

ИСО 9001



ACCESS CONTROLLER

S2000-2

User's Manual

WARNING:

To change configuration parameters of the controller please use **UProg.exe software utility of versions 4.1.0.54 and higher. DO NOT use UProg.exe of versions 4.0.0.821 and below**

CONTENTS

1 Description and Operation	4
1.1 Functions of the Controller	4
1.2 Specifications	5
1.3 Standard Delivery	8
1.4 Access Modes	8
1.5 Two-Factor Authentication	10
1.6 Access Levels.....	11
1.7 Two (or More) Person Rule Access Control.....	12
1.8 Time Zones	13
1.9 Antipassback Rules	14
1.10 Coerced Access	17
1.11 Centralized Access and Operating Partitions.....	17
1.12 Access by ID Templates	19
1.13 Connecting Readers	20
1.14 Connecting Door Open Sensors (Passage Sensors).....	25
1.15 EXIT, PERMIT (CONFIRM) and DENY Buttons.....	26
1.16 Alarm Loops	27
1.17 BUSY Input / Output	31
1.18 Light and Sound Indication.....	33
1.19 Configuration Parameters	36
1.20 Programming Credentials	51
2 Operation.....	53
2.1 Two Entrance Doors Mode.....	57
2.2 One Entrance / Exit Door.....	60
2.3 Turnstile Mode.....	63
2.4 Boom Barrier Mode	66
2.5 Mantrap Mode.....	71
3 Maintenance	75
3.1 Functionality Test	75
4 Marking	77
5 Packaging	78
6 Storage.....	78
7 Transportation	78
8 Certificates	78
9 Manufacturer Data.....	79
Appendix A Overall and Mounting Dimensions of the S2000-2 Controller.....	80
Appendix B PCB Layout.....	81
Appendix C The Schematics for Connecting Readers to the S2000-2 Controller	82

This User's Manual is intended to help for studying operability principles and maintenance of S2000-2 Access Controller of version **2.20**.

The S2000-2 Access Controller (hereinafter referred to as the controller) is designed to control access through a single or two access points by reading the codes of presented credentials (Proximity cards, iButtons, PINs), verifying access rights, and closing (opening) the contacts of relays operating locking devices (electromechanical or magnetic locks or electric strikes, turnstiles, boom barriers).

The controller is designed to operate as part of a PC-based Orion integrated security system under Orion Pro software of the version 1.20 SP1 or higher, or as part of an Orion integrated security system based on an S2000 or S2000M control panel, or in standalone mode.

1 Description and Operation

1.1 Functions of the Controller

1.1.1 Local access control, that is granting or denying access for holders of credentials registered in the controller's database, depending on the access rights of the presented credentials, the current access mode and current access rule violations of the presented credentials.

1.1.2 Centralized access control, that is reading the code of a presented credential and transmitting it to the network controller (Orion Pro workstation) followed by granting or denying access for the holder of the presented credential by a command of the network controller (only if the controller operates as part of an Orion system based on a personal computer).

1.1.3 Arming and disarming partitions (when the controller operates as part of an Orion system based on a PC or an S2000M panel).

1.1.4 Arming and disarming up to four loops of an intrusion alarm system, monitoring loop conditions and sending alarms over the RS-485 interface to the network controller (Orion Pro workstation or S2000 panel).

1.1.5 The controller is intended to be installed inside premises and is designed for round-the-clock operation.

1.1.6 The controller is not designed to be used in aggressive or dust media or in explosion hazardous premises.

1.1.7 As to resistance to mechanical attacks the controller falls into the 03 placement category in accordance with Russian Standard OCT 25 1099-83.

1.1.8 As to resistance to climatic effects the controller is produced in the implementation 3 in accordance with Russian Standard OCT 25 1099-83 but for operating temperatures minus 30°C to +50°C.

1.2 Specifications

1.2.1 The controller is to be powered by an external dc power supply with 12 V rated voltage (10.2 V to 15.0 V). Battery backed power supplies of RIP-12 series manufactured by the Bolid Company are recommended for use.

1.2.2 The power consumed by the controller from an external dc power supply does not exceed 2 W.

1.2.3 The maximum current consumed by the controller from an external dc power supply does not exceed 120 mA.

1.2.4 The number of connected readers of iButtons, Proximity cards, or PINs with output interface Touch Memory (1-Wire, μ -LAN), Wiegand, or ABA TRACK II is 2.

1.2.4.1 The controller provides operating the two LEDs (the single two-color LED) of each reader. The control levels match logic levels of +5 V CMOS. In case of direct connection of LEDs the controller limits the current through the LEDs by 10 mA.

1.2.4.2 The controller provides controlling reader's beepers. The control levels match logic levels of +5 V CMOS.

1.2.5 The distance between the controller and the reader shall not exceed 100 meters.

1.2.6 Memory capacity: 32768 codes of credentials (iButtons, Proximity cards, PINs).

1.2.7 The number of actuator relay to control locking devices is 2.

1.2.7.1 The maximum switching current of each relay is 7 A.

1.2.7.2 The maximum switching voltage for each relay is 30 V.

1.2.7.3 The maximum switching power of each relay is 100 W.

1.2.8 The controller provides condition analysis for up to four intrusion alarm loops with arming and disarming them by means of presenting iButtons (Proximity cards, PINs) or over the RS-485 interface. The controller also transmits loop events over the RS-485 interface.

1.2.9 The controller can be used in one of the following operation modes:

- Two Entrance Doors;
- One Entrance / Exit Door;
- Turnstile;
- Boom Barrier;
- Mantrap.

1.2.10 In all operation modes the controller supports the following access modes:

- "Simple": access requires presenting one (a "primary") credential;
- "With extra code": access requires presenting two credentials (a "primary" and an "extra" ones);
- "Confirmed manually": after presenting a credential access must be confirmed by a guard manually, by pressing a CONFIRM button;
- "Two-person rule" ("Three-person rule"): access can be granted after presenting two or three credentials with specific access levels;
- "Centralized access": access with presenting a credential not registered in the controller itself with making a decision about granting / rejecting access by the network controller ("Orion Pro");
- "Access locked": local access is prohibited (centralized access can be granted);

- "Free pass": no credential is required to achieve access.

1.2.11 The following factors to limit access are taken into account while analyzing access rights of a presented credential:

- The credential must not be disabled;
- The credential must have a right to access the access zone;
- Validity of the credential;
- The Time Zone of the credential must be active;
- Antipassback rules;
- Conditions of alarm loops of the controller which lock access;
- Status of BUSY signal.

1.2.12 The access controller transmits the network controller (Orion Pro or S2000M panel) the following messages over the RS-485 interface:

- "Identification" – Authentication of the user has been completed but access rules have not yet been checked (in case of two- or three-person rules or manually confirmed access);
- "Access Granted";
- "Transaction" – After granting access a passage to the access zone has been detected;
- "Access Denied" – Access is denied for the presented registered credential;
- "Wrong Code" – An unknown credential is presented to a reader when there is no communications between the S2000-2 and the network controller (the message is stored in the S2000-2 memory);
- "Duress Code" – Access under coercion;
- "Access Locked" – Access is locked for all credentials;
- "Free Pass" – Access control is deactivated;
- "Access Restored" – Access control has just been activated;
- "Disarmed";
- "Armed";
- "Arming Delay";
- "Arming Failed";
- "Loop Alarm";
- "Authentication" – A credential for arming/disarming loops has been presented to a reader;
- "Door Open" – The passage sensor (door sensor) has responded;
- "Door Closed" – The passage sensor (door sensor) has returned to the quiescent mode;
- "Door Held Alarm" – The door has been open too long (for more than 30 s);
- "Door Forced Open" – The door is forced open without granting access;
- "Tamper Alarm" – The S2000-2 enclosure has just been opened;
- "Tamper Restored" – The S2000-2 enclosure has just been closed;
- "Power Failed" – The device input voltage is out of range;
- "Power Restored";
- "Battery Failed" – Low voltage or missing of the battery which backs up power for the real-time clock;
- "Battery Restored";
- "Programming" – The controller is switched to the programming mode by means of a Master credential or Master credential re-programming;

- "Manual Test" – Switching the self-diagnostic mode on;
- "Relay ON/Pulsing/OFF" – Changes in relay states;
- "Guessing" – The number of subsequent attempts to present unknown credentials to the reader has exceeded the programmed value.

1.2.13 If a temporary communication loss happens to be during generating of a message then the messages are stored within the S2000-2 nonvolatile memory (EEPROM). Then, when RS-485 communications are restored, the stored messages are transmitted to the network controller along with actual event data and time in accordance with the internal S2000-2 clock.

1.2.14 The capacity of the event buffer in the non-volatile memory of the controller is 32768 events.

1.2.15 The controller provides executing the following commands received over the RS-485 interface:

- Writing configuration;
- Assigning a network address;
- Arming / disarming alarm loops;
- Access control, that is granting, locking, unlocking, and restoring controlled access;
- Reading the list of credentials;
- Adding and editing the list of credentials;
- Synchronizing clock;
- Reading ATD values of resistance of the alarm loops;
- Requests for states of the controller, the alarm loops, the readers, the doors.

1.2.16 The controller doesn't send false alarms under electromagnetic interference of third severity level in accordance with Russian Standard ГOCT P 50009.

1.2.17 Radio disturbances from the controller operation do not exceed the values specified in ГOCT P 50009.

1.2.18 The pre-operation time after powering up doesn't exceed 5 s.

1.2.19 The mean time between failures of the controller in quiescent mode should be at least 80000 hours which is equivalent to the probability of no failure 0.98758 within 1000 hours.

1.2.20 The probability of a failure which can trigger a false alarm of the controller should be no more than 0.01 per 1000 hours.

1.2.21 The average lifetime of the controller is 10 years.

1.2.22 The weight of the controller does not exceed 0.3 kg.

1.2.23 The overall dimensions are 156 mm × 107 mm × 39 mm.

1.2.24 The ingress protection rating of the controller is IP30 in accordance with ГOCT 14254-96 (IEC 529-89) provided that the controller is mounted on a wall.

1.2.25 According to the content of precious materials the product does not require accounting for storage, writing-off, and/or disposal.

1.3 Standard Delivery

S2000-2 Access Controller	1 pcs.
Resistor MF 1/4W-8.2k + 5%	6 pcs.
Woodscrew 1-3×25.016 ГОСТ 1144-80	3 pcs.
Wall Plug	3 pcs.
DIN 7982 Flat Head Tapping Screw with Cross Drive 2.2×6.5	1 pcs.
S2000-2 Datasheet	1 pcs.
S2000-2 Installation Manual	1 pcs.

1.4 Access Modes

For all operation modes of the controller (Two Entrance Doors, One Entrance/Exit Door, Turnstile, Boom Barrier, and Mantrap) each of the two access directions (each reader) can operate in one of the three following access modes:

- Controlled Access;
- Access Locked;
- Free Pass.

The access mode of one reader (access in one direction) can differ from the access mode of the second reader (access in opposite direction).

In addition to the long-duration access modes mentioned above, for any of the readers the Access Allowed mode can be enabled providing granting access while presenting any credential.

Moreover, until an access procedure started before has been terminated the readers of the controller can be in the *Busy* state.

1.4.1 Controlled Access

In the Controlled Access mode the controller provides both local and centralized access.

Local access in this mode is granted for holders of those credentials which are enrolled in the database of the controller, are in effect at the time, are authorized to access the specified area, meet the access conditions (the required number of credentials has been presented) and when no access rule violations (time zone violations, antipassback rule violations, validity violations) are detected provided that no alarm loop locking access is armed.

By a similar way access is granted for holders of credentials which are not enrolled in the controller's database but their codes match one of the ID Templates of the controller.

Centralized access is granted by a network controller (Orion Pro Workstation) commands for holders of credentials which are not enrolled in the controller's database and meet no ID Template.

Further in the text, while describing functions of the controller local access is implied unless otherwise specified.

1.4.2 Locking Access

Access is locked or by presenting a special Locking credential, or by a remote command over the RS-485 interface, or by arming the alarm loops locking access. If access was locked by a Locking credential or remote command then the LED of the relevant reader starts pulsing once per second with short pauses in red.

If access is locked by a special credential or by command then it is locked for all the credentials stored in the controller's memory (locked local access). In this case only centralized access or access by Exit button, if applicable, can be allowed. (Centralized access can be locked only by settings of the network controller). In addition, the reader can be switched to the Access Allowed mode for a single authentication.

The Controlled Access mode can be restored or by second presenting of the Locking credential, or by presenting an Unlocking credential, or by a command of the network controller over the RS-485 interface. To make the credential Locking or Unlocking, the Passage Mode parameter in the access level of the credential is to be set to "Locking" or "Unlocking" respectively.

If access is locked because the alarm loops locking access are armed then on presenting a combined credential authorized to disarm these alarm loops the alarm loops are disarmed and simultaneously access is granted. For other credentials (intended only for requesting access or combined without rights to disarm locking alarm loops) access is denied. Locking access by alarm loops prohibits also access by EXIT button.

Locking access by alarm loops is canceled by disarming alarm loops locking access.

1.4.3 Unlocking Access

Access is unlocked on presenting a special Unlocking credential, or after activation of a special alarm loop (see Section 1.16.14), or by a command of the network controller over the RS-485 interface. In this case the LED of the relevant reader starts pulsing ones per second with short pauses in green.

In this mode free access can be achieved by everybody without presenting credentials.

In the Free Pass mode the controller activates the relevant relay to be open permanently (the relay for this direction is either always on or always off) or in pulse mode (the relay is switched on or off on every door closing). The second way to control a relay in the Free Pass mode is suitable for such kind of barrier devices as electric strikes. *Please take into account that applying voltage continuously to some kinds of strikes can make them inoperative.*

In the operation modes Two Entrance Doors and Turnstile each of the two readers (directions) can be switched to the Free Pass mode without regard to another reader. In other operation modes (One Entrance / Exit Door, Boom Barrier, Mantrap) activation of the Free Pass mode on one reader automatically activates this mode for another reader.

If before passing a user has presented its credential enrolled in the controller memory and intended for access then its passage in the Free Pass mode is logged by the same way as in case of the Controlled Access mode. It can be necessary for time & attendance purposes or for correct operation of antipassback functions.

If the Free Pass mode was switched on by means of the alarm loops then to restore the Controlled Access mode it is necessary to normalize the resistance of the alarm loops. In other cases the Controlled Access mode is achieved or by the second presenting of the Unlocking credential, or by presenting a Locking credential, or by a command of the network controller over the RS-485 interface. To make the credential Locking or Unlocking, the Passage Mode parameter in the access level of the credential is to be set to "Locking" or "Unlocking" respectively.

1.4.4 Access Allowed Mode

This mode can be switched on by pressing the PERMIT access button and is effective only for one authentication. In this mode the LED of the relevant reader pulses with green once per second.

In this mode a holder of any credential can achieve access regardless of the purpose of the credential (Master, Unlocking, Locking, Operating, etc.) even if access rules are violated or the credential is not enrolled in the controller.

The Access Allowed mode terminates just after granting access for a presented credential or the expiry of 10 s timeout (if no credential was presented) as well as after the second press on the PERMIT button. The reader returns to its long-term mode in which it was before: Controlled Access, Access Locked, or Free Pass.

The PERMIT button is supposed to be situated near a guard and is used for those cases when it is necessary to approve granting access with logging passage with a credential without access rights or with registered access rule violations (for time & attendance purpose or correct operation of antipassback rules).

1.4.5 Busy State

Until a current access procedure is completed the controller generates an *internal Busy* signal. For such operation modes as Turnstile, Boom Barrier, and Mantrap, while this signal is in effect no access is provided for a next credential. In the operation modes One Entrance/Exit Door and Two Entrance Doors an internal Busy signal is ignored.

In spite of internal Busy signals an external Busy signal can be sent to the BUSY input of the controller. Its effect on each of the readers is defined by a relevant configuration parameter of the reader and doesn't depend on the operation mode of the controller. The BUSY input/output is designed to synchronize operation of several controllers in case of arranging sophisticated access points and to connect a presence detector (occupancy sensor) in a mantrap, vehicle loop detector at a parking lot etc.

If a credential is presented when an internal or external Busy signal is being active, then access cannot be achieved, please try to access later.

1.5 Two-Factor Authentication

One of the ways to strengthen protection against unauthorized access is *two-factor authentication* when a user is required to present two credentials rather than a single one (for example, a Proximity card and a PIN).

In case of two-factor authentication a procedure of granting access or operating alarm loops begins with presenting a first credential – a Primary Code. After that the controller proceeds to the mode of waiting for presenting an additional code, with the reader LED flashing with green five times per second. Within 30 seconds a second credential should be presented – the Extra Code.

If the presented code does not coincide with the Extra Code then the controller generates an Access Denied message with the Extra Code Error attribute. If a correct additional code is presented then the authentication is considered to be completed successfully and the controller or grants access, or proceeds to authentication of a next user (if a two-person rule or three-person rule is in effect), or arms or disarms the alarm loops operated by the presented credential.

Necessity to apply two-factor authentication is programmed for every group of users (for every access level) individually for each reader by setting the configuration parameter *Two-Factor*

Authentication on. In this case for all the users which fall under this group (assigned with this access level) in addition to a primary credential code an extra code must also be defined.

A primary and an extra codes are presented to a single reader, so combinations of codes of various types (for example, a Proximity card and a PIN) can be used only if the relevant combined readers are connected which provide reading credentials of various types and sending them to the controller in a single format (Touch Memory, or Wiegand, or ABA TRACK II). These combined readers include, in particular, readers of the Proxy-Key series.

If Two-Factor Authentication is set on then presenting the relevant extra code is required without regard to the function of the credential for the current reader (granting or confirming access, locking or unlocking access, arming / disarming alarm loops). Only for a Master credential two-factor authentication is never applied because an access level of a Master credential defines authorities of the credentials programmed by means of the Master credential rather than the authorities of the Master itself.

1.6 Access Levels

To simplify the process of description of access rights for every credential and its rights to operate the alarm loops, the *Access Level* category is used. An access level is a set of rights and limitations applied to a group of credentials (users). Thus, defining access rights for all the credentials is substituted by defining access rights for all groups of credentials (defining access levels) and assigning every credential with one or another access level.

Thus, on adding a new credential (user) for defining its access rights only specifying its access level is required. And to change access rights for a whole group of credentials it is only required to change these rights for their access level.

For the S2000-2, user authorities described in an access level are programmed for each reader individually. So, an access level includes two identical sets of parameters: one set for the first reader and once more set for the second one.

The parameter Two-Factor Authentication requires requesting for an extra code from a credential holder when he or she is authorized at the reader (see Section 1.5).

Other parameters to be programmed for user via an access level fall into two groups. The functions of a credential assigned with access control are enabled by setting on the *Access* attribute. If the attribute is set on then the additional parameters of the Access group can be programmed:

- Passage Mode (which access function the credential performs at the reader);
- Access Time Zone (the intervals of time allowed for access, see Section 1.8);
- Antipassback Mode (see Section 1.9);

The functions of a credential assigned with arming and disarming are activated by setting on the attribute *Operating*. Also other parameters of the Operating group are programmed:

- Rights to arm and/or disarm alarm loops LP1... LP4 of the controller;
- Operating Time Zone (the time intervals allowed for operating alarm loops, see Section 1.8).

Passage Mode (access function) can be:

- Prohibited (no rights to access the zone controlled by the reader);
- Simple (by authentication of a single credential holder);

- Two-Person Rule (see Section 1.7);
- Three-Person Rule (see Section 1.7);
- Confirmed Manually (a confirmation of a guard is required);
- Confirmation (for those who doesn't request access via the access point but confirms pass for other credential holders in accordance with a two(three)-person rule);
- Unlocking (activates Free Pass mode for the reader, see Section 1.4.3);
- Locking (activates Access Locked mode for the reader, Section 1.4.2).

If in access level of the credentials both the parameters Access and Operating are set on then for this reader the credential is combined, i.e. is used both for access and for arming / disarming alarm loops of the controller (see Section 1.16.10) or partitions of fire or intrusion alarm system (see Section 1.11).

All access level parameters are applied to credentials of User and Duress types. For credentials of Master type access levels are given only for inheriting by User credentials to be programmed by using this Master one.

Configurations of access levels with the numbers 1 to 100 are programmable. The parameters of the access level No.0 are fixed and imply that for both readers of the controller a credential with zero access level is used only for access with Time Zone 0 ("Always"), Simple passage mode, disabled antipassback.

