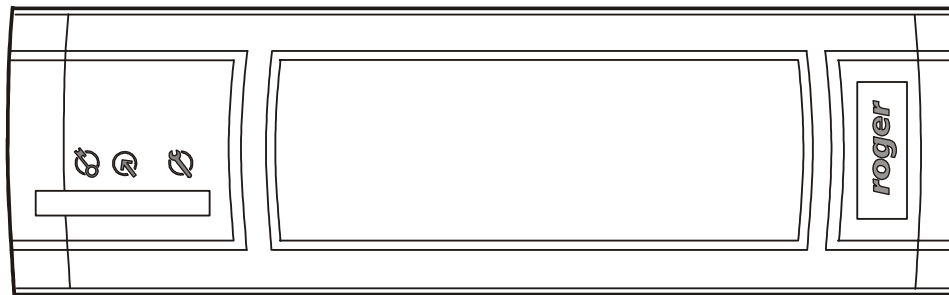
Table 12. Document history

Hardware	Firmware	Date	Description
PR311-BK fv102.00 Rev. A.	102.00	24/09/05	Initial product version.

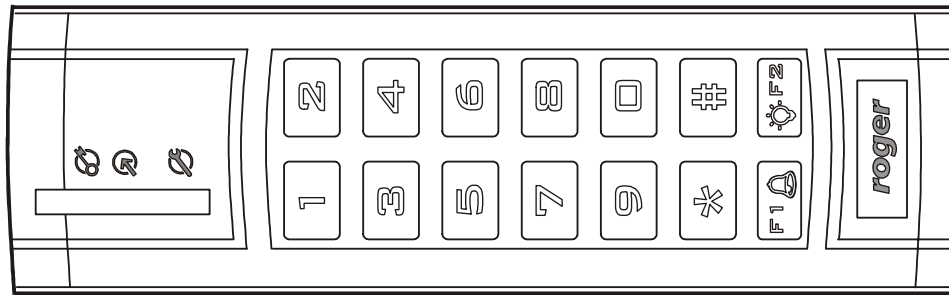
Contact information:**Roger sp. j.****82-416 Gościszewo****Gościszewo 59****Phone: 055 272 0132****Fax: 055 272 0133****e-mail: biuro@roger.pl**

PR311 and PR311-BK Views and Installation Diagram

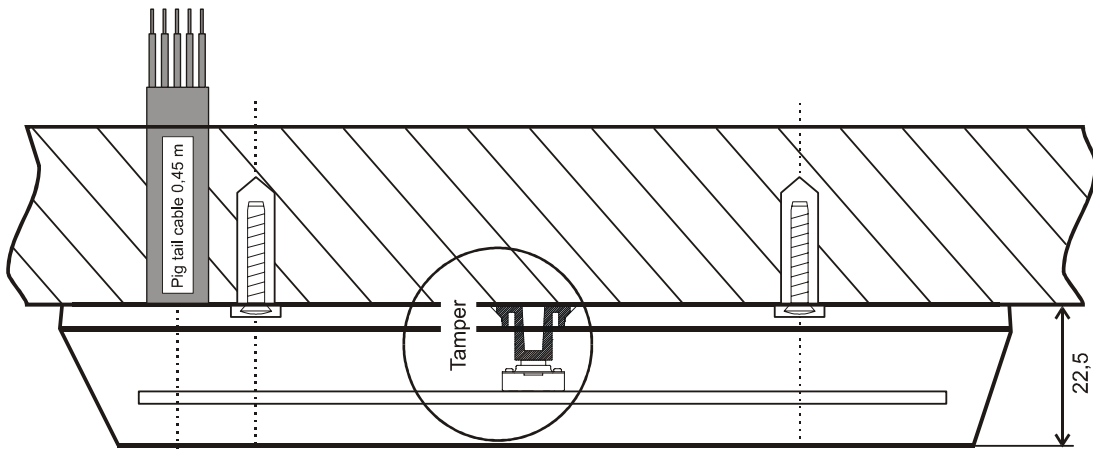
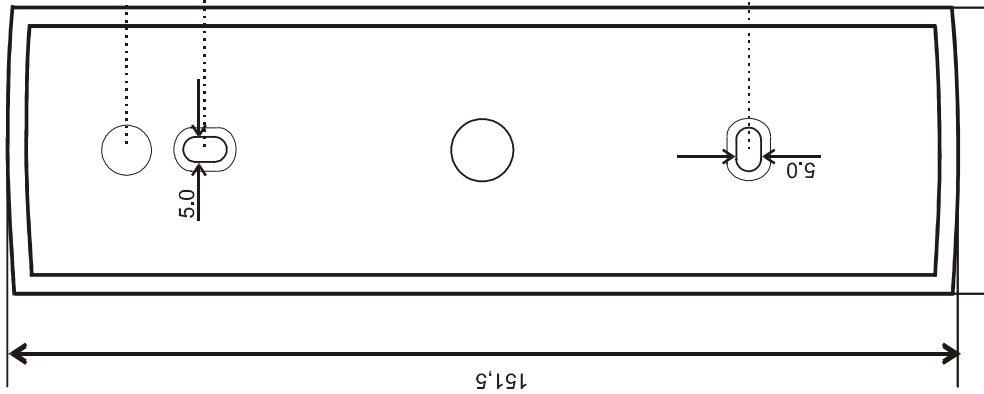
-  LED STATUS
-  LED OPEN
-  LED SYSTEM