1.7 Two (or More) Person Rule Access Control

In order to control access to zones with increased safety requirements, *two or three person access rules* can be used when two or three persons must present their credentials with matched access levels to gain access. Implement this by doing the following:

- Set on the Access parameter of the access level;
- Set Passage Mode to the value "Two-Person Rule" ("Three-Person Rule");
- Select the Access Level 1 to confirm passage;
- Select the Access Level 2 to confirm passage if a three-person access rule is in effect.

If the access level of a presented credential implies passage in accordance with a two(three)-person access rule then an Identification message is generated, the green LED of the readers starts pulsing five times per second, and the controller within 30 seconds is waiting for authentication of the credential(s) which access level is (are) confirming for the presented credential.

If the next presented credential has a mismatched access level and granting access conditions are also not met for the credential then the controller generates an Access Denied message with the attribute *Confirmation Error*.

If the presented credential has a matched access level but granting access conditions have not yet been met for both the presented credentials (three-person access rule) then an Identification message is generated and the controller is waiting for presenting a third credential for 30 seconds.

If after presenting the second or third credential the access conditions are met for at least one of these credentials, access is granted. If the controller operates in the Two Entrance Doors or One

Entrance/Exit Door mode, Access Granted messages are generated for all the credentials which meet the access conditions. In all other operating modes, the controller generates the Access Granted message for the first credential only.

If not all the persons, involved in the two(three)-person rule access procedure, are supposed to enter the restricted zone (for example: a security guard confirms access of another staff member), it is necessary to set the *Confirmation* passage mode for the access level of such persons. The passage itself is not permitted for the holders of credentials in such passage mode and neither Access Granted nor Passage messages is generated for such credential during the two(three)-person rule access procedure.

Two-(three) person access rules like other parameters of Access Level are programmed for each reader (each passage direction) separately. For example, to entry a zone (to pass into a zone controlled by the first reader) the two-person rule is used, while to exit this zone (to pass into a zone controlled by the second reader) the Simple passage mode (authentication of one person only) is used, and vice versa.

Passage modes to access zones controlled by the first and the second readers (entry mode and exit mode) for every access level are programmed independently of another access level. Thus, for example, for one access level passage to one zone can be programmed in accordance with a two-person access rule while for the second access level simple passage can be given to the same zone (via the same reader).

If for the access level X the parameter Passage Mode for one of the readers of the controller is set in accordance with a two-person access rule and the access level Y is specified as *Access Level 1 to Confirm Passage* then:

- If two-person rule access via the reader is set for the access level Y too and the access level X is selected to be the *Access Level 1 to Confirm Passage* for the level Y then access for holders of the credentials included in the access level X is granted only accompanied by a holder of a credential included in the level Y, and vice versa;
- If the simple passage mode is selected for the access level Y, then such credential holder is allowed as to confirm access by an access level X credential, as to pass in specified direction (via this reader) by himself.

1.8 Time Zones

To restrict access rights for users depending on the date, the day of the week, and/or the time within a day the so called *time zones* are programmed for the S2000-2 and assigned with access levels.

For every access level each reader of the controller is assigned with two time zones, the first one being used for access and the second one being used for arming / disarming alarm loops.

An access level can be assigned with time zone numbers 0 to 100. Time zone 0 means no time / date / day of the week limitations. Configuration of time zones with numbers from 1 to 100 is programmed for the controller.

A time zone descriptor is composed of a list of time slots (ten) and a list of "holidays" within one year.

A descriptor includes the start and stop times for every time slot (hours and minutes) and activity flags for this slot in every day of the week as well as in holiday.

The list of holidays allows reassigning a day of the week for any day for a year ahead or to announce any day to be a holiday. If a day in the holiday list is not reassigned (being an ordinary day), the day of the week corresponds to a calendar day. If the day is reassigned, the calendar is ignored and the controller considers this day as it is defined in the holiday list. The reassigned value of the day of the week may take one of the following values: 1 (Monday), 2 (Tuesday), ..., 7 (Sunday), 8 (eighth day of the zone), ... 14 (fourteenth day of the zone), Holiday. The Holiday value is entered solely to facilitate in the list reading and in principle does not differ from other values (1 ... 14), therefore it may be qualified as fifteenth day of the zone.

Thus, the holiday list allows:

- Announcing any day to be a holiday (that is the day with active time slots different from the slots set for other days of the week);
- Transferring working days (for example, a day stated in the calendar as Saturday may be announced as Monday);
- Programming complex flexible access schedules with repeatable period lasting for less than 7 days or exceeding 7-day period;
- Programming complex access schedules without an explicit repeatable period.

Two typical ways of filling the holiday list may be supposed among all the diversified variants:

1) If the access schedule (schedule of work) for employees is bound to the calendar week (for example, days from Monday to Friday are working days, and Saturday and Sunday are the weekends), most of days are not reassigned in the list (a 'Daily' day is determined by the calendar). Only a few days in the list are marked as the 'Holiday' day, or redefined (if working days are re-announced), or redefined for values more than 7 (if special time intervals must be active for these days).

2) If sophisticated and variable access schedules (schedules of work) are not assigned with a calendar week then days of the week are assigned explicitly for all the listed days (reassigned) and no ordinary days (for which a day of the week is defined according to the calendar) are left in the list.

In order to limit access rights for a credential by time, date, and validity, the controller clock has to be synchronized with the network controller. This is provided automatically when the S2000-2 operates as a part of the Orion system based on PC or the S2000M/S2000 control panel of ver.1.20+, provided that the date and time are set for the PC or the control panel. The controller is equipped with a non-volatile clock and calendar, thus turning off the network controller, the RS-485 interface communication fault, and even an S2000-2 outage will not cause the clock failure, time limitations operating correctly after the controller starting up again. Meanwhile, one should be kept in mind that if the S2000-2 operates standalone for a long time its clock can shift. That is why it is not recommended to use time zones while the controller operates in standalone mode (without a network controller): all time zones for all access levels should have the number 0. The controller backup battery provides power supply to the S2000-2 clock for at least 5 years.

1.9 Antipassback Rules

In order a credential cannot be used for second entry in an access zone without preceding exit, the *antipassback* feature is used.

An antipassback rule is considered to be violated if after a passage to a target zone of the reader no passing back to the source zone was registered and an attempt to access the target zone second time

with the same credential is detected. The respond of the controller after violating of antipassback rules depends on the current antipassback mode programmed for both the readers in the access level of the presented credential.

One of the following antipassback modes can be applied:

- None (violation of antipassback are not monitored);
- Hard;
- Timed;
- Soft.

Hard antipassback denies next entry (access to the target zone of the reader) until egress from the zone is detected (access to the source zone of the reader). Upon an attempt to violate antipassback rule access is not granted and an Access Denied message is generated with the attribute *Antipassback Violation*.

Soft antipassback does not deny second access but following violation of antipassback rules Access Granted and Transaction messages are generated with the attribute Antipassback Violation.

Timed antipassback uses an additional parameter, *Lockout Period*. Within this predefined amount of time after credential holder's passage to the access zone timed antipassback is similar to hard antipassback (the controller inhibits any second access if antipassback rule is violated and generates an Access Denied message), but on expiry of this time timed antipassback is similar to soft antipassback (second access is granted but Access Granted and Transaction messages are generated with the attribute Antipassback Violation).

If the S2000-2 operates as part of an Orion system, it checks antipassback rules taking into account all passages to the access zone registered by other controllers of the system (the *Global* antipassback rule is implemented). So, if an access zone comprises several access points (for example, several barriers in office lobby or several turnstiles operating in parallel) equipped with S2000-2 controllers then in case of entry to this zone through one access point (one S2000-2 controller) entry at all other points (S2000-2 controllers) is locked while egress from the zone is unlocked and, vice versa, in case of exit from this zone through one access point for all other access points exit from the zone is locked while entry is open (if however an antipassback rule is applied for this credential).

An antipassback feature is used correctly between two access zones only if the following requirements are met:

- Authorized passages from one zone to another are only possible via the access points controlled by S2000-2 controllers;
- Access points between the zones have to be equipped with readers providing authentication both for entry and for exit as well as be equipped with passage sensors;
- The parameter Target Access Zone must be set to the same value for all the readers which control passage to the same access zone.

For all operation modes of the controller apart from Two Entrance Doors it is implied that a target access zone of one reader is on the other hand also the source access zone of another reader, so the readers should be assigned with different Target Access Zone numbers. In the Two Entrance Doors operation mode the readers of a controller belong to two separate access points, so in addition to Target Access Zone for each reader the Source Access Zone parameters also must be defined.

Applying antipassback rules, the S2000-2 takes into account all the transactions registered by other S2000-2 controllers of the Orion system but only if the transactions refer to the two access zones

assigned with the S2000-2 in question. Passages relevant to zones not assigned with the S2000-2 controller are ignored.

An antipassback rule can be made stronger by setting *Zonal Antipassback* (“Entry/Exit Control”). If this parameter is set on for an access level, the S2000-2 controller takes into account all passages of credential holders assigned to the access level to all the access zones programmed within the system. If access is requested at one of the controller readers then the antipassback rule requires that the last passage for this credential holder was to the source zone of the reader.

Thus, for example, if the controller is located on the bound between *Zone 1* and *Zone 2* and entering *Zone 2* is registered followed by entering *Zone 3* (access to which is controlled by another device of the system), an attempt to pass via the access point located between the *Zone 1* and *Zone 2* will lead to the following:

- If the *Zonal Antipassback* parameter is set on, the antipassback rule will be violated regardless of the passage direction, because the last accessed zone differs from *Zone 1* and *Zone 2*, and user presence in one of these zones is considered to be incorrect;

- If the *Zonal Antipassback* parameter is set off, the antipassback rule will not be violated by the attempt to enter the *Zone 1* and will be violated by the attempt to enter the *Zone 2*, because the controller considers the user to be located in the *Zone 2* (passage to the *Zone 3* was ignored by the controller).

The *Zonal Antipassback* parameter is in effect only if one of the antipassback modes (hard, timed or soft) is used. If the *antipassback* parameter is not used, *Zonal Antipassback* is meaningless.

The antipassback feature is included to the Access group of credential access level parameters and is programmed for each of the two readers individually (see Section 1.6).

In order to prevent a possibility of simultaneous access of several persons by means of sequential presenting of the same credential at closely located readers (for example, opening several adjacent turnstiles for pass) after granting access and until a transaction is detected, other readers of the system are locked for a short time for this credential. Namely, if access is granted for a credential presented at one of the readers and no passage has yet been logged, any attempt to present the same credential at any other reader (a reader of another controller) will violate the antipassback rule. If the hard or timed antipassback mode is used for the reader, access for this credential will be denied. As soon as actual transaction is detected, the lockout is canceled. If no passage is detected (or a passage sensor is not in use), the lockout will be canceled in a minute. While the lockout is active an access for the credential is possible only via the lane controlled by the reader where the credential was presented for the last time or through any other lane controlled by a reader where antipassback rules are not applied for this credential.

This must be taken into account while designing an access control system at the premises. If some access points exist not far from the access point where antipassback rules are applied (may be reached in one-minute walk), the other points have to be equipped with passage sensors (to generate a passing event after granting access) or the zone number 65535 has to be assigned for these access points (access granting and passage to this zone are not transferred to other system devices and do not cause lockout of other readers).

1.10 Coerced Access

The controller provides a capability to warn a security service at the premises that access or operating partitions is requested under coercion. For doing so user presents a *Duress Code* to the reader instead of a normal credential. In this case a *Duress Code Presented* message is generated and messages about granting access and transaction (if the credential is used for requesting access) are generated with the Duress Code attribute. In other respects, such credential is used as a usual one.

The controller provides two ways to present a duress code. For the first way, a user is enrolled with two credentials instead of a single one. Both credentials are registered in the controller's memory. The Credential Type parameter of the first credential is set to "User" while for the second credential this parameter is set to "Duress". Other parameters of the credentials are usually the same. In normal conditions the first credential is used, and the second credential is used under coercion.

If two-factor authentication is in use then the second way to present the duress code can be programmed. For this purpose the primary code of the user (credential) is assigned with a second, special Extra Duress Code. Usually a PIN is used as an extra credential code for two-factor authentication. So it is enough for a user to have a single primary credential and keep in memory two PINs: an access PIN and a duress PIN.

1.11 Centralized Access and Operating Partitions

If the controller operates as part of an Orion system, for all its operation modes the credentials presented to the readers of the controller can be used for centralized access (when Orion Pro workstation makes a decision about granting access) and for operating (arming and disarming) partitions (under Orion Pro workstation or S2000M panel). Moreover, the function of operating partitions can be combined both with local and centralized access.

If credentials are intended for centralized access they must not be stored in the controller's memory, so they are enrolled in the Orion Pro database (without setting the attribute of storing credentials in devices).

Credentials for operating partitions must be enrolled in the database of the panel or PC with relevant rights. Such credentials are registered in the memory of the controller only if operating partitions is combined with local access or (and) for applying validity period and time-zone limitations to credentials.

The controller switches to the mode of centralized access (centralized access or operating partitions) in the cases as follow:

- 1) Upon presenting a credential unknown for the controller. Both centralized access (under Orion Pro software) and operating partitions can be achieved in this case (under Orion Pro or S2000M panel).

- 2) If the controller is in the Ready to Arm / Disarm mode and a credential is presented which is either unknown or known but not authorized to operate the alarm loops of the controller (the Operating attribute in the access level is set off). In this case only operating partitions is enabled.

- 3) If the credential is presented which is enrolled in the controller and for which in its access level the attribute Access is set off and the attribute Operating is set on but operating the own alarm loops is not permitted. In this case only partitions can be operated.

Upon proceeding to the mode of centralized control, the controller sends the code of the presented credential to the PC (panel) while the reader LED flashes with red and green alternately five times per second until the controller receives a response from the PC or S2000M panel (it can take from fractions of a second to several seconds depending on the number of devices connected to the RS-485 interface).

If the network controller (PC) has made a decision to grant access then centralized access is granted by the same way as local access is.

If the presented credential is authorized to operate a partition then the reader LED indicates the current status of the partition in accordance with Table 2. When the credential is presented repeatedly the partition is armed (if it was disarmed) or disarmed (for all other states). Every next presenting of the credential follows in the action opposite to the previous operation, i.e. if the second presenting of the credential disarmed the partition then the third presenting will arm the partition and so on. If the credential is restricted in its rights to operate the partition, for example if only arming is permitted then a second presenting (just as the next presenting) of this credential will cause only the permitted action (arming) regardless of the current state of the partition. The time for indicating partition states by the reader LED after first and next presenting of the credential is given by the relevant configuration parameter of the controller.

If the presented credential is not known for the panel or PC or is not properly authorized then the controller indicates reject in access – the beepers of the reader and the controller issue a long Error sound, the red reader LED flashes three times and proceeds to its initial state (the quiescent mode).





If upon proceeding to the centralized access mode communication with the computer or panel is lost then the controller generates a Wrong Code message for unknown credential or an Access Denied message for a known credential. This message (just as other messages) is stored in the non-volatile memory of the controller to be sent to the PC on restoring communication.

If centralized access (arming/disarming partitions) is achieved by presenting a credential enrolled in the controller, then the controller verifies for this credential all the rules and limitations applicable to an arming/disarming credential: current activity, validity period, under two-factor authentication an extra code is requested and verified, and if the Operating attribute is set on for the access level then time zone activity is verified. If there are violations, an Access Denied message is generated and operating partitions is not implemented.

If a combined credential is presented (centralized access + operating partitions or local access + operating partitions) then access is granted for this credential. To operate partitions with this credential, the controller should be preliminary switched to the Ready to Arm / Disarm mode as well as for using combined credentials for local operating partitions (see Sections 1.16.10 and “Operating Alarm Loops” in Section 2). If the credential integrates local access and operating partitions then in the access level of this credential in addition to the Access attribute the Operating attribute can be set on for partitions to be operated without switching the controller to the Ready to Arm / Disarm mode by only keeping the credential near the reader (see Sections 1.16.10 and “Operating Alarm Loops” in Section 2).

Starting with the release 1.11, Orion Pro software supports two-factor authentication and two(three)-person access rule for centralized access.

Table 1. Indicating Partition Conditions

Partition Status	Indicator Performance	Color
Disarmed	Off	–
Arming in process... (arming delay)	Pulses five times per second	 (green + red)
Armed	On	
Intrusion Alarm, Fire Alarm, Fire Prealarm, Arming Failed	Pulses twice per second	
Trouble (in a fire partition)	Pulses once per second	

1.12 Access by ID Templates

To provide access to a wide range of persons whose credentials are difficult or impossible to enroll to the controller memory (for example, too many credentials to enroll) provided that the codes of the credentials are subject to a known rule (for example, start from a certain sequence of digits), the mechanism of access by ID Templates can be implemented.

Every template consists of a credential code and a mask that “opens” certain positions of the code. If the digits of the code of a presented credential in open positions are the same as the digits in the relevant positions of the template then access for the credential holder can be granted with the access rights specified for the template. Other digits of the code (not “open”) of the presented credential are ignored.

To limit access rights of all the credentials which match to a template, a template is associated with an access level and a validity period. Granting access for a person presenting a credential which meets rules of any template is equivalent to that for the credential which is stored in the controller memory, has access rights of the template’s access level and validity period, except for the following limitations:

- The credential can be only of User Type and cannot be “Master”;
- Antipassback rules are not monitored (for the credentials that are not stored in the controller memory passage events are not logged);
- Two-factor authentication cannot be implemented (neither a primary code nor extra code of the credential is stored in the controller memory).

When a credential has been presented to a reader of the S2000-2, the controller firstly checks whether the credential code is stored in the database. If the code is not found in the controller memory, it is compared with the first ID template, then with the second one, etc. So, if the code is stored in the controller database, the access rights set for this credential will be applied. Otherwise, if the code is not stored in the memory but meets at least one template, access rights set for this code template will be applied (for the first of the templates, if the credential code meets several templates simultaneously).

It should be kept in mind that the codes that are used for centralized access and/or arming/disarming must neither be stored in the controller memory nor meet any ID template programmed.

By default, all the five ID templates of the controller are disabled.

To enable access by an ID template do the following:

- Unlock one of the templates;
- Define a template code by reading (presenting to the reader) any card which code meets to the template or type the code manually in the configuration program (it is important to enter correctly those digits of the code which will be "open" and must match for all the credentials for which this template is intended);
- "Open" the significant positions in the code and "close" the rest positions ("opening"/"closing" is implemented by double clicking on the relevant position of the ID template in the configuration program).

A typical example of using access by ID templates is controlling access to an ATM for bank clients who have bank cards with serial numbers starting with the specified numerical sequence.

If it is necessary to grant access for all holders of cards then all position in the template should be 'covered' (no position of the code is required to be the same).

1.13 Connecting Readers

To read codes of credentials, two readers with Touch Memory, Wiegand, ABA TRACK II interface are to be connected to the controller.

The terminal sets to connect the first and the second reader to the controller are similar and are described in Table 2.

Table 2. Terminals for Connecting Readers to the S2000-2

Terminal		Input or Output	Purpose
D0	Touch Memory mode	Input/output	Data of the readers
	Wiegand mode	Input	D0 data of the reader
	ABA TRACK II mode	Input	DATA data of the reader
D1	Touch Memory mode	-	Unused
	Wiegand mode	Input	D1 data of the reader
	ABA TRACK II mode	Input	CLOCK signal of the reader
LEDG		Output	Green LED control
LEDR		Output	Red LED control
BEEP		Output	Beeper control

The digit "1" or "2" in the terminal designation means which reader the terminal is related to. For example, the control circuit of the green LED of the first reader is connected to the LEDG1 terminal of the controller.

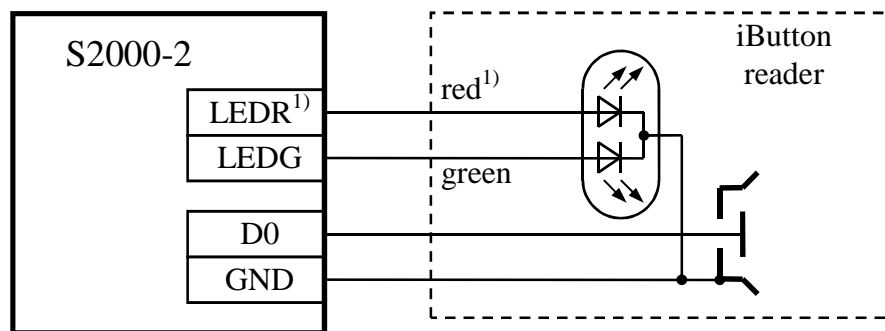
In addition to the terminals mentioned above, for convenient connecting of readers there are power voltage output contacts on the controller's PCB (" +12V1", "GND1" and "+12V2", "GND2").

This terminals can be used for connecting power circuits of readers provided that the current consumed by a reader doesn't exceed 100 mA and the length of the wires between the controller and the reader doesn't exceed 50 meters (the current and the length are an approximate values because they depend on the reader model, the cable type and cross section area, and the output interface of the reader). Readers with high current consumption and (or) located far from the controller shall be powered by a separate power supply. In this case, the "negative" circuit of the reader (commonly designated as "0V" or "GND") must be obligatory connected to the terminal GND1 (GND2) of the controller.

The main factors to limit the maximum distance between a reader and the controller is the resistance of cable wires (especially in a "GND" circuit) and the unit-length capacitance of cable (especially for the Touch Memory interface). Therefore, effective measures to ensure operability of a reader located far from the controller can be:

- Use of a cable with a large cross-section of wires;
- Use of vacant wires of the cable to duplicate the GND circuit;
- Use of a cable of a smaller capacitance (refuse to use a shielded cable);
- Use of the Wiegand interface instead of Touch Memory.

1.13.1 Connecting readers with Touch Memory interface



- 1) If the reader is equipped with a single-color LED then it should be connected with the LEDG terminal of the controller without regards to its actual color.

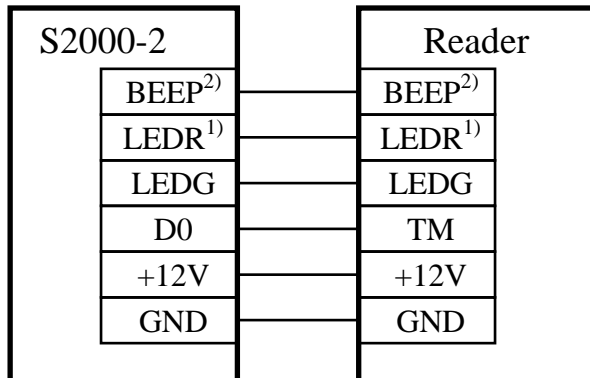
Figure 1. The Diagram for Connecting an iButton Reader

The configuration parameters of the controller shall be as follows:

- Output Interface: Touch Memory;
- LED Control Polarity: Direct (active "1").

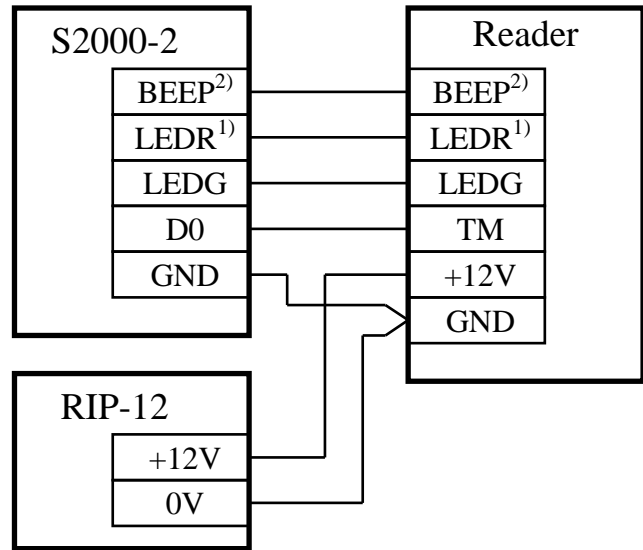
Variant 1

For readers with current consumption of less than 100 mA located within 50 m from the controller



Variant 2

For readers with high current consumption or located more than 50 m from the controller



- 1) If the reader is equipped only with a single LED control circuit then the circuit shall be connected to the LEDG terminal of the S2000-2 (the LEDR terminal is left unconnected).
- 2) If the reader is not equipped with a control circuit to control a beeper then the BEEP terminal of the S2000-2 is to be left unconnected.

Figure 2. The Diagram for Connecting a Reader with the Touch Memory Interface

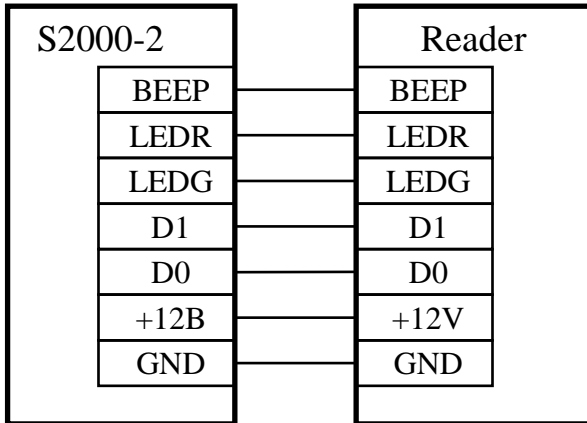
The configuration parameters of the controller shall be as follows:

- Output Interface: Touch Memory;
- LED Control Polarity depends on the reader in use, commonly it is “Direct” (active "1");
- Sounder Control Polarity depends on the reader in use, commonly it is “Direct” (active "1").

1.13.2 Connecting Readers with the Wiegand Interface.

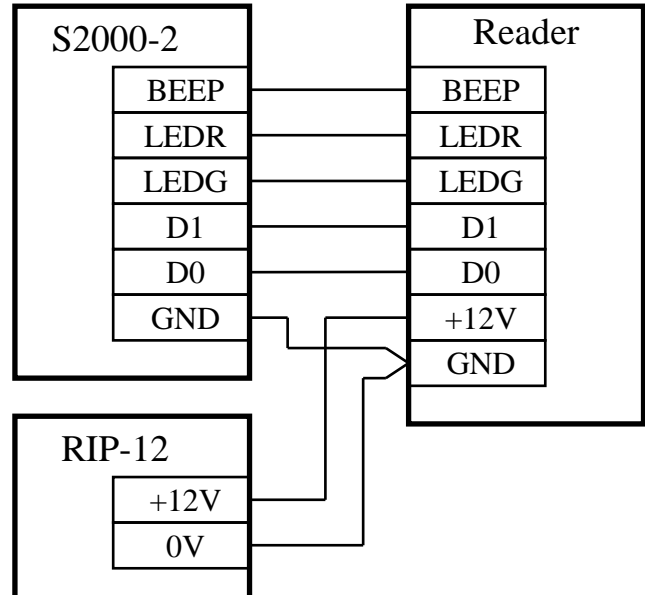
Variant 1

For readers with current consumption not exceeding 100 mA and located within 50 m from the controller



Variant 2

For readers with high current consumption or located more than 50 m from the controller



- 1) If the reader is equipped only with a single LED control circuit then the circuit shall be connected to the LEDG terminal of the S2000-2 (the LEDR terminal shall be left unconnected).
- 2) If the reader is not equipped with a control circuit to control a beeper then the BEEP terminal of the S2000-2 shall be left unconnected.

Figure 3. The Diagram for Connecting a Reader with the Wiegand Interface

The configuration parameters of the controller shall be set as follows:

- Output Interface: Wiegand;
- LED Control Polarity depends on the reader in use, commonly it is “Inverse” (active "0");
- Sounder Control Polarity depends on the reader in use, commonly it is “Inverse” (active "0")

While the read code of a credential is transmitted over the Wiegand interface, parity bits are included in data format. If the Parity Bits parameter is set to Auto (by default) then the controller by itself makes a decision about the number of parity bits in use. Another value of this parameter ("0", "1", or "2") shall be selected only if the controller determines the number of parity bits wrongly. For example, if after reading two cards with adjacent serial numbers the read codes are the same then the true number of parity bits is less than the controller has detected (for Auto mode) or than explicitly set value of this parameter. In this case the value of Parity Bits shall be corrected.

1.13.3 Connecting readers with magnetic stripe card interface ABA TRACK II is performed similarly to connecting readers with the Wiegand interface. In this case the DATA output of a reader is connected to the D0 input of the controller while the CLOCK output of the reader is connected to the "D1" input of the controller. Output Interface is set to ABA TRACK II.

1.13.4 If readers with different output interface types (Touch Memory, Wiegand-26, Wiegand-44, etc.) designed for operating with credentials of the same type are connected to S2000-2 controllers in an Orion system, then the code of a credential presented to one reader can differ with the code of the same credential presented to another reader.

For instance, the code of a Proximity card read by a reader with the Wiegand-26 interface can be not equal to the code of the same card read by a reader with the Wiegand-44 or the Touch Memory interface.

Or, for example, a PIN entered from a keypad with the Wiegand-4, Wiegand-6, or Wiegand-8 interface (every entered digit is sent to the controller apart from another) will differ from the same code entered from a reader with the Wiegand-26 or Touch Memory interface (all code digits are sent to the controller as a whole).

So, while designing and operating an access control system it is required to follow the recommendations given below.

1) Whenever possible use readers with the same data output format.

2) For readers with different interfaces use compatible formats whenever possible. For example, a Proximity card code in the Wiegand-44 format for the S2000-2 controller in most cases is compatible with the card code in the Touch Memory format, i.e. if a reader with the Wiegand-44 interface is used for entering the card code into the controller memory, the card will be recognized correctly by the controller via a reader with the Touch Memory interface and vice versa.

3) If readers have incompatible formats then it is required to restrict **Serial Number Length** by a value which is the least for all the readers used in the system. Usually readers with the Wiegand-26 interface (6 hex digits) feature the least value of the credential serial number length.

4) For remote writing of credential codes to the controller when the codes are read from a reader connected to another controller, the data format of the reader in use shall be the same as the data format of the readers connected to the programmed controller.

The format of PINs entered from readers with the Wiegand-4, Wiegand-6, or Wiegand-8 interface (every entered digit is sent to the controller apart from another) and from a PC keyboard (for **UProg** and Orion Pro Database Administrator) is the same. So, while programming an S2000-2 operating with such readers, PINs (in **UProg**) can be entered from the PC keyboard. For PIN readers with another output data formats, while programming credentials the codes shall be entered only from the keypads of the relevant readers.

The diagrams of connecting some models of readers to an S2000-2 controller are given in Appendix C.

1.14 Connecting Door Open Sensors (Passage Sensors)

The circuits for monitoring the doors (the terminals DOOR1 and DOOR2) are designed for:

- Generating a *Transaction* message upon triggering of this circuit after granting access (necessary to implement antipassback features and for correct operation of time & attendance management function in Orion Pro software);
- Implementing a flexible relay control tactics while providing access (see the configuration parameters *Switch Off When Door Is Open* and *Switch Off When Door Is Closed*);
- Generating *Door Forced Open* alarms when the door is detected to be open without granting access and *Door Held Open* alarms when the door is being open for longer than a permissible time (*Held Open Timeout*);
- Generating *Door Open* and *Door Closed* messages.

If one or more of these functions is to be implemented then using a passage sensor (door open sensor) is obligatory. If a passage sensor is in use then the *Passage Sensor* parameter should be set on for the relevant reader.

If neither of the functions mentioned above is required then for the operation modes Two Entrance Doors, One Entrance / Exit Door, and Turnstile this circuit can be not used (the terminal can be kept unconnected). In the modes Boom Barrier and Mantrap using this circuit is obligatory and the Passage Sensor parameter is considered to be always set on.

If a passage sensor is in use but it is not required to monitor the door for being forced open or propped open then the parameters *Door Forced Open Monitoring* and *Door Held Open Monitoring* respectively must be set off.

If monitoring the door for being held open is used then it is required to define the maximum permissible time for the door to be open, i.e. Held Open Timeout.

The following devices can be brought into the circuits of door open sensors:

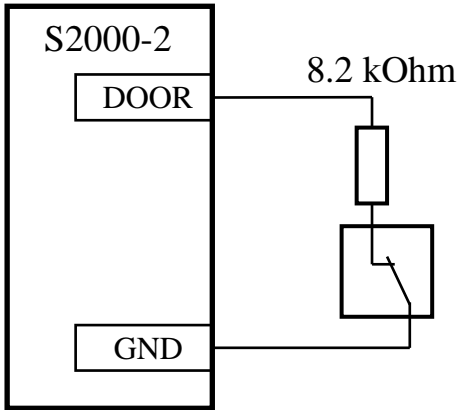
- Reed switches;
- Optical passage sensors;
- Arm rotation sensors;
- Vehicle presence loop detectors.

The controller allows connecting detectors with normally closed outputs and normally open outputs or open collector outputs. The diagrams for connecting passage sensors (door open sensors) to the S2000-2 are shown in Figure 4. For all the diagrams it is implied that in normal conditions (the door is open, the turnstile is in its initial position, no vehicle is near the boom barrier) a termination resistor of 8.2 kOhm is connected between the circuits DOOR... and GND (the voltage at the DOOR... contact relatively to the GND contact is about 36 % of the controller power voltage). In activated state of the passage sensor the circuit of the termination resistor is either open (the voltage at the DOOR... contact exceeds 50 % of the controller power voltage) or short (the voltage at the DOOR... contact is about 0 V).

In order the controller to detect a fact of passage, the detector should generate a signal of at least 50 ms duration.

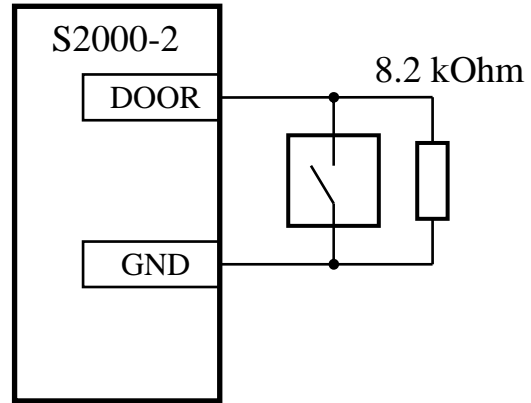
Variant 1

Normally closed with contact output
(reed switch)



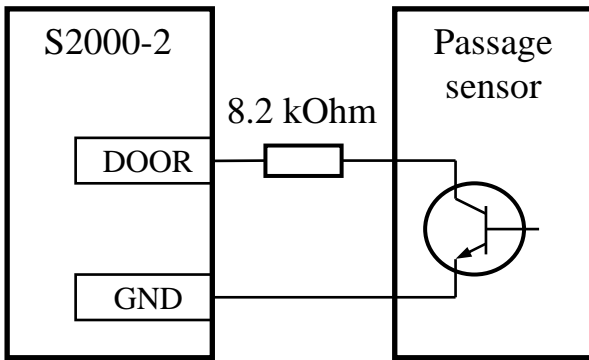
Variant 2

Normally open with contact output



Variant 3

Normally closed open collector output



Variant 4

Normally open output of the open collector type

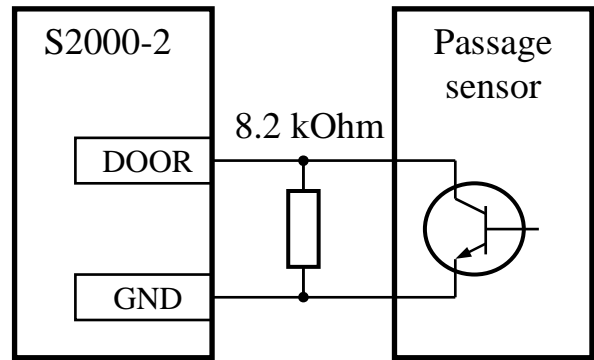


Figure 4. Connecting a Door Status Sensor (Passage Sensor)

1.15 EXIT, PERMIT (CONFIRM) and DENY Buttons

The terminals EXIT1 and EXIT2 of the controller are intended for connecting EXIT, PERMIT (CONFIRM), and DENY buttons.

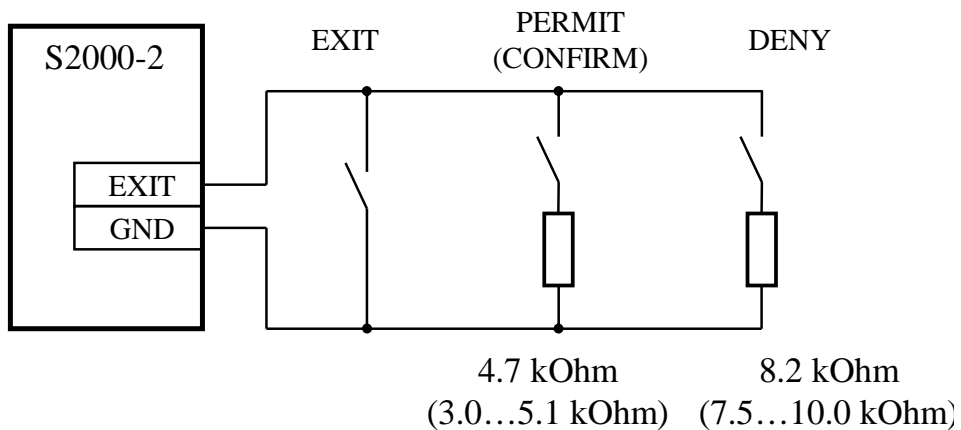


Figure 5. Connecting EXIT, PERMIT, and DENY buttons

1.15.1 An EXIT button is used for opening a door (turnstile, boom barrier) without presenting a credential. For the Two Entrance Doors operation mode the EXIT button is the only available way to unlock a door while leaving the premises. For all other operation modes EXIT buttons provide granting access to an individual who has no credential with the relevant access rights.

On pressing the EXIT button access is granted in the similar way as in case of presenting a credential aside from the fact that events about granting access followed by a passage are generated with no code of a credential ("impersonal" events).

1.15.2 A PERMIT (CONFIRM) access button is used for two purposes.

A PERMIT button is to be pressed before presenting a credential if it is necessary to authorize access and to log access for the credential which is expected to be rejected (out of time zone, not valid, violated antipassback rule, or unknown credential). Pressing the PERMIT button initiates for a single authentication the Access Allowed mode when access is granted for any presented credential and the passage is logged. In order this can be done, the configuration parameter *PERMIT Button* for the relevant reader must be set on.

A CONFIRM button is to be pressed after presenting a credential with a passage mode that is required to be confirmed manually to gain access. The passage mode "Confirmed Manually" (a parameter of access level) implies that after presenting the credential a security guard authorizes access by pressing the CONFIRM button or rejects access by pressing the DENY button.

Accordingly, the same button performs two various functions (permitting or confirming access) depending on the moment when it is pressed but for both cases it approves access. If no PERMIT button is expected to be used (or it is unacceptable) then to avoid accidental activation of the Access Allowed mode when the CONFIRM button is pressed out of time, it is advised to set the PERMIT Button configuration parameter for the reader off.

In the Mantrap operation mode no PERMIT button is in use (the relevant parameter is considered to be always off). But the CONFIRM button is to be pressed by a security guard when a person is inside the mantrap in order to authorize access and open the second door of the mantrap or to release the person through the door he has entered (The CONFIRM button of the relevant door is pressed).

1.15.3 DENY Button

The button is intended to provide rejecting access for presenting a credential with the passage mode of "Confirmed Manually".

Moreover, pressing the DENY button in a process of multi-step authentication (two-factor authentication, two-person rule, three-person rule) aborts the procedure and follows in denying access with already presented credentials.

In the Boom Barrier operation mode pressing the EXIT button closes the barrier.

1.16 Alarm Loops

The controller is equipped with two additional inputs ("Z1" and "Z2") which can be used as:

- Intrusion alarm loops (LP1, LP2);
- Inputs for commands to enable reading of credentials;
- Inputs for commands to switch the controller to the Free Pass mode.

Moreover, the circuits for connecting door open sensors ("DOOR1" and "DOOR2") can also be used as intrusion alarm loops (LP3, LP4) along with their primary function of monitoring passage sensors.

The purpose of each alarm loop is programmed by defining the configuration parameter *Loop Type*.

When LP3 and LP4 are programmed with the *Intrusion* loop type, the inputs DOOR1 and DOOR2 still can be used to monitor conditions of connected door open sensors but in addition they also can be armed. Sometimes this allows not equipping doors with additional intrusion detectors connected to another alarm loops. If no passage sensor is used in access tactics (the reader parameter Passage Sensor is set off) then not only a door open sensor but any intrusion detector can be connected to the DOOR1/DOOR2 input to operate as an intrusion alarm loop. This is always true for the DOOR2 input in the operation mode One Entrance / Exit Door, because the input in this operation mode is not used for access control purposes. The circuits "DOOR1" and "DOOR2" are always involved in access tactics in the operation modes Boom Barrier and Mantrap but this does not prohibit using them as intrusion alarm loops.

Condition of LP1 (LP2, LP3, LP4) is monitored by measuring the resistance between the Z1 (Z2, DOOR1, DOOR2) contact and the GND contact. The schematic for connecting normally closed and normally open intrusion detectors and circuits enabling reading and unlocking access to LP1 (LP2) is shown in Figure 6. The inputs DOOR1 and DOOR2 are to be connected with the detectors similarly (see Section 1.14).