PR311-BK



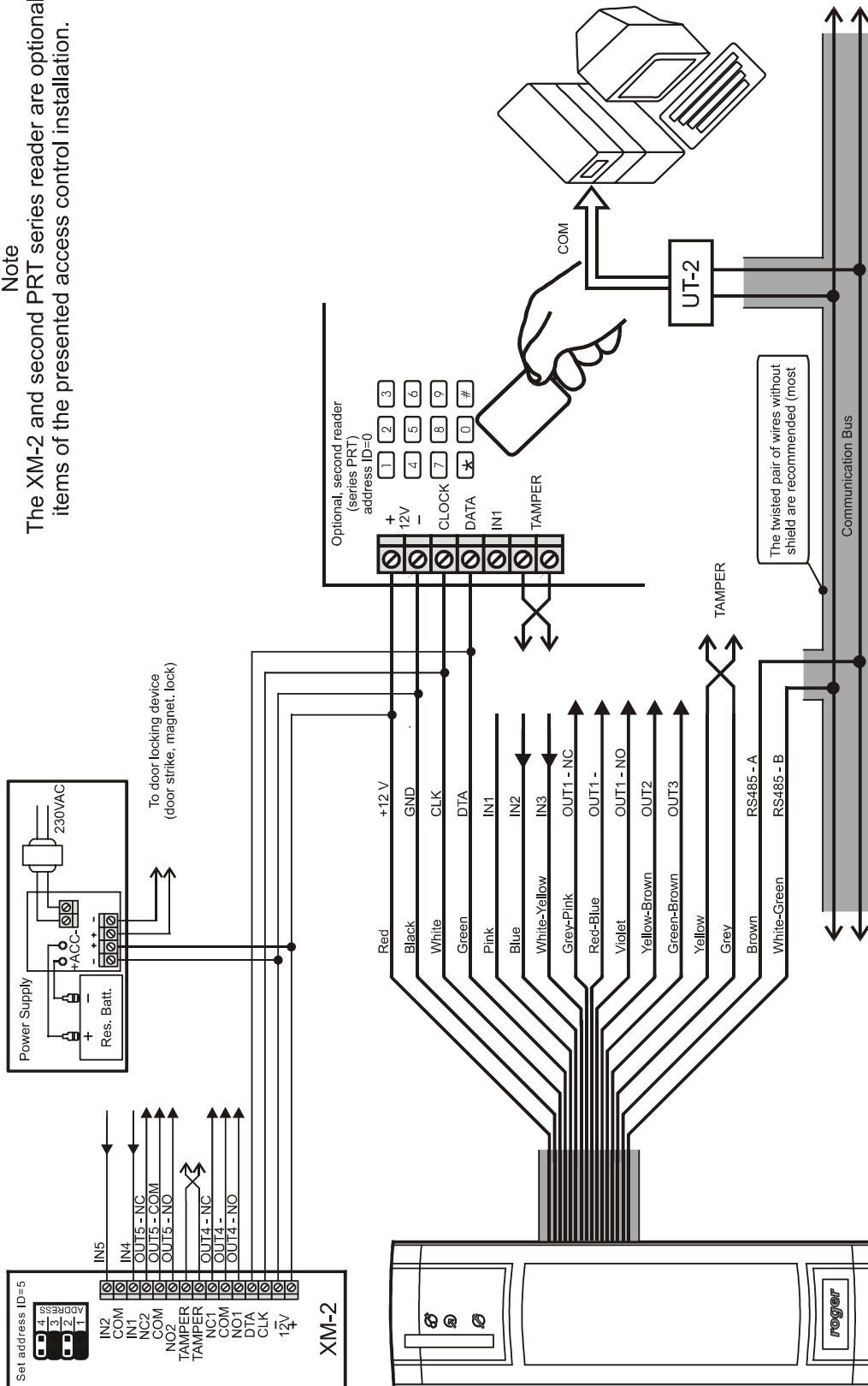
PR311



cd1r171 EN

PR311-BK Typical Wiring Diagram

Note
The XM-2 and second PRT series reader are optional items of the presented access control installation.



cdr180-BK