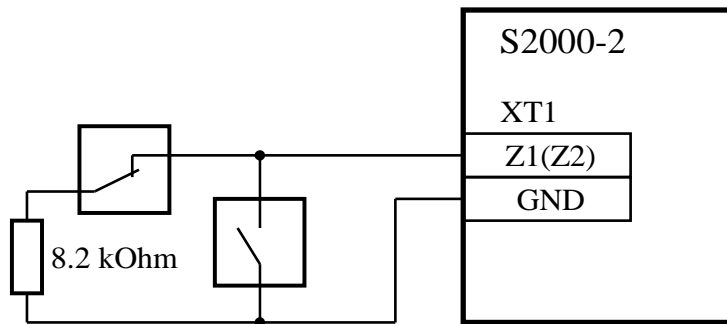


Figure 6. The Schematic for Connecting Normally Closed and Normally Open Intrusion Detectors as well as Enable Reading and Unlock Access Circuits into LP1 and LP2 of the S2000-2

1.16.1 To use LP1, LP2, LP3, or LP4 as an intrusion alarm loop, set its Loop Type to the value "Intrusion".

1.16.2 The detectors that can be connected into an alarm loop of the controller are intrusion detectors with dry contact outputs.

1.16.3 The requirements for wiring an intrusion alarm loop are as follows:

- The resistance of the wires without regard to termination resistor shall not exceed 1 kOhm;
- The leakage resistance between the alarm loop wires or between each wire and the earth shall not exceed 20 kOhm.

1.16.4 The controller provides arming an alarm loop on receiving an arming command if the resistance of the alarm loop together with the termination resistor is within the range of $2\text{ k} \pm 10\%$ to $11\text{ k} \pm 10\%$. Otherwise, the alarm loop proceeds to the Arming Failed state.

1.16.5 If the alarm loop has entered the Arming Failed state and the attribute *Auto Arming After Failure* is set on for the alarm loop then the alarm loop will automatically proceed to the Armed state as soon as its resistance is within the normal range (2 kOhm to 11 kOhm).

1.16.6 The controller issues no messages in case of an open or short circuit failure of an alarm loop for a time not exceeding 50 ms.

1.16.7 The controller issues no messages if the alarm loop resistance being within the range of 2 kOhm to 11 kOhm varies slowly with the rate of maximum 10% per hour.

1.16.8 An alarm loop is considered to be activated if it is armed and its resistance has jumped by 20% or more or it is out of the 2 to 11 kOhm range for more than 70 ms. In this case the controller generates an Intrusion Alarm message for this alarm loop.

1.16.9 If an alarm loop has entered the Intrusion Alarm status and the attribute *Auto Arming After Alarm* is set on for this alarm loop then this one will proceed to the Armed state as soon as its resistance is in norm (2 kOhm to 11 kOhm) within *Loop Recovery Time*.

1.16.10 The intrusion alarm loops can be operated (armed and disarmed) by one of the following ways:

- By presenting to the reader a Proximity card or iButton programmed in the controller with an access level with the *Operating* attribute set on which enables operating these alarm loops (local control);
- By an arming / disarming command received over the RS-485 interface from the network controller (centralized control).

To operate the alarm loops by means of a Proximity card or iButton, the credential shall be programmed in the controller configuration and assigned to an access level with the Operating parameter set on and with a given list of alarm loops to be armed / disarmed (see Table 9).

When such credential is presented to a reader, all the alarm loops operable by this credential are armed if they were disarmed or are disarmed in any other case.

While using credentials programmed both for operating alarm loops and access (combined) the controller shall be preliminary switched to the *Ready to Arm / Disarm mode* (commonly such credentials are used for access). For doing so press on the Arming Request button (see Figure 7) and hold it pressed for longer than 1 s – until the LED of the reader starts pulsing rapidly. Instead of pressing on the Arming Request button you can close both contacts of the iButton reader for the same time. After that, within 20 s while the reader LED is pulsing, the combined credential is recognized by the controller as a credential for operating. The Ready to Arm / Disarm mode is in effect only for a single presenting and terminates after presenting a credential to the reader, or upon the expire of 20 s, or after a repeated press on the Arming Request button (closing the terminals of the iButton reader).

If there are access locking alarm loops armed (see the reader parameter "Lock Access if ... Armed") then on presenting a combined credential (not switching to the Ready to Arm / Disarm mode) the alarm loops are disarmed and at the same time access is granted (if of course the credential is authorized to disarm access locking alarm loops). So, the Ready to Arm / Disarm mode is activated as usually for arming by means of combined credentials while disarming happens on the first granting access with the combined credentials.

The alarm loops can be operated by a combined card (for operating and access) without switching the controller to the Ready to Arm / Disarm mode. For doing so the parameter *Time to Hold*

Credentials for Operating should be set to a non-zero value. If a combined card is presented and kept near one of the readers for the given time then the relevant alarm loops are armed or disarmed. Presenting the card for a short time still grants access (actually the relay is activated and access event is generated with a small delay – after the card is taken away from the reader). This way to operate alarm loops can be used only for readers with Touch Memory interface. If the parameter *Time to Hold Credentials for Operating* is set to zero then this way to arm / disarm alarm loops is disabled and the controller responds immediately when a combined card is presented for access.

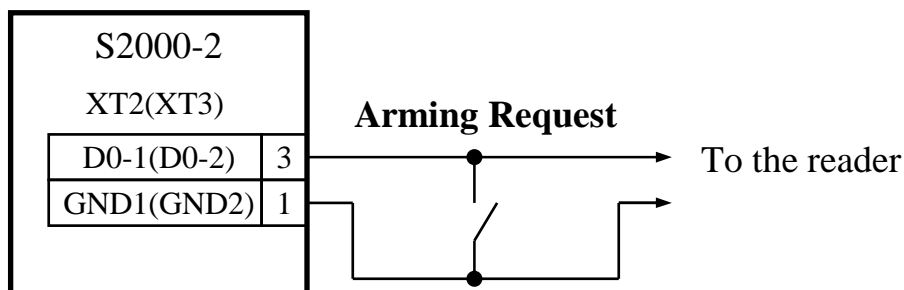


Figure 7. Connecting an Arming Request Button

Arming and disarming commands over the RS-485 interface reach the controller in case of arming or disarming from the computer, S2000M panel, or one of the Orion system devices, by using the technique of operating partitions. To operate partitions of a fire alarm or intrusion alarm system this access controller can also be used (see Section 1.1.3).

1.16.11 Alarms of the alarm loops and messages about arming, disarming, and failures to arm the alarm loops are issued by sending relevant messages over the RS-485 interface. Loop alarms can be indicated by LEDs and beepers of the controller and the readers.

To enable sounding in case of alarms in alarm loops for the controller or a reader, switch on the relevant category of sound signals for the controller or the reader respectively.

To indicate alarms of alarm loops by the LEDs of the controller and any reader set on for this reader the attribute *Indicate Alarms in LP1* (LP2, LP3, LP4).

In addition, the LED of a reader can indicate the state of one or more alarm loops by showing red light if the alarm loops are armed or by switching off if the loops are disarmed (see the *LED Quiescent Mode* parameter).

1.16.12 Each reader of the controller can be programmed in such a way that arming one or several intrusion alarm loops will lock local access via this reader (see the reader configuration parameter *Lock Access if ... Armed*).

"Armed" here is understood to mean any state of an intrusion alarm loop other than the Disarmed state (Armed, Arming Delay, Arming Failed, Intrusion Alarm).

Access is to be unlocked when the locking alarm loops have been disarmed.

If there are alarm loops locking access which are armed then on presenting a combined card (not switching to the Ready to Arm/Disarm mode) the loops are disarmed and simultaneously access is granted (if of course the card is authorized to disarm the alarm loops locking access).

1.16.13 Instead of intrusion alarm loops (LP1 and LP2) the inputs "Z1" and "Z2" can be used to deny / enable reading credentials intended for requesting access. A typical example of use of this function is connecting vehicle loop detectors (presence loops) in the Boom Barrier operation mode so that access can be granted only if a vehicle is actually standing in front of the reader.

For doing so the input(s) shall be programmed with Loop Type set to the Enable Reading value while for the reader(s) the relevant parameter(s) *Enable Reading Via...* should be set on.

Then, if the resistance of the alarm loop is in norm (2 to 11 kOhm) processing credentials which request for access is disabled (on reading the credentials denying access is indicated), but if the alarm loop is activated (the resistance is less than 2 kOhm or more than 11 kOhm) processing is permitted and presented credentials are processed properly. In processing credentials used for another purposes (Master, Operating, Unlocking, Locking) this function is ignored.

The option to enable reading via an alarm loop can be switched on or off by setting the relevant parameters for any operation mode of the controller, not only for the Boom Barrier mode.

1.16.14 In addition to the described functions of intrusion alarm loops and inputs to enable processing credentials for the readers, the LP1 and LP2 inputs of the controller can be used to switch the Free Pass mode on. This is useful for switching the Free Pass mode on and off by means of a switch or from the output of a control and indicating equipment, for example in case of a fire. (If the controller operates as part of an Orion system then to open access via the interface, control scenarios can be programmed in the S2000M panel; in this case no additional inputs or outputs of devices are to be involved).

To activate the Free Pass mode via an alarm loop, the Loop Type parameter of the alarm loop shall be set to *Open Access* and the relevant parameter *Open Access Via...* (LP1 or LP2) of the reader shall be set on.

Then, if the alarm loop resistance is within normal range (2 to 11 kOhm) the alarm loop doesn't affect operation of the access point, but after activation of the alarm loop (the alarm loop resistance has dropped below 2 kOhm or exceeded 11 kOhm) the Free Pass mode is switched on (see Section 1.4.3).

If the Free Pass mode is activated via one of the alarm loops it can be changed neither by Unlocking or Locking credential nor by a remote command via the RS-485 interface while the alarm loop is activated. The mode of controlled access can be restored on restoring the alarm loop resistance. And then the access mode can be operated both by Unlocking and Locking credentials and over the RS-485 interface.

In such operation modes of the controller as One Entrance / Exit Door, Boom Barrier, and Mantrap the Free Pass mode is switched on for both readers simultaneously (for both access directions). For the Two Entrance Doors and Turnstile modes the Free Pass mode can be switched on independently for each of the readers (as for operating via the interface or by Unlocking credential).

1.17 BUSY Input / Output

A BUSY signal is intended to lock an access point temporarily (that part of the access point which relates to a reader) from an external signal.

1.17.1 BUSY signal can be used to coordinate operation of several controllers for managing a complicated access point if while access is granted via a reader of one controller access via readers of other controllers must be locked. In this case, on presenting a credential a controller analyses the BUSY input and grants access or starts authentication procedure (with an extra code or a two-person rule) only if this one is not active. Since this moment and until the fact of passage has been registered the controller activates its BUSY output in order to lock for this time the readers of the other controllers. The "BUSY" terminal is both the input and the output of the controller. To coordinate cooperation of several controllers it is enough to interconnect their BUSY contacts (and also GND contacts if the controllers are powered by various power supplies). Moreover, the reader parameters

Receive BUSY and *Send BUSY* shall be set on in order access via this reader to be locked when access is granted via readers of other controllers and, vice versa, when access is granted via this reader readers of other controllers to be locked for a time.

1.17.2 *BUSY* signal can be used for connecting an occupancy sensor if a next access granting procedure can be initiated only after the access point is free again, for example after a person has left the mantrap or a vehicle has left the ramp at the entrance to the parking lot. An occupancy sensor with normally open contacts (which are to close when activated) is connected to the *BUSY* and *GND* terminals of the controller. In order the sensor to be monitored and its conditions were analyzed, the *Receive BUSY* parameter of the reader (or both readers) must be set on. The parameter *Send BUSY* is not required to be set on (if only the occupancy sensor is to be monitored, without coordinating operation with other controllers in the network).

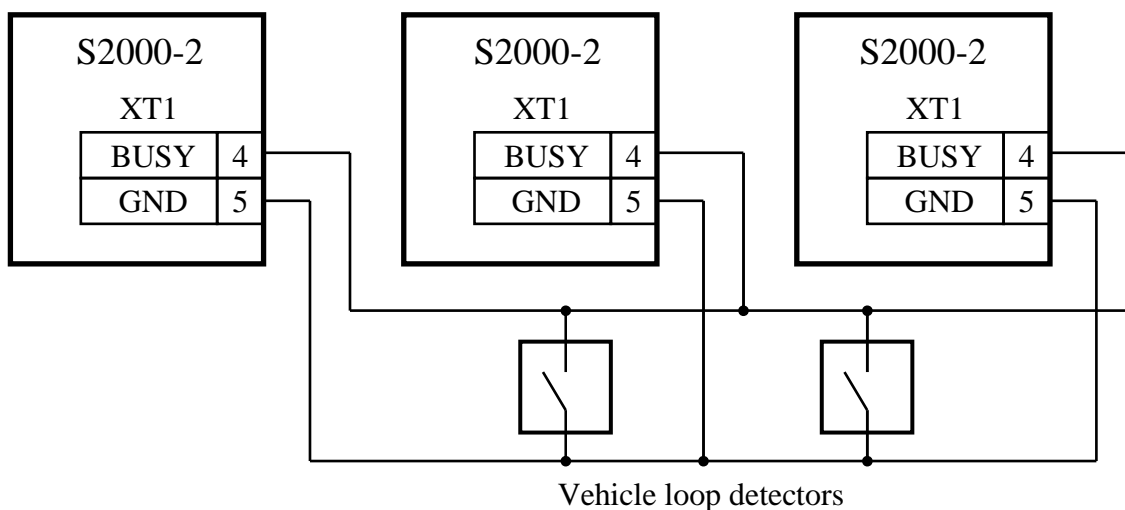


Figure 8. The Schematic for Interconnecting Controllers via Their *BUSY* Inputs/Outputs and Connecting Vehicle Loop Detectors (Occupancy Sensors)

Figure 8 shows the schematic for interconnecting three controllers to provide their coordinated operation and with connecting two presence loop detectors. Such schematic can be used, for example, for the equipment of entrance to a two-level parking. One controller controls a road side boom barrier while two other controllers control barriers at the entrances to the first and the second level. The occupancy sensors monitor the presence of a vehicle at the ramps. To prevent simultaneous entry of a vehicle to a ramp from different levels, the parameters *Send BUSY* and *Receive BUSY* must be set on for one reader of each controller (the one that allows entry to the ramp). For those readers that controls exit from the ramp these parameters must be set off.

Up to ten controllers can be coordinated in their operation by *BUSY* signal. The number of vehicle loop detectors connected in parallel is not restricted.

In addition to coordinating controllers' operation and connecting occupancy sensors, the *BUSY* input can also be used for other purposes when access should be locked via the first, the second, or both readers of a controller. As opposed to disabling a reader via an alarm loop (see Section 1.16.13), *BUSY* signal locks access not only for credentials and pressing Exit button but also access by remote commands received over the RS-485 interface. A locking circuit of dry contact type or open collector type should couple the *BUSY* circuit with the *GND* circuit.

1.18 Light and Sound Indication

The controller indicates events and conditions by its internal indicators (LEDs) and the internal beeper as well as by light and sound indicators of the readers.










1.18.1 Table 3 shows the messages indicated by READY LED of the S2000-2.

Table 3. READY LED

Event / Condition	Indicator Performance
Quiescent mode	Illuminates
Power failure (the power voltage is out of normal range)	Pulses twice per second
Programming a Master credential	Pulses in the mode of two short flashes with a long pause
Self-diagnostic mode	Pulses 5 times per second

1.18.2 Messages indicated by the internal controller indicators "1" and "2" and by light indicators of the readers are identical (duplicate) and are shown in Table 4.

Table 4. LEDs of the Readers (and "1"/"2")

Event / Condition	Indicator Performance	Color	
Quiescent mode no alarms, controlled access)	LED Quiescent Mode: 1 (Off)	Off	–
	LED Quiescent Mode: 2 or 3 (Indicate armed loops)	On when the loops are armed. Off if the loops are disarmed	
	LED Quiescent Mode: 4 (Solid red light)	On	
	LED Quiescent Mode: 5 (Solid red light when BUSY)	On if BUSY. Off if not BUSY	
Access is locked	Turns off for a short time periodically		
Access is free	Turns off for a short time periodically		
Access is permitted	Flashes once per second		
Access granted (A passage is expected)	On		
Waiting for confirmation... (The code is accepted, waiting for presenting an extra code, or pressing the CONFIRM button, or second authentication in case of two-person rule applied)	Pulses 5 times per second		
Access not granted (The credential is unknown, or an essential access rule is violated, or an access point is busy)	Three short flashes		

Event / Condition	Indicator Performance	Color
An unknown credential has been presented and a decision of the network controller is being expected...	Illuminates with red and green alternately with 5Hz frequency	 
Loop Alarm *	Pulses twice per second	
Arming Failed*	Pulses twice per second	
Centralized operating of partitions, the partition is armed	On	
Centralized operating of partitions, arming in process... (Arming Delay)	Pulses 5 times per second	
Centralized operating of partitions, the partition is disarmed	Off	–
Centralized operating of partitions, an alarm in the partition	Pulses twice per second	
Centralized operating of partitions, a trouble in the partition	Pulses once per second	
A pause between the vehicle has passed and the boor barrier is closed	Pulses twice per second	
The door is forced open (the door is open without granting access)	Pulses 5 times per second	
The door is held/propped open (the door is being open for longer than Door Held Timeout)	Pulses 5 times per second	
Waiting for closing the door after entering the mantrap or exiting it	Pulses 5 times per second	
Programming credentials	Pulses with red and green alternately twice per second	 
Programming Master-credentials	Pulses twice with red and green alternately	 
* The condition is indicated only if indication for this alarm loop is enabled for this reader		

1.18.3 The sound signals issued by the internal sounder of the controller and the beepers of the readers are similar and are shown in Table 5.

Both for the internal sounder and for the readers' beepers any category of sound signals ("Access", "Propped or Forced Open", "Loop Alarms" and "Programming") can be disabled.

Table 5. Internal Sounder and Reader's Sounders

Event / Condition	Category	Sound Signaling
Quiescent mode	–	Off
Access granted	Access	Two beeps
Access denied	Access	A long sound ("Error")

Event / Condition	Category	Sound Signaling
Under two-factor authentication condition a primary code is presented	Access	A beep
Under two-person rule access condition a first credential is presented	Access	A beep
Busy	Access	Two beeps and a long sound ("Please Wait")
Access is free (unlocked with a special credential)	Access	A beep, two beeps, two beeps ("Free Pass")
Access is locked with a special credential	Access	A long sound followed by four beeps ("Access Locked")
The normal access mode is restored with a special credential	Access	Two beeps, two beeps, a beep ("Access restored")
The door is forced open (the door is open without granting access)	Propped or Forced Open	Pulses 4 times per second
The door is propped/held open (the door is being open for more than Door Held Timeout)		
Loop Alarm	Loop Alarms	Pulses twice per second
Start of the credential programming mode	Programming	Three pairs of short sound signals ("Programming")
Exiting the mode of programming credentials	Programming	Three short and a long sound signals ("End of programming")
The mode of programming Master credential has been started	Programming	Master Programming Melody
The Master credential has been programmed	Programming	End of Master Programming Melody
A new credential is enrolled or parameters of existing credentials are changed in the credential programming mode	Programming	Two beeps ("Code Saved")
Presenting an already enrolled credential in the credential programming mode	Programming	A beep ("Credential Already Exists")

1.19 Configuration Parameters

The configuration parameters of the controller fall into seven groups:

- System Parameters;
- Reader Parameters;
- Relay Parameters;
- Alarm Loop Parameters;
- Access Level Parameters;
- Time Zone Parameters;
- Credential Parameters.

1.19.1 System configuration parameters of the controller are shown in Table 6.

Table 6. System Configuration Parameters

Parameter	Description	Range	Factory Value
Network Address	The address of the controller for communication within the RS-485 interface bus	1...127	127
Operation Mode	The fundamental parameter which defines the controller's operation	1 (Two Entrance Doors) 2 (One Entrance/Exit Door) 3 (Turnstile) 4 (Boom Barrier) 5 (Mantrap)	1 (Two Entrance Doors)
Max PIN Length	The maximum number of digits in a PIN for Wiegand readers which transmit the PIN to the controller as one digit at a time	1...12	6
Serial Number Length	Limits the number of significant bits in a serial number to be read while reading the codes of credentials. Required to insure identity of codes of a credential received from readers of different type	16...48 bits (4...12 digits)	48 bits (12 digits)
Passage Timeout	The time during which a transaction is expected after granting access	0.125...8192 s (0.125 s... ...2 h 16 min 32 s)	10 s
Barrier Close Delay	The time between vehicle's leaving and barrier's closing	0.125...31.875 s	5 s
Confirmation Timeout (Mantrap Occupancy Time)	The time to wait for pressing the CONFIRM button	0.125...8192 s (0.125 s... ...2 h 16 min 32 s)	20 s

Parameter		Description	Range	Factory Value
Sound Alarms	Access	Enables the built-in controller sounder signaling for access events, door being forced and held open, loop violation, and the credential programming mode entering respectively	On / Off	On
	Door Forced/ Held Open		On / Off	On
	Loop Alarms		On / Off	On
	Programming		On / Off	On
Guessing Protection	Number of Attempts	The number of attempts to present unknown credentials to lock the relevant reader for a time	0...255	3
	Reader Lockout Time	The time for which the reader is temporary disabled after a given number of presenting unknown credentials	0.125...8192 s (0.125 s... ...2 h 16 min 32 s)	30 s
Time to Indicate Partition Status	After Authentication	The time to display a partition status after first presenting of a credential	2...60 s	30 s
	After Operation	The time to display a partition status after second and all next presenting of the credential	2...60 s	10 s

Network Address is used to communicate data over the RS-485 interface. If the controller operates as part of an Orion system it must to be assigned to a unique address.

If one of the controller's readers is a Wiegand keypad which sends the controller codes of pressed keys one-by-one then entering a PIN is considered to be completed when the number of entered symbols reaches **Max PIN Length**. To complete entering of a shorter PIN press the "#" key (the code 0B(hex)).

The codes of the credentials stored in the controller memory have a 64-bit representation (16 hexadecimal digits), which is similar to that for codes stored in Dallas iButtons. The lower 8 bits (2 right-most hexadecimal digits) are the family code (generally 01). The high-order 8 bits (2 left-most hexadecimal digits) are used for the cyclic redundancy checksum (CRC) of the succeeding 56 bits. Located between them 48 bits (12 hexadecimal digits) represent a serial number of the credential. The **Serial Number Length** parameter enables limiting the size of the significant part of the credential serial number. This can be suitable for a system where readers with different output interfaces are used to read credentials of the same type (for example, Proximity cards). Thus, the card code received from the reader with the Touch Memory output interface (48 bits) will differ from the code of the same card received from the reader with the Wiegand-26 output interface (24 bit), causing the controller, as well as other components of the Orion system, to regard these codes to belong to two different cards. If however the value of the **Serial Number Length** parameter is set to 24 bit (6 hexadecimal digits), then on receiving the code of the card from any reader the controller the high-order bits (from 25 to 48) of the card code will be set to 0, and the code will be the same regardless of the type of the reader.

Decreasing the **Serial Number Length** value (to less than 12 hexadecimal digits) can be used while importing a credential database from any other system to the Orion system in the case if the credentials were stored with shortened serial numbers. In such case the **Serial Number Length** is to be selected according to the quantity of known digits of the credential serial numbers.

If no task said above is set, it is not advised to modify the **Serial Number Length** parameter (let it be 12 hexadecimal digits as set by default).

If this parameter is decreased for a controller which stores some previously entered codes in its memory, the UProg Configuration Tool generates a prompt asking for permission to correct existing credential codes (setting their high-order bits to zeroes and recalculating the codes' CRC). This action is irreversible, i.e. if the **Serial Number Length** is increased afterwards it will be necessary to write the codes to the controller again (for example, to load them from the previously saved file).

When access has been granted, the S2000-2 disables reading new credentials for a time equal to **Passage Timeout** and is waiting for a passage sensor response. For this time the green controller's LED is being turning on, inviting to pass. If no passage is detected then after this time green LED is turned off, and the controller is ready to process a next credential (if the relay is turned on for more than Passage Timeout then the green LED will illuminate longer). The data of the presented credential is being stored for 10 seconds after this, and if the passage sensor has been responded, then an event about the passage rather than about door forcing open will be generated. The Passage Timeout should be selected so that it will be enough for passing through (a next credential must not be operated before a passage has been logged for the previous credential) but one shouldn't wait too much for unblocking the reader if previous user didn't pass through. If no passage sensor is in use (it can be in such operation modes as Two Entrance Doors, One Entrance/Exit Door, and Turnstile) then Passage Timeout (or the time of locking the reader) is non-programmable and equal to 2 s.

In the Boom Barrier operation mode, after a vehicle has passed through (both passage sensors have returned to the quiescent mode) in order to avoid hitting of the vehicle, **Barrier Close Delay** is being kept. Red LEDs of the readers as well as the red traffic light (if connected) are flashing for this time warning about expected lowering the barrier boom.

If the passage mode for a credential implies a confirmation by pressing the button manually, then after presenting the credential the green reader LED begins flashing and **Confirmation Timeout** is being counted. If within this time a security guard presses the CONFIRM button then access will be granted while if he or she presses the DENY button then access will be rejected. If none is pressed then after expiration of Confirmation Timeout the reader returns to the quiescent mode.

In the Mantrap operation mode, after presenting a valid credential which must be confirmed by button the lock of the first door is open and Confirmation Timeout starts being counted just after a person has entered and the first door has been closed. After successful verification a security guard gets access by pressing the CONFIRM button of the second door. If within Confirmation Timeout neither the CONFIRM button nor the DENY button was pressed, the mantrap is considered to be unoccupied (if no occupancy sensor is in use) and a new access procedure in any direction can be started. If however upon expiration of Confirmation Timeout the person has still been within the mantrap, he or she can leave the mantrap only through that door through which he/she has entered because the CONFIRM button of the another door is not in effect. So, in the Mantrap mode Confirmation Timeout bounds the maximum time of person's being within the mantrap.

All sound alarms of the controller fall into four categories: **Access**, **Door Forced/Held Open**, **Loop Alarms**, and **Programming** (see Table 6). Activation of the controller's sounder for any event category is defined by relevant sound alarm configuration settings.

To protect the system against brute-force guessing (it is of importance in case of using PINs) the S2000-2 disables reading credentials for **Reader Lockout Time** if the number of fault attempts to present credentials has reached the value given by **Number of Attempts**. In this case a Guessing message is generated. The counter of invalid attempts is increased after presenting a credential which differs from the last presented one and is recognized neither by the S2000-2 nor by the S2000 panel (Orion Pro software). Presenting a valid credential resets the counter. Once having been locked, the reader is locked repeatedly on presenting a new unknown credential until a valid credential resets the counter of invalid attempts. When locking is active, no credential can be read at the reader. Guessing protection can be disabled by setting the Number of Attempts parameter to the value of zero ('No').

When a partition is operated via the S2000-2 (see Section 1.11), the partition's state is being indicated by reader LED for some time. During this time the partition can be operated. After the first presenting of the credential you should consider the current state of the partition and make a decision about further operation. The duration of the time in question is defined by the **Time to Indicate Partition Status/ After Authentication** parameter. If the partition state should be changed, the credential should be presented once more. The duration of the time for which the partition state is being indicated after repeated presenting of the credential is defined by the **Time to Indicate Partition Status/ After Operation** parameter. Within this time you can see the result of operation and probably continue operating.

1.19.2 Both of the readers have the same sets of configuration parameters shown in Table 7.

Table 7. Configuration Parameters of the Readers

Parameter	Description	Range	Factory Value
Output Interface	Defines how the read code of the presented credential is transmitted to the controller	1. Touch Memory; 2. Wiegand; 3. ABA TRACK II	1 (Touch Memory)
Time to Hold Credentials for Operating	The time a credential (card) should be kept near the reader for operating partitions (only for Touch Memory readers)	0...32 s	5 s
Parity Bits	The number of parity bits for the Wiegand format	0, 1, 2, Auto	Auto
Target Access Zone	The number of the access zone entry to which is controlled by the reader	0...65535 (65535 means that no zone is defined)	65535

Parameter	Description	Range	Factory Value
Source Access Zone	The number of the access zone where the reader is situated	0...65535 (65535 means that no zone is defined)	65535
Passage Sensor	A door open sensor is connected	On / Off	On
Door Forced Open Monitoring¹	Monitors if the door is open without granting access	On / Off	Off
Door Held Open Monitoring¹	Monitors the time the door is being open	On / Off	Off
Held Open Timeout¹	The acceptable time for the door to be open	1...255 s	20 s
Door Open Event¹	Generates a message when the door is open	On / Off	Off
Door Closed Event¹	Generates a message when the door is closed	On / Off	Off
LED Control Polarity	Selecting an active logic level to turn the LEDs of the reader on	Direct (active "1") / / inverse (active "0")	Direct (active "1")
LED Quiescent Mode	Defines the mode of LED indication in the quiescent mode	1: Off; 2: Solid red light if any of the given alarm loops is armed, otherwise is off; 3 – Solid red light if all of the given alarm loops are armed, otherwise is off; 4 – Solid red light; 5 – Solid red light when BUSY	4 (shows red light)
Indicate Armed Loop	LP1	The list of the alarm loops for which the reader indicates their having armed by illuminating of the red LED (for 2-nd and 3-rd LED Quiescent Mode)	Off
	LP2		Off
	LP3		Off
	LP4		Off

Parameter		Description	Range	Factory Value
Indicate Alarms In	LP1	The list of the alarm loops activation of which is to be indicated by the reader LED	On / Off	On
	LP2			On
	LP3			On
	LP4			On
Sounder Control Polarity		Selecting an active logic level to turn the reader's sounder on	Direct (active "1") / / inverse (active "0")	Direct (active "1")
Sound Alarms	Access	Activation of the reader sounder to indicate access events, door being forced/held open, alarms from alarm loops, and programming credentials	On / Off	On
	Door Forced/Held Open			On
	Loop Alarms			On
	Programming			On
Lock Access If Any Loop Is Armed	LP1	The list of the alarm loops to lock access when any of the loops is armed (OR-locking)	On / Off	Off
	LP2			Off
	LP3			Off
	LP4			Off
Lock Access If All Loops Are Armed	LP1	The list of the alarm loops to lock access when all of the loops are armed (AND-locking)	On / Off	Off
	LP2			Off
	LP3			Off
	LP4			Off
Enable Reading Via	LP1	If set on, credentials can be read only if the alarm loop is activated ²	On / Off	Off
	LP2			Off
Open Access Via	LP1	Activation of the alarm loop initiates the Free Pass mode ³	On / Off	Off
	LP2			Off
Send BUSY		Generates the output signal BUSY during an access procedure	On / Off	Off
Receive BUSY		Do not start a new access procedure while the external BUSY signal is active	On / Off	Off

Parameter	Description	Range	Factory Value
PERMIT Button	Process PERMIT button	On / Off	Off
<p><i>Notes:</i></p> <ol style="list-style-type: none"> 1. This parameter is effective only if Passage Sensor is set on. 2. This parameter is effective only if Loop Type is set to <i>Enable Reading</i>. 3. This parameter is effective only if Loop Type is set to <i>Open Access</i>. 			

Output Interface (Touch Memory, Wiegand, or ABA TRACK II) is set to be in agreement with the output interface of the reader connected to the S2000-2.

If the controller operates with a reader with Touch Memory interface then the parameter **Time to Hold Credentials for Operating** provides operating alarm loops by means of a combined credential without preliminary switching the controller to the Ready to Arm / Disarm Mode. In order to arm (disarm) the alarm loops, the credential should be kept near the reader within this time. To achieve access, the combined credential should be presented to the reader for a shorter time (actually the relay is switched on after a short delay, when the credential is removed from the reader).

By default (on receipt of the S2000-2 controller) **Time to Hold Credentials for Operating** is equal to zero and such way of operating alarm loops is disabled while access for the combined credential is granted without any delay (after presenting the credential, not after removing it).

If a Wiegand reader is in use then the **Parity Bits** parameter indicates how many non-significant bits the controller must discard when the code of the presented credential is received from the reader. In most cases this parameter should be set to the Auto value (the default value should be left as it is).

Every reader belongs to an access point which separates two adjacent access zones. Let us call the zone the reader is located within by the "source" access zone of the reader. But the zone access to which is controlled by the current reader (to reach which credentials should be presented to the reader) by the "target" access zone of the reader. In order antipassback (see Section 1.9), time & attendance management, and personnel location functions to operate correctly, every reader of the controller must be assigned to correct **Target Access Zone** and **Source Access Zone**. For all operation modes of the controller except for Two Entrance Doors, Source Access Zone of the first reader is the same as Target Access Zone for the second reader and vice versa. So, two zone numbers for a single reader can be given only in the mode Two Entrance Doors. For other modes, only Target Access Zone is programmed for a reader.

Not the absolute values of these numbers are of importance but these numbers must coincide for all the controllers controlled access to the same zone.

The max possible access zone number (65535) means that the zone "is not defined". The Global Antipassback rule will not be verified and the time & attendance rules will not be monitored for such zone because the zone passage events is not sent by the network controller to other access controllers. It is recommended to assign this zone number for the readers where the functions said above are not needed to lower data traffic over the RS-485 interface.

The parameter **Passage Sensor** shows that a door open sensor is in use. In this case:

- After granting access in the modes Two Entrance Doors and One Entrance / Exit Door the controller waits for a fact of transaction (opening the door) within Passage Timeout, and until the door is open or this time has been expired presenting new credentials is ignored by the controller;
- If the passage sensor has responded (the door has been open) the controller generates a Passage event;
- The door can be monitored for being forced open and propped open (see the parameters **Door Forced Open Monitoring** and **Door Held Open Monitoring**);
- The relay to control the lock can switch off before *Relay Activation Time* expires (see the parameters *Switch Off When Door Is Open* and *Switch Off When Door Is Closed*);
- Door Open and Door Closed messages can be generated.

If Passage Sensor is set off then the functions said above are unavailable, no passage is expected, and in such operation modes as Two Entrance Doors, One Entrance / Exit Door, and Turnstile the reader LED indicates a fact of granting access within Relay Activation Time but for at least 2 seconds.

If the parameter **Door Forced Open Monitoring** is set on then on opening the door without granting access a Door Forced Open alarm is generated and light and sound indication is activated.

If the parameter **Door Held Open Monitoring** is set on then when the door has been open during a passage for a time longer than **Held Open Timeout** then a door propped open alarm is generated and light and sound indication is activated.

If the parameters **Door Open Event** and **Door Closed Event** are set on then on every respond and restoring of the passage sensor the relevant messages are generated. These events are not generated in the Boom Barrier mode.

If the door has closed after being forced or propped open then a Door Closed message is generated even if Door Closed Event is set off.

LED Control Polarity defines the active logic level to control red and green LEDs of the reader. If the **Direct** control polarity is set, the high logic level is used to activate the LEDG and LEDR terminals of the controller. If the **Inverse** polarity is selected, the LEDs will be activated by low logic level.

Sounder Control Polarity defines the active logic level to control the sounder of the reader similarly to those of LED Control Polarity.

The parameters of the **Sound Alarms** group enable activation of the reader beeper for every category of sound signals (see *Light and Sound Indication*).

Switching on the parameter **Enable Reading Via LP1 (Enable Reading Via LP2)** prohibits processing of presented credentials if LP1 (LP2) is not activated (see Section 1.16.13). The credentials can be read only when the alarm loop is activated. The parameter *Loop Type* for LP1 (LP2) must be set in the *Enable Reading* value.

By default (on delivering the S2000-2 controller) the parameters **Enable Reading Via LP1** and **Enable Reading Via LP2** is set off and credentials are read regardless of the conditions of LP1 and LP2.

The parameters **Open Access Via LP1** and **Open Access Via LP2** provide usage of LP1 and LP2 for switching the reader to the Free Pass mode (see Section 1.16.14). In addition to setting these parameters on, the relevant value ("Open Access") should be selected for Loop Type of LP1 and LP2.

Setting the parameter **Send BUSY** on activates the BUSY output in the process of access at this reader (since presenting a credential and until a passage is registered). This is used to coordinate operation of several controllers (see Section 1.17).

Setting the parameter **Receive BUSY** on locks access through this reader (both for presenting credentials and for pressing RTE buttons) in case of active level at the BUSY input (closed on the ground). This is used to coordinate operation of several controllers (see Section 1.17).

Setting the **PERMIT Button** parameter on causes the controller to perceive pressing the PERMIT (CONFIRM) button to switch the reader to the Access Allowed mode for a single authentication (see Section 1.15.2).

By default the parameter is set off and this button is processed only as the CONFIRM button (the last one doesn't switch the controller to the Access Allowed mode).

1.19.3 The configuration parameters of each of the two relays of the controller are shown in Table 8.

Table 8. Relay Configuration Parameters

Parameter	Description	Value Range	Factory Value
Control Program	Defines the way to control the relay when access is being granted	3: Switch On for a Time; 4: Switch Off for a Time	3: Switch On for a Time
Relay Activation Time	Maximum duration of execution of the "opening" program to control the relay when access is being granted	0.125...8192 s (0.125 s... ...2 h 16 min 32 s)	5 s
Switch Off When Door Is Open	Aborts execution of the "opening" program as soon as the door has been open (when a transaction has been registered)	On / Off	On
Switch Off When Door Is Closed	Aborts execution of the "opening" program as soon as the door has been closed after a transaction	On / Off	Off
Send On /Off Events	Initiates (terminates) sending events on changing the relay state	On / Off	Off
Free Pass Relay Control	Defines whether the relay is operated continuously or in pulse mode in Free Pass mode	Continuous / for a time on every door closing	Continuous

Control Program defines the way for the relay to be controlled while granting access. The control program 3 ("Switch On for a Time") is used to control electromechanical locks and strikes, turnstiles, gate and barriers actuators. The initial state of the relay is "switched off" but while granting access the relay is switched on (is closed) for a given time. The control program 4 ("Switch Off for a Time") is used in general to control electromagnetic locks. The initial state of the relay is "on" but while granting access the relay is switched off (open) for a given time.

Relay Activation Time gives the maximum duration of activation the relay when access is being granted. The maximum possible time of relay activation is 2 hours 16 minutes 31.875 s while the increment is 0.125 s.

If after granting access a door has not been open when Passage Timeout has expired but Relay Activation Time has not yet expired then the green LED of the reader stays on and a passage has still been expected. However, for the operation modes "One Entrance / Exit Door" and "Two Entrance Doors" since that moment reading a next credential is enabled and if a credential is presented a new access procedure is started.

If the attribute **Switch Off When Door Is Open** is set on for the relay then on granting access the relay returns to its initial state just after the door is open (after activation of the passage sensor), before expiration of Relay Activation Time.

If the attribute **Switch Off When Door Is Closed** is set on for the relay then on granting access the relay returns to its initial state after opening and following closing of the door (after restoring of the passage sensor), before expiration of Relay Activation Time. In the Mantrap mode this parameter is considered to be always set on.

If neither of the two attributes is set then the relay is switched on (off) exactly for **Relay Activation Time** (except for the Boom Barrier mode, see Section 2.4).

When the parameter **Send On /Off Events** is set on, then any change of the relay status is transmitted as the event with specifying current performance of the relay. If not necessary, do not set this parameter on in order not to load the RS-485 interface and the event log of the controller. (These events are not yet supported for an S2000 panel but for an S2000M panel they are supported started with the version 2.05).

Free Pass Relay Control defines whether the relay is switched on (off) steadily in the Free Pass mode. In general, continuous control is used. But in case when electric strikes are in use which are open by short pulses and proceed to the "closed" state only after the door is open and then closed back, so the more suitable way to control the relay in the Free Pass mode is switching for a time when the door is being closed. In this case, when the Free Pass mode is activated the relay will be switched on for a short time (for the same time as when granting access) every time the door is closed and the lock will always be open. In the Boom Barrier mode this parameter is ignored and in the Free Pass mode the first relay of the controller is switched on continuously.

1.19.4 Configuration Parameters of Alarm Loops

The parameter **Loop Type** is programmed individually for every of the four alarm loops of the controller (inputs "Z1", "Z2", "DOOR1", and "DOOR2") and defines the function the alarm loop performs (see Section 1.16). For LP1 and LP2 ("Z1" and "Z2") Loop Type can take one of the values:

- Intrusion;
- Enable Reading;
- Open Access.

For LP3 and LP4 ("DOOR1" and "DOOR2") Loop Type can take one of the following values:

- Intrusion;
- Disabled.

By default LP1 and LP2 are assigned to the type Intrusion while LP3 and LP4 are of the Disabled type (this has no effect on using "DOOR1" and "DOOR2" to monitor passage sensors).

To enable reading or open access via an alarm loop it is necessary not only to assign the relevant loop type for the LP1 or LP2 but also to assign this alarm loop with the reader by setting the relevant reader parameter *Enable Reading Via LP1/LP2* or *Open Access Via LP1/LP2* on.

In order the input "DOOR1" or "DOOR2" to operate as an intrusion alarm loop, select the *Intrusion* loop type for LP3 or LP4 respectively.

There are a number of parameters for every intrusion alarm loop.

The parameter **Arming Delay** defines a delay for an alarm loop to proceed to the Armed status (or to the Arming Failed status if the alarm loop is being activated) after receiving a command to arm the alarm loop.

An intrusion alarm loop proceeds to the Arming Delay status under a loop arming command from the states Disarmed, Intrusion Alarm, Arming Failed. If the alarm loop has already been in Armed state then Arming Delay is ignored.

Arming Delay is programmed in seconds in the range of 0 to 255 s. The factory value is 0 for all the alarm loops.

The parameters **Auto Arming After Failure** and **Auto Arming After Alarm** enable automatic proceeding of the alarm loop to the Armed state from the states Arming Failed and Intrusion Alarm if the resistance of the alarm loop is within the normal range (2 kOhm to 11 kOhm). Proceeding from the Arming Failed status is performed just after the alarm loop resistance has been restored while for proceeding from Intrusion Alarm the alarm loop resistance should be in normal range within **Loop Recovery Time**. By default, the parameters Auto Arming After Failure and Auto Arming After Alarm are set off for all the alarm loops and Loop Recovery Time is equal to 15 seconds (the last one is of no importance when Auto Arming After Alarm is set off).

1.19.5 Authorities of every credential are given by assigning an Access Level to this credential. The rights and restrictions defined for an Access Level refer to all credentials with the types User and Duress with this Access Level. Up to 100 access levels can be described for a single controller. Every access level has two identical sets of parameters – for the first and the second reader. These parameters are shown in Table 9.

Table 9. Parameters of Access Levels

Parameter	Description	Value Range
Two-Factor Authentication	Authentication requires presenting the relevant additional credential	On / Off
Access	Access (passage) is permitted	On / Off
Access Time Zone (see Section 1.8)	The number of the time zone which defines time slots for access	0...100
Antipassback Mode (see Section 1.9)	Defines the controller's access policy in case of violation of antipassback rules	- None (not verified); - Hard; - Timed; - Soft
Lockout Period	The period of time in HH:MM format used for the Timed Antipassback mode. During this time after user's entering the target zone Hard Antipassback rule is applied while after expiration of this time Soft Antipassback rule is applied	00:30
Zonal Antipassback (see Section 1.9)	More formal checking of antipassback rules (full entry / exit control)	On / Off
Passage Mode	Defines the rules for getting access or the function of the credential	- Simple; - Confirmation; - Two-Person Rule; - Three-Person Rule; - Confirmed Manually; - Unlocking; - Locking; - Prohibited
Access Level 1 to Confirm Entry	The number of an access level to confirm entry for the two(three)-person rule	0...100
Access Level 2 to Confirm Entry	The number of a second access level to confirm entry for the three-person rule	0...100
Access Level 1 to Confirm Exit	The number of an access level to confirm exit for the two(three)-person rule	0...100
Access Level 2 to Confirm Exit	The number of a second access level to confirm exit for the three-person rule	0...100
Operating	Operating (arming / disarming) alarm loops is permitted	On / Off
Operating Time Zone (see Section 1.8)	The number of the time zone specifying the time slots when arming/disarming is permitted for holders of the credentials included in the programmed access level	0...100

Parameter	Description	Value Range
Arm LP1	Setting these switches on permits arming of the relevant alarm loops of the S2000-2 for all the credentials included into the access level	On / Off
Arm LP2		On / Off
Arm LP3		On / Off
Arm LP4		On / Off
Disarm LP1	Setting these switches on permits disarming of the relevant alarm loops of the S2000-2 for all the credentials included into the access level	On / Off
Disarm LP2		On / Off
Disarm LP3		On / Off
Disarm LP4		On / Off

The parameter **Two-Factor Authentication** directs to users with the current access level to present an extra code after presenting their primary code (see Section 1.5). Two-factor authentication is applicable both for credentials designed to achieve access and for credentials for arming / disarming.

An access level with the **Access** parameter being set on is to be assigned to credentials designed to gain access or to operate access modes.

Access Time Zone is the number of the time zone which defines the time slots when access can be achieved or operating access modes is allowed. If this number is equal to 0 then access is permitted at any time. Parameters of Time Zones with numbers from 1 to 100 can be programmed (see Section 1.8).

The parameters **Antipassback Mode** and **Zonal Antipassback** define how the controller responds to violation of the antipassback rule (see Section 1.9).

Passage Mode defines necessary conditions to achieve access to the reader target zone or a reader access mode control function.

If Passage Mode is set to Simple value then for granting access presenting a single credential is enough.

If Passage Mode is set to Confirmation then credentials with such access level can be used only to confirm access in accordance with two(three)-person rule and cannot be used for standalone access.

If the Two-Person Rule passage mode is selected (see Section 1.7) then apart from authentication of a user with this access level authentication of another user is required whose access level is **Access Level 1 to Confirm Entry**. For three-person rule authentication of once more person is required whose access level is **Access Level 2 to Confirm Entry**.

If Passage Mode is set to the Confirmed Manually value then after presenting a credential a security guard must press on the CONFIRM button to authorize access (see Section 1.15.2).

Unlocking (Locking) Passage Mode transforms a credential with this access level to a means of enabling / disabling the Free Pass (Access Locked) mode for the reader (see Sections 1.4.2, 1.4.3).

If the **Operating** parameter is set on then credentials with this access level are used to operate (arm and/or disarm) alarm loops. The parameters **Arm LP1 – Arm LP4** and **Disarm LP1 – Disarm LP4** give the list of alarm loops to be armed or disarmed respectively.

Operating Time Zone is the number of a time zone which defines time slots when arming and disarming alarm loops are permitted. If this parameter is set to zero then the alarm loop can be armed or disarmed at any time of a day (see Section 1.8).

If both parameters **Access** and **Operating** are set on for an access level then credentials with this access level are said as combined, that is they combine an access function with a function of arming / disarming alarm loops.

To operate alarm loops by means of a combined credential, the controller is to be preliminary switched to the Ready to Arm / Disarm mode or the credential is to be kept near the reader for a programmed time (see Section 1.16.10).

1.19.6 Up to 32,768 codes of credentials can be written to the database of the controller. The credentials can be iButtons, Proximity cards, PINs and so on. Every credential is described by a set of parameters shown in Table 10.

Table 10. Credential Configuration Parameter

Parameter	Description	Range
Primary Code	The unique code of a credential	8 bytes (16 hex digits)
Extra Code	An additional code presented in a process of two-factor authentication	8 bytes (16 hex digits)
Extra Duress Code	A special additional code used under coercion	8 bytes (16 hex digits)
Credential Type	Defines the purpose of the credential	- User - Master - Duress
Disabled	The credential is disabled (inoperative)	On / Off
Access Level	The number of an access level which defines common access rights and limitations for the credential	0...32
Validity	Defines whether or not the credential access rights are limited by a time	On / Off
Validity Period	Defines the effective date and time and the expiration date and time for the credential to be valid (to the exact minutes)	00:00 01.01.2000 23:59 31.12.2255

Primary Code is the value of the unique credential of a user in 8-byte format usual in Orion system (matches with the format of iButtons).

Extra Code is an additional credential used for two-factor authentication (see Section 1.5) to enhance the degree of protection against unauthorized access. In the capacity of an extra credential in most cases a PIN is used because it is more difficult to steal it or to “forget it at home”. An extra code does not have to be unique.

Extra Duress Code is a special credential which is presented (entered) instead of the relevant extra code under coercion. This code is understood by the controller as a valid extra code but a special message is generated for alerting guard service of the premises.

It makes no sense to define an extra code or an extra duress code if two-factor authentication is not in use. If the access level of a credential implies applying two-factor authentication algorithm at least at one of the readers then an extra code must be defined mandatorily while an extra duress code should be defined only if you need a feature of notification about access under threat.

Credential Type defines the destination of a credential.

The type **User** means that the credential is intended for access or for operating alarm loops (arming / disarming).

The type **Master** is intended for programming (adding) new credentials. Credentials programmed with the help of a Master credential will be of the User type.

The type **Duress** is similar to the User type but in case of presenting such credential an additional message “Duress Code” is generated (see Section 1.10).

Setting the **Disabled** switch on for a credential of any type prohibits operation of the credential. This is used to lock the credential for a time (for example, if the credential has been lost) with a possibility to enable the credential later.

Access Level (the access level number) defines access rights and access restrictions for the credential as well as rights to operate (arm / disarm) alarm loops of the controller for credentials of the User and Duress types (see Section 1.6).

The access level of a Master credential is inherited by user credentials programmed with the help of the Master (see Section 1.20).

If the **Validity** parameter is set on then the effective / expiration date and time is given by **Validity Period**. Otherwise, the credential has no expiry date. Limitations of validity period can be applied for all the types of credentials.

To change configuration parameters of the controller, please use the software utility **UProg.exe of versions 4.1.0.54 and higher** installed on a PC under Windows-98 or higher. In **UProg.exe** of earlier versions not all the configuration parameters can be available; also the number of credentials, access levels, and time zones can be limited. DO NOT use **UProg.exe** of versions less than **4.0.0.821**. To connect the controller to the COM port of the PC please use one of the interface converters PI-GR, S2000-PI, S2000-USB, USB-RS485, or an S2000 (ver. 1.20+) or S2000M panel. The last version of **UProg.exe** along with additional information can be found in Internet at the address of <http://bolid.ru> at the page of the S2000-2.

1.20 Programming Credentials

If the S2000-2 operates as part of a PC-based Orion system then PINs and codes of iButtons, Proximity cards, and other credentials are written to the controller's database (to the non-volatile memory of the controller) with the help of the *Orion Pro Database Administrator* software utility.

If the S2000-2 operates as part of an Orion system based on an S2000 panel or in standalone mode, to program credentials a PC with the **UProg.exe** software utility is used. This utility provides adding and deleting credential descriptors, setting and modifying attributes of credentials, saving a list of descriptors to a file, loading the list of credential descriptors from a file to the controller's memory and so on.

In addition, credentials can be programmed without a PC, by means of one or several Master credentials. A Master credential is any credential with the type "Master". Presenting a Master credential to a reader initiates the mode of programming credentials. Credentials presented in this mode are enrolled to the memory of the controller with the User type, inherit the access level of the Master credential, and are of unlimited validity.

One Master credential with the access group #0 can be programmed by hardware only, without a PC. For doing so, remove the controller's cover and perform a prolonged press (longer than 1.5 s) on the tamper switch of the controller, then a short-duration press (less than 0.5 s), and finally once more prolonged press. Pauses between presses should be no longer than 0.5 s. The beepers of the controller and the first reader shall play a *Master Programming* melody, the READY indicator and the LED of the first reader shall synchronously flash doubly, the reader LED shall flash with red and green alternately. If the first reader is busy (the last access procedure is being in progress) then the mode of programming Master credential is initiated for the second reader. Then, within 30 s a credential to be programmed should be presented to the reader. The beepers of the controller and the reader shall play the final part of the Master Programming melody, while the READY LED and the LED of the reader shall show solid light.

Warning: Programming a Master credential by using the tamper switch deletes all the previously programmed credential descriptors from the memory of the controller (programming Master credentials with the help of **UProg.exe** has no effect on previously programmed credentials).

Master credentials with another (non-zero) access levels can be programmed only by means of **UProg.exe**.

To switch the controller to the mode of programming ordinary credentials (intended for access) a Master credential should be presented to one of the readers of the controller. The beepers of the controller and the reader shall issue three pairs of beeps and the reader LED shall flash with red and green alternately. In this mode presented credentials are registered by the controller with the access level of the Master credential. A double-beep sound and reader green LED's illuminating for 2 s mean that a new credential code has been written to the controller or the access level of an existing credential has been changed. A single beep and reader green LED's illuminating for 1 s mean that the same credential with the same access level the Master credential belongs to has already been written to the controller. A long sound and triple flashing of the red LED mean the credential code cannot be registered by the computer (memory is full).

If the access level of programmed credentials implies two-code authentication for the reader then after presenting a primary credential the controller requests for an extra code: the LED of the reader pulses with green five times per second. After that within 30 s a credential should be presented or a PIN should be entered which will be written as an additional code for the primarily presented main code.

After adding or re-programming all the required credentials the mode of programming can be terminated by presenting **the same** Master credential which activated the programmed mode. Besides, the mode of programming credentials is terminated automatically if within 30 s no credential has been presented to the current reader. In this case the beepers of the controller and the reader issue three beeps and one long sound ("Programming is finished") while the READY LED and the LED of the reader illuminate.

If credentials with various access levels are to be added then programming the credentials with the second access level (presenting the next Master credential) should be started only after exiting from the mode of programming credentials with the first access level. Otherwise, the second Master credential will be re-programmed as a User credential with the first access level.

The hardware way of programming credentials without using a PC has the following limitations:

- No Master credential with a non-zero access level can be programmed;
- No credential with the Duress type can be programmed;
- Validity of credentials cannot be limited;
- When two-factor authentication is in use no Extra Duress Code can be programmed.

If credentials are programmed with the help of **UProg.exe**, nothing of these limitations exists. In addition, any credential can be deleted or disabled. And a possibility to add text comments for credentials (names of holders) and to save this information in a PC file (the comments are not stored in the controller) essentially facilitates the process of editing the credential list.

2 Operation

Performance of the controller is defined by the set operation mode (Two Entrance Doors, One Entrance / Exit Door, Turnstile, Boom Barrier, or Mantrap) and by the current access mode (Free Pass, Access Locked, or Controlled Access).

In the Controlled Access mode the S2000-2 operates as follows (with some differences for different operation modes).

Granting Access

To achieve access (open a door, lift a barrier boom etc.) it is necessary to present (bring up, touch etc.) to a relevant reader a credential (iButton, Proximity card, PIN) which is registered in the controller's memory with the *User* type and is designed for access or for access and operating alarm loops (combined credential).

After presenting the credential to one of its readers the controller verifies that the reader is not busy, the code of the credential is stored in the controller's database; the credential has the relevant access rights and no violations of access rules and meets all the required conditions to achieve access.

If the reader is busy or reading is disabled due to alarm loop settings then the credential is not processed:

- The beepers of the controller and the reader issue *Please Wait* signals (see Table 6);
- The red LED of the reader flashes three times.

If the credential is enrolled in the controller database, no access violation is registered for it, and the conditions for granting access are met then access is granted and:

- The sounders of the controller and the readers generate two beeps;
- The green LED of the reader switches on;
- The relay is switched on (off) to open the door (turnstile, boom barrier);
- An *Access Granted* message is generated.

If the credential is enrolled in the controller database, no access violation is registered for it, but conditions for granting access have not yet been met (two-factor authentication, two-person access rule, or manually confirmed access) then the controller is waiting for an extra code, confirming credential, or pressing the PERMIT button:

- The sounders of the controller and the reader generate a beep;
- The green LED of the reader starts pulsing five times per second;
- The relay is not activated;
- If authentication was completed (two-person access rule or manual confirmation) then an *Identification* message is generated.

If the credential is enrolled in the controller database but access rules are violated (no authorities, out of time zone, antipassback violation, expired validity period, armed alarm loops locking access) then access is denied:

- The sounders of the controller and the readers issue *Error* sound signals (see Table 5);
- The red LED of the reader flashes three times and then returns to its initial state (quiescent mode);
- The relay is not activated to grant access;

- An *Access Denied* message is generated.

If the credential is not enrolled in the controller memory and communication with the network controller is being lost (standalone operation) then access is rejected:

- The sounders of the controller and the readers generate long *Error* sounds (see Table 5);
- The red LED of the reader flashes three times and then proceeds to the initial state (quiescent mode);
- The relay is not switched on (off) to grant access;
- A *Wrong Code* message is written to the event log of the controller.

If the credential is not enrolled in the controller memory and the controller communicates with the network controller properly:

- The sounders of the controller and the readers beep;
- The code of the credential is sent to the network controller for making a decision;
- The LED of the reader flashes with red and green alternately five times per second until a decision has been made (it can take fractions of a second to some seconds).

A decision of the controller can be:

- To grant access;
- To reject access (the credential is unknown for the network controller);
- To deny access (the credential is known but has no access rights or access violations);
- To enable operating a partition (a group of alarm loops) of the fire or intrusion alarm system: the LED of the reader indicates the current partition status in amber (red + green): "Armed" (the LEDs are on), "Arming in process..." (the LED flashes five times per second), "Disarmed" (the LEDs are off), "Alarm" (the LED flashes twice per second), "Trouble" (the LED illuminates for a short time once per second).

Granting access, denying access and rejecting access centrally (in accordance with the decision of the network controller) are indicated similarly to these procedures for local access.

In the mode of operating a partition the reader LED indicates the current state of the partition (illuminates with amber, flashes with amber, or is switched off – see Table 1) while every next presenting of the credential inverts the current status of the partition (if it was disarmed then the partition is armed, otherwise the partition is disarmed). A partition state is being indicated by the reader LEDs for some time (programmed by the relevant configuration parameters) or until another credential is presented.

Pressing the EXIT button causes granting access but Access Granted messages are generated without a credential code ("impersonal").

If after granting access within Passage Timeout or Relay Activation Time (if the last value is more) the door open sensor (passage sensor) responds then a *Transaction* message is generated, otherwise the access is considered to be unimplemented and the controller starts waiting for a new access procedure. In both cases (in case of a transaction has happened or the timeout has expired) the green LED switches off and the reader LED returns to the quiescent mode (switches off, illuminates with red or indicates the partition status).

Operating Alarm Loops

To arm / disarm alarm loops by means of a credential intended for this reader only for these operations (a User-type credential with the enabled Operating and disabled Access parameters in its access level) it is necessary just to present the credential at this reader of the controller.

The controller verifies whether the credential is registered in its database, authorities of the credential to operate alarm loops, current activity its time zone for operating alarm loops, and whether authentication has been completed (for two-factor authentication one more code must be presented).

If the right to operate alarm loops is verified and all alarm loops controlled by the credential are disarmed then these alarm loops will be armed but if at least one alarm loop is disarmed then all alarm loops will be disarmed.

If loops are being armed the reader LED switches on for 2 seconds with amber (green + red). If loops are being disarmed then the reader LED switches off for 2 seconds.

To operate alarm loops by means of combined credentials (Access + Operating, Unlocking + Operating, Locking + Operating) the controller must be previously switched to the Ready to Arm / Disarm mode. For doing so, prior to presenting the credential press the Arming Request button (see Figure 7) and hold it pressed for more than 1 s until the reader LED starts flashing rapidly. Instead of pressing the Arming Request button the terminals of the Touch Memory reader can be closed for the same time. Then, as long as the LED is flashing (within 20 s) a combined credential is considered by the controller as the credential for operating.

For the readers with the Touch Memory interface, for arming / disarming alarm loops the combined card (credential) can just be kept near the reader within **Time to Hold Credentials for Operating**. In this case to switch the controller to the Ready to Arm / Disarm mode is not required. At the time of holding the card the reader LED pulses with amber four times per second and after the expire of **Time to Hold Credentials for Operating** the alarm loops will be armed (the reader LED will turn on for 2 s) or disarmed (the reader LED will switch off for 2 s). If the card is removed before expiration of **Time to Hold Credentials for Operating** the main function of the card will be implemented: granting access or unlocking / locking access.

Unlocking and Locking Access

To activate Free Pass mode or Locked Access mode for a reader the controller (see Section 1.4), present at this reader a User-type credential with an access level with set on Access attribute and the passage mode *Unlocking* or *Locking* respectively.

If the Free Pass mode is activated then the sounder plays a sequence of sounds "Free Pass" (see Section 1.18.3) while the reader LED illuminates with green turning off for a short time periodically.

If the Access Locked mode is activated then the sounder plays the sequence of sounds *Access Locked* (see Section 1.18.3) while the reader LED illuminates with red turning off for a short time periodically.

If in the Free Pass mode a credential intended for access is presented then after opening the door (rotation of the turnstile arm) a *Transaction* event is generated.

Presenting Unlocking or Locking credential in the modes Free Pass and Access Locked restores the Controlled Access mode.

In case of free access a door (turnstile gate, boom barrier) is always open for access (without authentication and logging passages).

When access is closed, access can be achieved only by pressing the EXIT button or switching the reader to the Access Allowed mode for a single transaction.

The Access Allowed mode can be activated with the help of a switch (stick button) brought into the LP1 or LP2 of the controller. For doing so, Loop Type should be set to the value "Open Access" and the reader parameter Open Access via LP1 or Open Access via LP2 should be set on. As long as the alarm loop is being activated (the button is being pressed) access is being open while on restoring the alarm loop the Controller Access mode is restored.

Allowing Access

To allow access one time with logging the transaction by the credential, the PERMIT button is to be pressed for a short time. The reader LED illuminates for a short time once per second in green. Any credential presented within 10 seconds after that achieves access. Then the reader returns to a previous access mode.

By default the PERMIT button is inoperative; to activate it set the parameter *PERMIT Button* on.

In the Mantrap mode the PERMIT button is inoperative even if the parameter is set on.

Presenting a Master credential initiates the mode of programming credentials (local programming, see Section 1.20).

2.1 Two Entrance Doors Mode

2.1.1 In this operation mode the S2000-2 controls access through two independent access points (doors) provided that granting access in one direction requires presenting credentials while to grant access in the other direction an EXIT button is pressed.

The recommended setting for Passage Timeout after granting access is 10 seconds.

2.1.2 The diagram for connecting the S2000-2 in the Two Entrance Doors operation mode is shown in Figure 9.

Equipment for the first door (a reader, a lock, an EXIT button, a door open sensor) is connected to the terminals of the controllers with the digit "1" at the end of their marking. Equipment for the second door is connected similarly – to the controller terminals with "2" at the end of their marking.

The electromagnetic lock (electric strike) can be powered by the same power supply as the controller or from a separate power supply. In case of powering by the same power supply the input power circuits of the controller and input power circuits of the lock must be separate pairs of wires which are connected only at the power supply terminals.

If the lock is not equipped with a circuit for suppression of high-voltage pulses generated during commutation then a reverse switched diode must be connected at the lock terminals in parallel with the lock's winding (the admissible direct current of the diode must not be less than operating current of the lock).

If the readers are powered by another power supply then "GND" circuits of the controller and the readers must be coupled.

To open the lock for passing through the doors in another direction, EXIT buttons are used.

If mechanical or electrical buttons or other appliances are in use which can open the lock bypassing the controller then the Door Forced Open Monitoring and Door Held Open Monitoring parameters must be set off to avoid false forced door open or propped open alarms.

A passage sensor can be missed. In this case:

- Passage events are not generated;
- On granting access the relay is switched on for a time given by Relay Activation Time regardless of the values of the parameters Switch Off When Door Is Open and Switch Off When Door Is Closed;
- The doors cannot be monitored for being forced open or held open;
- On granting access the green LED of the reader illuminates within the time of activation of the relay (but at least two seconds) regardless of the actual time the passage takes.

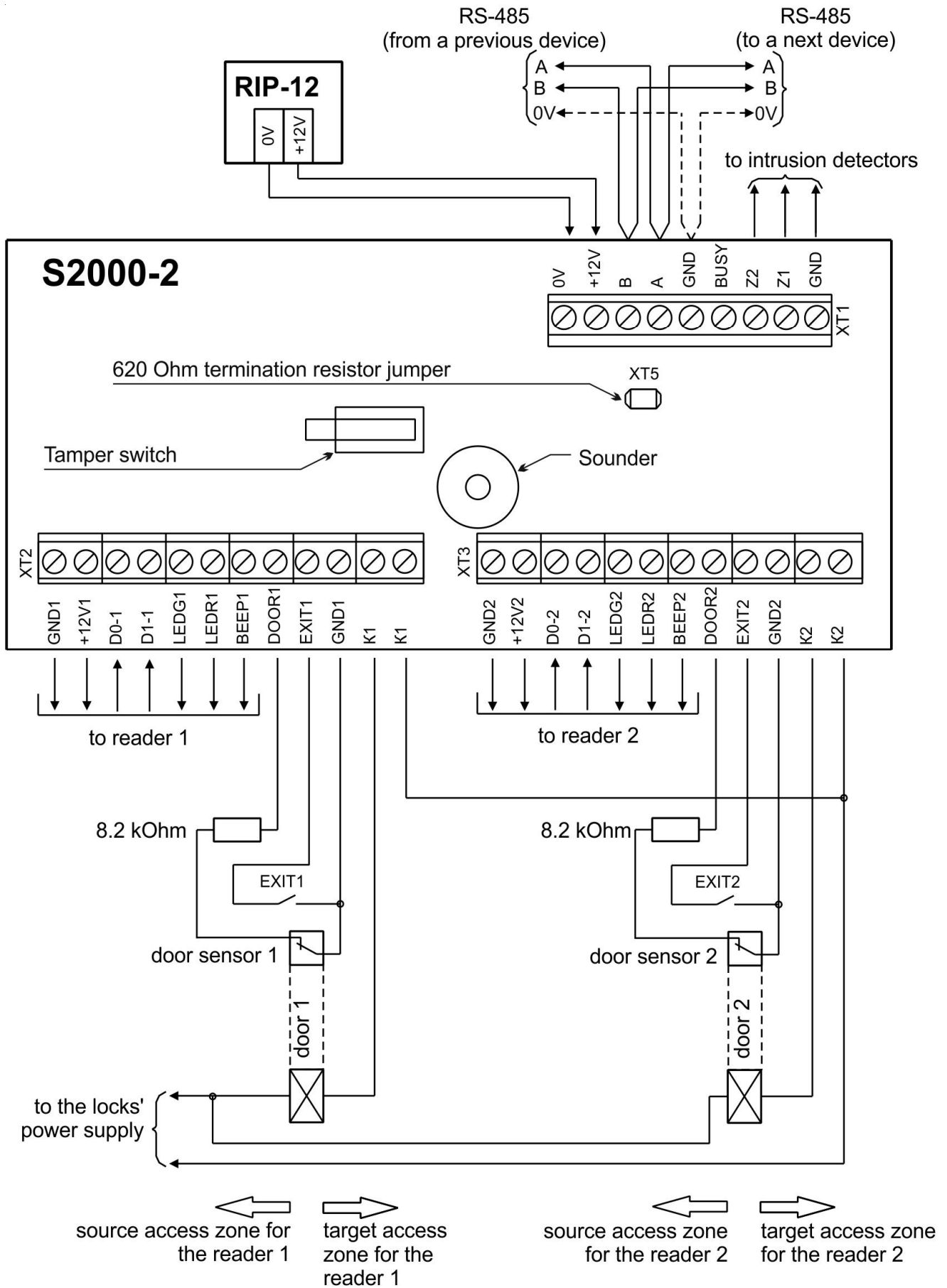


Figure 9. Connection Diagram for the Controller in the Two Entrance Doors Mode

2.1.3 Configuration Settings

- 1) Set the operation mode of the controller to the Two Entrance Doors value.
- 2) Set the value of the Passage Timeout (10 s is advised).
- 3) If a door sensor is in use then set the Passage Sensor parameter on, else set it off.
- 4) If electric strikes are in use then for each relay set:
 - Control Program to the value 3 (Switch On for a Time);
 - Relay Activation Time to 1...5 seconds (the time enough for the strike to operate);
 - The relay parameter Switch Off When Door Is Open to the value “On” (for the strike to be latched correctly in case of a fast passage).Otherwise, if magnetic locks are in use then for each relay set:
 - Control Program to the value 4 (Switch Off for a Time);
 - Relay Activation Time to the value of Passage Time (10 s is advised);
 - One of the relay parameters Switch Off When Door Is Open and Switch Off When Door Is Closed to the value "On" (to lock the door just after completing a passage).

Other settings depend on the specific operation conditions.

2.1.4 Operation

To achieve access in forward direction, a User-type credential with the set Access attribute is to be presented to the reader installed in front of the door.

If authentication has succeeded the reader sounder beeps twice, the green LED starts illuminating, the door can be open (is unlocked), and an Access Granted message is generated with the code of the presented credential.

If for the access level of the credential two-factor authentication is to be applied at this reader (for this door) then the green LED of the reader starts flashing five times per second and access can be granted only after presenting an extra code (see Section 1.5).

If for the access level of the credential a two(three)-person rule is applied then access can be granted only after authentication of all the participants (two or three ones) of the procedure having specific access levels (see Section 1.7).

After the door has been open the reader LED proceeds to the quiescent mode (the red LED switches off or on) and a Transaction message with the code of the presented credential is generated.

If no door open sensor is in use then on granting access the green LED of the reader switches on for the time of relay activation but at least for 2 seconds.

To open a door on passing in opposite direction an EXIT button installed in front of the door within the premises is to be pressed. In this case the reader sounder beeps twice, the green LED starts illuminating, the door is open (unlocked), and an Access Granted message without specifying a credential code (impersonal) is generated. After opening the door a Transaction message without specifying a credential code (impersonal) is generated.

Access through the second door is achieved by the same way.

2.2 One Entrance / Exit Door

2.2.1 In this mode the S2000-2 controls access through one access point (door) which has a common circuit to control a locking device provided that granting access in both directions requires presenting credentials at the readers installed on both sides of the door.

EXIT buttons also can be used to achieve access, for example for remote opening the door from a guard post.

The recommended setting for Passage Timeout after granting access is 10 seconds.

In this mode antipassback functions can be used because authentication is performed on passages in both directions. But an ordinary door doesn't provide registering all the passages (on granting access for a single credential several persons can achieve access).

2.2.2 The diagram for connecting the S2000-2 in the in the One Entrance / Exit Door mode is shown in Figure 10.

To control the lock and to monitor the door open sensor, the first channel of the controller is used. The second relay and the circuit monitoring the second door open sensor are dormant. The second relay can be controlled by commands over the RS-485 interface from a PC or S2000M panel.

ENTRY and EXIT buttons are connected if necessary, for example for granting access from a guard post.

The electromagnetic lock (electric strike) can be powered by the same power supply as the controller or from a separate power supply. In case of powering by the same power supply the input power circuits of the controller and input power circuits of the lock must be separate pairs of wires which are connected only at the power supply terminals.

If the lock is not equipped with a circuit for suppression of high-voltage pulses generated during commutation then a reverse switched diode must be connected at the lock terminals in parallel with the lock's winding (the admissible direct current of the diode must not be less than operating current of the lock).

If the readers are powered by another power supply then "GND" circuits of the controller and the readers must be coupled.

A passage sensor can be missed. In this case:

- Passage events are not generated (antipassback rules cannot be applied);
- On granting access the relay is switched on for a time given by Relay Activation Time regardless of the values of the parameters Switch Off When Door Is Open and Switch Off When Door Is Closed;
- The doors cannot be monitored for being forced open or held open;
- On granting access the green LED of the reader illuminates within the time of activation of the relay (but at least two seconds) regardless of the actual time the passage takes.

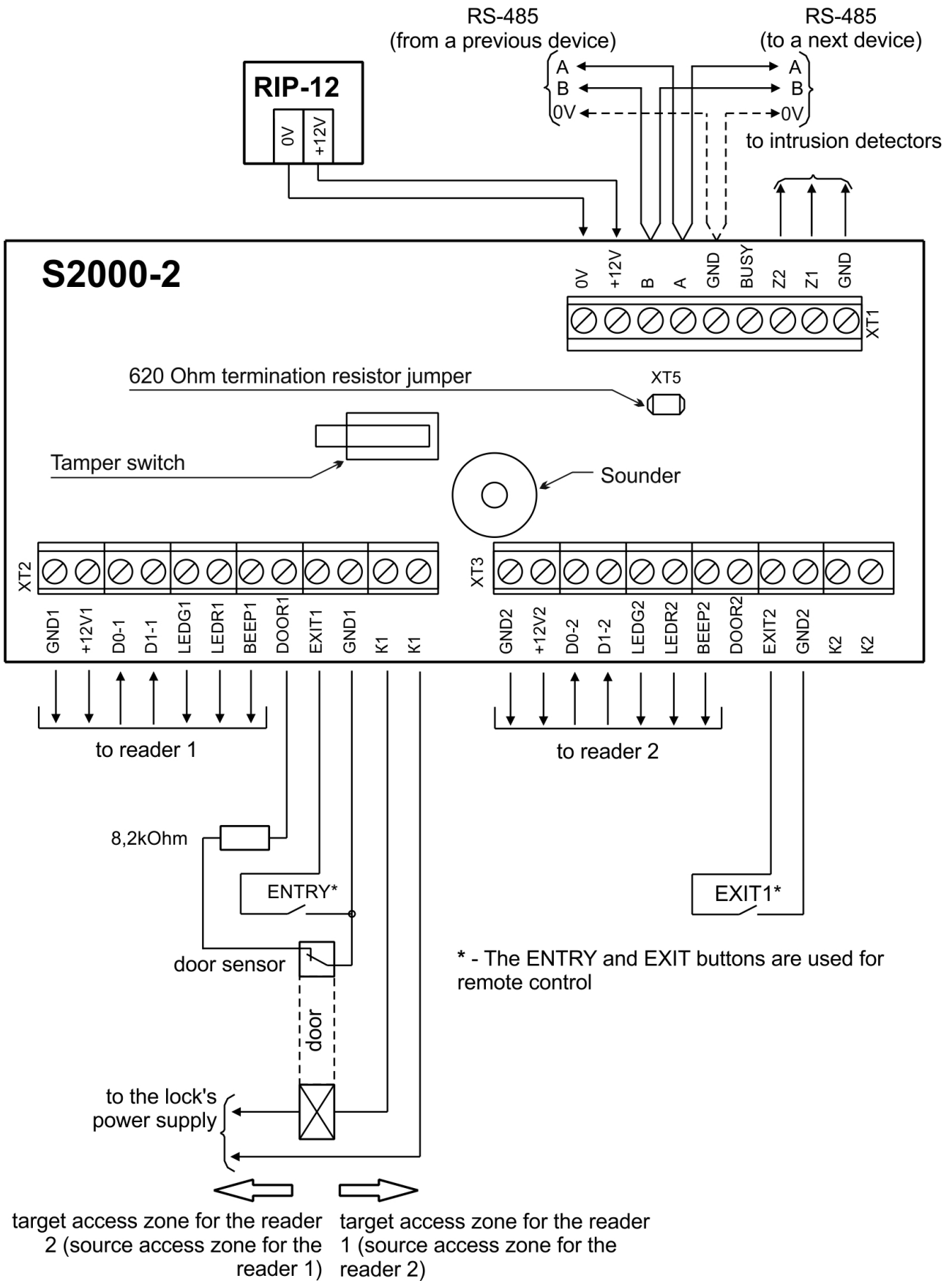


Figure 10. Connection Diagram for the One Entrance/Exit Door Mode of the Controller

2.2.3 Configuration Settings

- 1) Set the operation mode of the controller to the value "One Entrance / Exit Door".
- 2) Set the value of the Passage Timeout (10 s is advised).
- 3) If a door sensor is in use then set the Passage Sensor parameter on, else set it off.
- 4) If an electric strike is in use then set:
 - Control Program to the value 3 (Switch On for a Time);
 - Relay Activation Time to 1...5 seconds (the time enough for the strike to operate);
 - The relay 1 parameter Switch Off When Door Is Open to the value "On" (for the strike to be latched correctly in case of a fast passage).Otherwise, if a magnetic lock is in use then set:
 - Control Program to the value 4 (Switch Off for a Time);
 - Relay Activation Time to the value of Passage Time (10 s is advised);
 - One of the relay 1 parameters Switch Off When Door Is Open and Switch Off When Door Is Closed to the value "On" (to lock the door just after completing a passage).
- 5) If Global Antipassback or time & attendance monitoring is in use then select correct Target Access Zone values for both readers.

Other settings depend on the specific operation conditions.

2.2.4 Operation

To achieve access in both directions at the reader installed in front of the door a User-type credential with the Access attribute is to be presented.

If authentication has succeeded the reader sounder beeps twice, the green LED starts illuminating, the door can be open (is unlocked), and an Access Granted message is generated with the code of the presented credential.

If for the access level of the credential two-factor authentication is to be applied at this reader then the green LED of the reader starts flashing five times per second and access can be granted only after presenting an extra code (see Section 1.5).

If for the access level of the credential a two(three)-person rule is applied then access can be granted only after authentication of all the (two or three) participants of the procedure having specific access levels (see Section 1.7).

After the door has been open the reader LED proceeds to the quiescent mode (the red LED switches off or on) and a Transaction message with the code of the presented credential is generated.

If no door open sensor is in use then on granting access the green LED of the reader switches on for the time of relay activation but at least for 2 seconds.

To achieve access in another direction the procedure is similar but applying two-factor authentication and two(three)-person access rules is programmed for the access level individually for each reader (each passage direction).

2.3 Turnstile Mode

2.3.1 In this mode the S2000-2 controls access through a single access point (an electromechanical turnstile) with a separate control circuit for each passage direction provided that granting access in each direction requires presenting credentials at readers installed on the relevant sides of the turnstile.

EXIT and PERMIT buttons can also be used to grant and permit access remotely from a guard post.

The recommended Passage Timeout after granting access is 10 seconds.

In this mode antipassback functions can be used because authentication is performed on passages in both directions and on granting access once only one person can achieve access.

2.3.2 The schematic for electric connections of the S2000-2 in the Turnstile operation mode is shown in Figure 11.

This schematic implies that access for entry and exit is granted by closing the relevant pairs of contacts of the turnstile designated in the figure as ENTRY and EXIT.

The schematic shows connecting passage sensors with normally open dry-contact outputs (which are closed on passing). Connecting passage sensors (arm rotation sensors) with another type of output is discussed in Section 1.14. There can be both separate sensors and outputs of turnstile control circuits.

If a turnstile is equipped with a single arm rotation sensor which responds for any passage direction then it is to be connected in parallel to the relevant inputs of both channels of the controller as shown in Figure 12.

Correctness of connecting passage sensors can be checked easily if the reader parameters LED Quiescent Mode are set to the recommended value "1-Off". Then in initial state of the turnstile the LEDs of the readers as well as the "1" and "2" readers of the controller should be off. Any passage sensor having actuated (the turnstile arm having rotated), red LEDs shall illuminate.

To control the turnstile manually, buttons connected to the EXIT1 and EXIT2 terminals of the controller are used. Granting access by pressing buttons manually and following passages are logged by the controller and can be seen in the event log of the Orion Pro Workstation or S2000 panel. If a control connected immediately to the turnstile is used for granting access manually, bypassing the controller then facts of granting access will not be logged.

If the readers are powered by a separate power supply then the GND circuits of the controller and the readers must be coupled.

It is acceptable not to use passage sensors (arm rotation sensors). However in this case no passage events are generated and antipassback and time & attendance functions for Orion Pre software cannot be used. Moreover, the minimum time for a passage in this case is two seconds (only after the expiry of this time the controller can process a next credential). If a passage sensor is in use then turnstile throughput can be higher, because the next credential will be taken into account by the controller just after registration of the passage and returning the sensor into initial state.

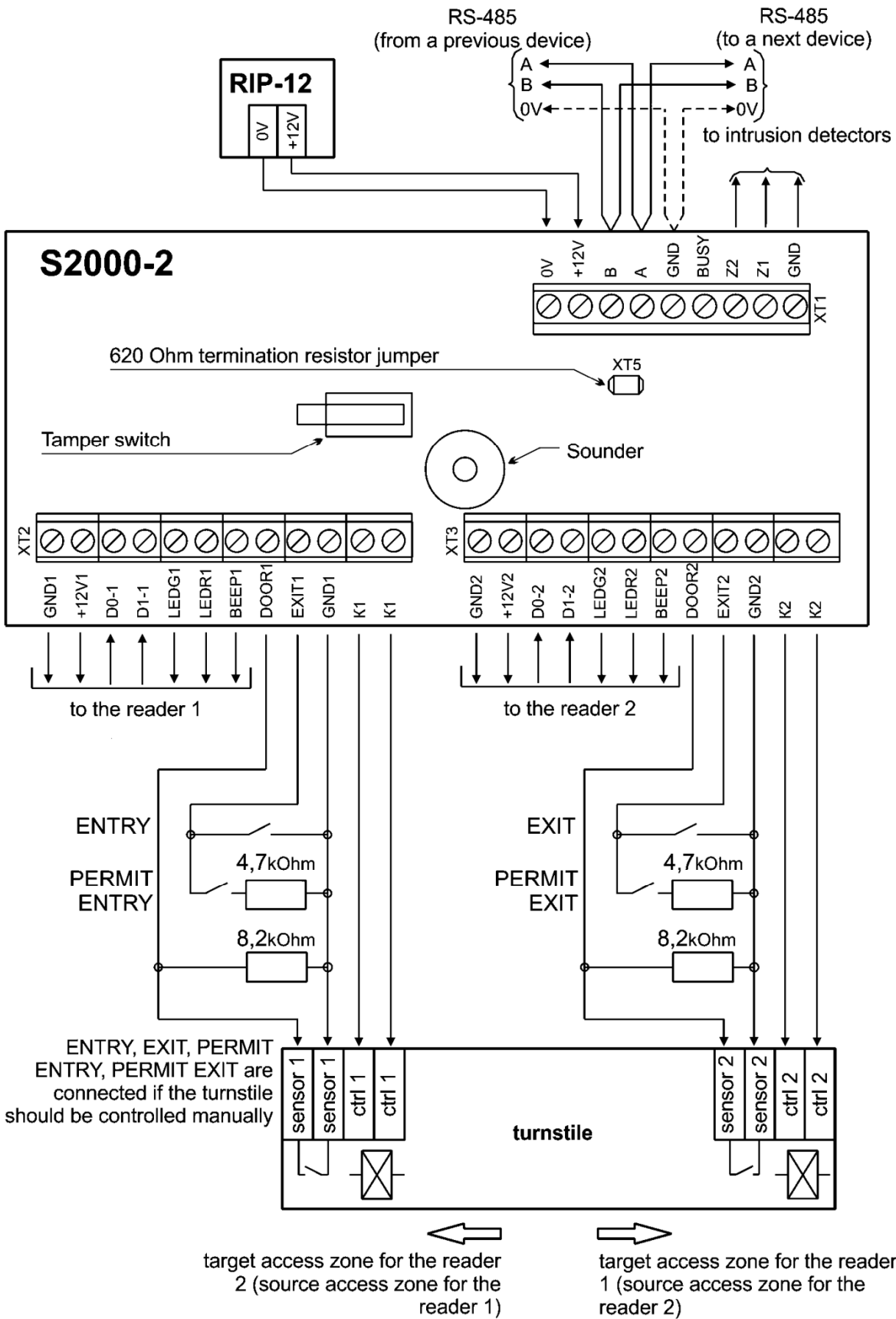
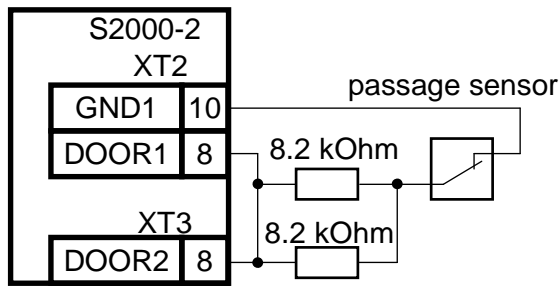
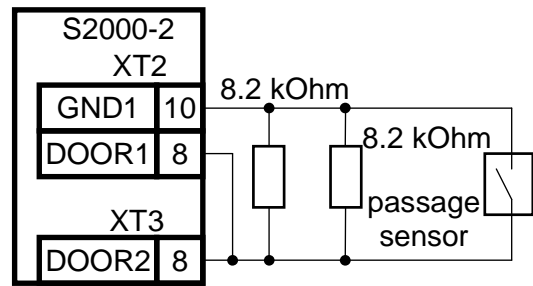


Figure 11. Hardware Connections for the S2000-2 in the Turnstile Operation Mode



Connecting a single passage sensor with normally closed contacts



Connecting a single passage sensor with normally open contacts

Figure 12. Connecting a Single Passage Sensor (Arm Rotation Sensor)

2.3.3 Configuration Settings

- 1) Set the operation mode of the controller to the value "Turnstile".
- 2) Set the value of the Passage Timeout (5 to 10 s is advised).
- 3) If a passage sensor (arm rotation sensor) is available then set the Passage Sensor parameter on else set this one off.
- 4) Set the parameters Door Forced Open Monitoring and Door Held Open Monitoring off.
- 5) Set the Control Program to 3 ("Switch On for a Time").
- 6) Set Relay Activation Time for both relays to 0.25...1 s (enough to enable turnstile rotation for a single passage).
- 7) For both readers set LED Quiescent Mode to "1-Off".
- 8) When Global Antipassback or time & attendance function is in use then give correct Target Access Zone values for both the readers.
- 9) To use PERMIT ENTRY and PERMIT EXIT buttons set the parameter PERMIT Button on for both the readers.

Other settings depend on the specific operation conditions.

2.3.4 Operation

Ensure that the LED of the reader installed in front of the turnstile is switched off (the turnstile is ready) and present a credential with the Access attribute.

If authentication has succeeded then the reader LED beeps twice, the green LED of this reader and the red LED of the another reader start illuminating, the turnstile is unlocked for a single passage in the given direction, and an Access Granted message is generated with the code of the presented credential.

After the passage sensor has actuated the green LED of the reader change its light color for red and a Transaction message with the code of the presented credential is generated.

After restoring of the passage sensor (completing of the turnstile rotation) the LEDs of both readers are switched off and this means that the turnstile is ready for passing in any direction.

The procedure of passing in the other direction is similar to that said above.

2.4 Boom Barrier Mode

2.4.1 In this mode the S2000-2 controls bi-directional access through a single access point – a gate barrier with a single boom for both travel direction. The relay 1 of the S2000-2 opens the boom (lifts it) while the relay 2 closes it (lowers this one). Granting access in both directions requires presenting credentials at the readers located on both sides of the boom barrier.

EXIT buttons also can be used to grant access remotely, for example from the guard post.

The recommended Passage Timeout after granting access is 30 seconds.

In this mode antipassback functions are available because authentication is implemented on passages in both directions.

To increase mimic resistance, the alarm loops can comprise vehicle presence sensors located at the reader zones. In this case credentials are processed by the controller only if only a vehicle stands near the reader.

2.4.2 The diagram for connecting the S2000-2 in the Boom Barrier operating mode is shown in Figure 13.

This diagram implies that opening (lifting) the barrier is implemented by closing the contacts at the control unit of the boom barrier designated as "open" while closing (lowering) the barrier is implemented by closing the contacts of the control unit designated as "close". If to control the boom barrier more than 30 V voltage, or more than 7 A current, or more than 100 W wattage need to be commutated then at the controller output relay amplifiers such as UK-VK must be added. In this case the controller relay contacts will commutate the contacts of a more powerful relay while the contacts of that relay will commutate power of the boom barrier motor drive.

If a single opening relay is required to control the boom barrier (the barrier lowers automatically after a lifting command terminates) then only the relay 1 of the controller is in use. The relay 1 activation time in this case should be set no less than the time of expecting a passage to prevent lowering the boom barrier on a vehicle (the relay 1 is switched on until the vehicle has moved from under the barrier).

Vehicle passage sensors, in addition to registering travelling, protect the vehicle against lowering the barrier on them. As long as at least one sensor is being activated the barrier is not closed. For this reason, sensors (generally optical beam detectors are in use) are located from both sides of the boom barrier in order any vehicle standing under the boom barrier to cause actuation of at least one sensor. Protection against lowering the barrier on a vehicle is in effect starting with issuing a command to open the barrier and until the barrier has been lowered (until the time of activation of the second relay has been expired).

The diagram shows how to connect detectors with normally closed dry-contact output (which opens during a passage). Connecting detectors with another type of output is discussed in Section 1.14.

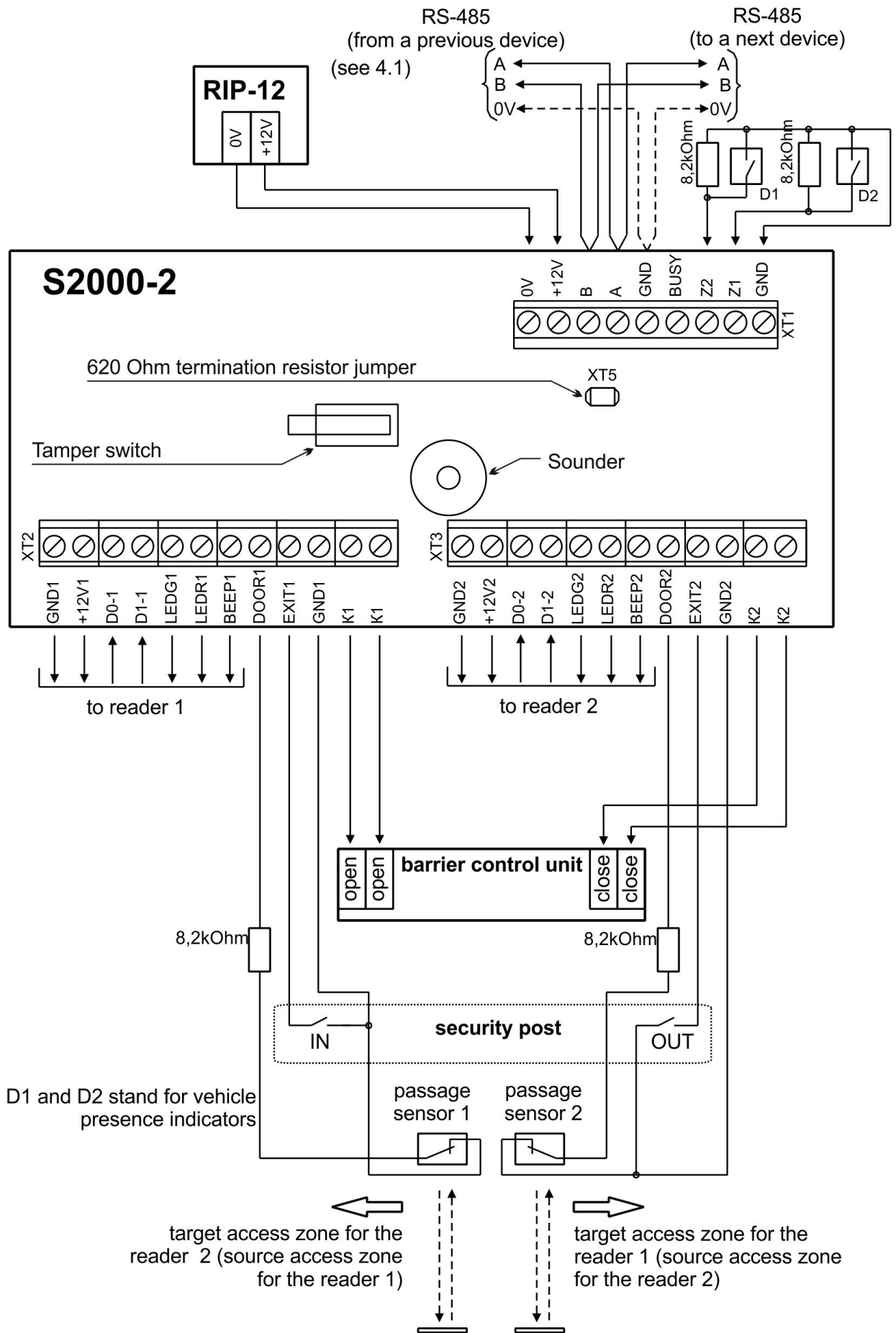


Figure 13. Connection Diagram for the Controller to Operate in the Boom Barrier Mode

Instead of two passage sensors located on both sides of the boom barrier it is allowed to use a single detector located just under the barrier or closely to it. In this case such detector is connected in parallel across the inputs of both channels of the controller as shown in Figure 12.

If traffic lights should be controlled at the entrance and the egress then they can be connected via relay amplifiers as shown in Figure 14. This diagram uses commutation devices UK-VK/06 controlled by logic signals of +5V CMOS levels so they can be connected directly to controller outputs in parallel across the reader LED control circuits. Commutation devices UK-VK/06 can commute voltages up to 220 V (ac) and currents up to 10 A providing control for almost any traffic light.

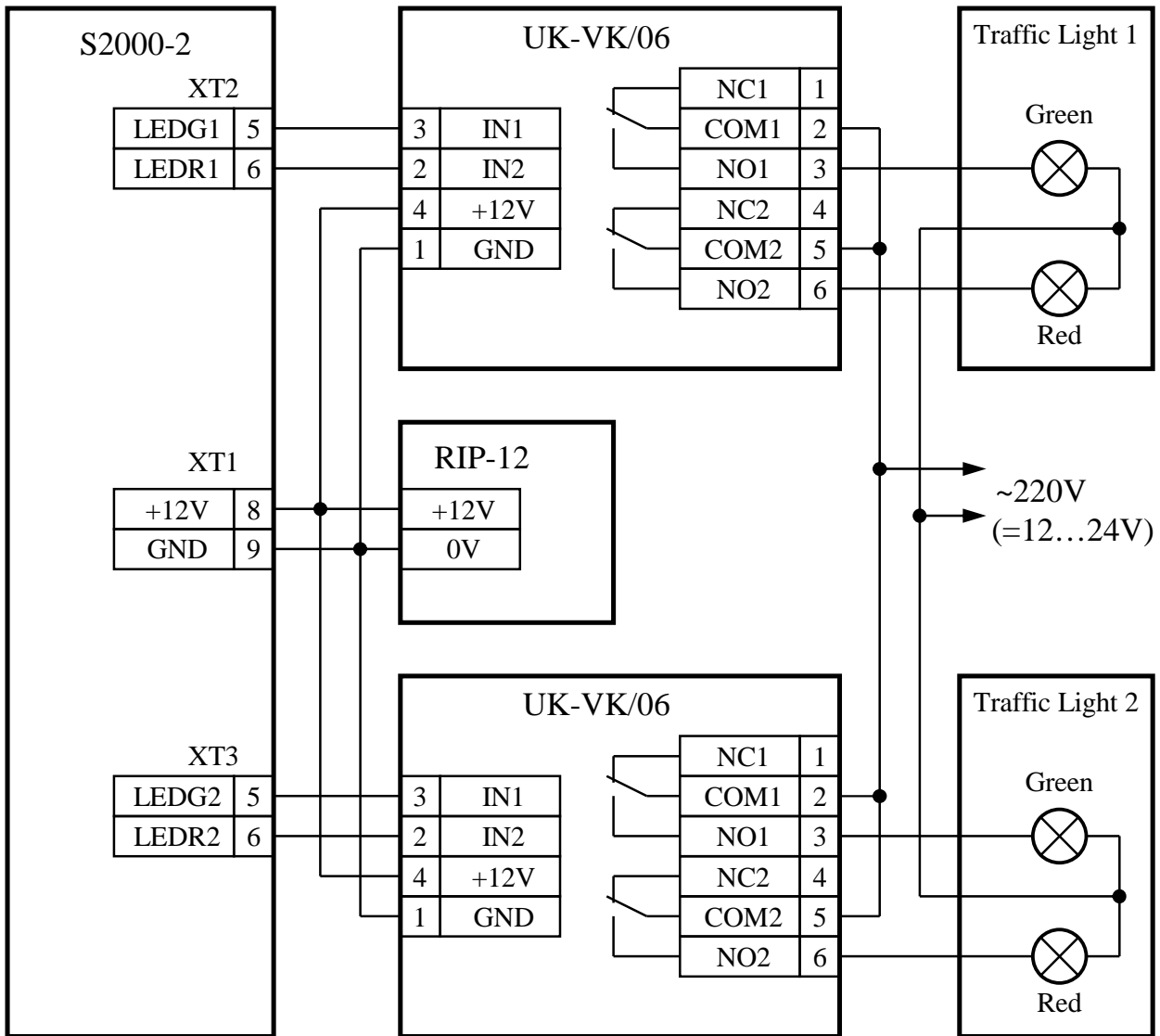


Figure 14. Schematic for Wiring Traffic Lights to the S2000-2 in the Boom Barrier Mode

To control (lift) the boom barrier from the guard post manually, IN and OUT buttons are used which are connected to the terminals EXIT1 and EXIT2 of the controller. To close the boom barrier by force, a DENY button can be used (it is not shown in the scheme). Pressing on the DENY button when the boom is being lifted causes lowering the boom even if the current access procedure has not been completed. The DENY button can be connected to any of the terminals EXIT1 and EXIT2 in accordance with the schematic shown in Figure 5.

If access is granted by the IN button then the green indicator of the first reader and/or green traffic light facing the reader 1 start illuminating.

If access is granted by the OUT button then the green indicator of the second reader and/or green traffic light facing the reader 2 start illuminating.

In the mode of locked access the buttons provide the only way to lift the barrier. In the free pass mode pressing on the buttons is ignored.

If vehicle presence detectors are used in front of the readers then authentication at the readers is ignored when no vehicle is present. The schematic shows connecting vehicle detectors with normally open contacts (they close if a vehicle is present). Connecting detectors with normally close contacts is shown in Figure 15.

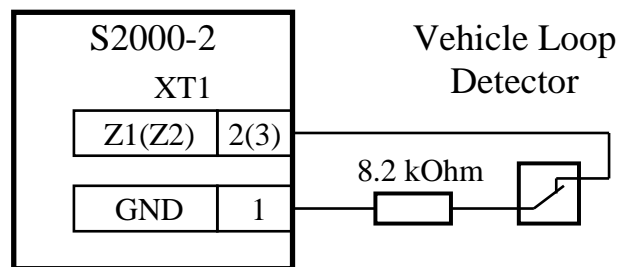


Figure 15. The Schematic for Connecting an NC Vehicle Presence Detector into LP1 and LP2 of the S2000-2

If the readers are powered by a separate power supply then the GND-circuits of the controller and the readers must be coupled.

2.4.3 Configuration Settings

- 1) Set the operation mode of the controller to the value "Boom Barrier".
- 2) Set the value of the Passage Timeout (30 s is advised).
- 3) Give the value for Barrier Close Delay (5 s is advised).
- 4) Passage Sensor in the Boom Barrier operation mode is always considered to be set on.
- 5) Set off the parameters Door Forced Open Monitoring and Door Held Open Monitoring.
- 6) Set the Control Program for both the relays to 3 ("Switch On for a Time").
- 7) Set Relay Activation Time for the relay 1 to 5...20 seconds (enough to lift the barrier). If the barrier is to be controlled by a single relay then set the activation time for the relay 1 to a value a bit more than Passage Timeout, for example 31 s.
- 8) Set Relay Activation Time for the relay 2 to 5...20 seconds (enough to lower the barrier).
- 9) For the LP1 and LP2 of the S2000-2 set Loop Type to the value "Enable Reading".
- 10) Set on the parameters Enable Reading Via LP1 and Enable Reading Via LP2 for the first and the second reader respectively.

Other settings depend on the specific operation conditions.

The relay parameters Switch Off When Door Is Open and Switch Off When Door Is Closed do not imply on relay operation in the Boom Barrier mode.

2.4.4 Operation

When a vehicle arrives to the reader it stops moving and a User-type credential with Access attribute and "Simple" passage mode is presented. If access is granted then green reader LED (green traffic light) starts illuminating, the boom barrier is lifted, and an Access Granted message is generated with the code of the presented credential.

If two-factor authentication is applied at the reader then the green LED of the reader starts flashing five times per second and access is granted only after presenting an extra code (see Section 1.5).

After vehicle's passing (after responds of the first and then the second passage sensors) the green LED of the reader (green traffic light) switches off and red LED (traffic light) starts pulsing twice per second warning of the imminent closing of the barrier. A Transaction message is generated with the code of the presented credential. On the expiry of Barrier Close Delay since the time the vehicle has left the red LED of the reader (red traffic light) starts showing solid light and the barrier is lowered. If the vehicle stands under the barrier (no both passage sensors have restored) then the barrier is not closed and the red LED of the reader (red traffic light) pulses until the vehicle leaves. Only after restoring both the passage sensors the barrier closing delay starts to be counted.

The next access procedure (next authentication) can be started only after the moment when the second passage sensor has responded, that is when the reader LED (traffic light) has changed lighting from steady green color for pulsing with red.

The procedure for travelling in another direction is similar but using or non-using of two-factor authentication is programmed for the access level of the credential individually for each reader (for each travel direction).

When the controller is expected for a vehicle to go out of the barrier, the second (closing) relay cannot be activated. And if the time of activation of the first relay has not yet expired then the first relay is being switched on until the vehicle leaves. As a result, both barriers with two control circuits and barriers with one control circuit can be kept open.

2.5 Mantrap Mode

2.5.1 In this mode the controller controls access through a single access point which is two doors with a closed space between them (a mantrap) provided that these two doors can never be open simultaneously. Each of two entrances to the mantrap is equipped with a reader (outside the mantrap). The guard post controlling the mantrap manually is equipped with two EXIT buttons so that a guard can let a person to enter into the mantrap without presenting a credential, two CONFIRM buttons to let an individual to leave the mantrap, and a DENY button to deny access. To pass through the first door (entrance to the mantrap) it is necessary to present a credential. The second door becomes open either automatically after the first door is locked or after a guard presses the relevant CONFIRM button (this is programmed while defining an access level). If there is no guard post and the mantrap operates only automatically then CONFIRM buttons anyway must be connected in order a person can leave via the same door through which he entered if he changes his mind or stays inside more than the programmed time. In order to pass in automatic mode, an access level must be programmed with the Simple passage mode.

If Confirmed Manually passage mode is set then after entering the mantrap a guard performs an additional visual identification (for example, compares the person who entered with the photo on the screen of the PC) and makes a decision to release the person from the mantrap. The allowed time for a person to stay within the mantrap is defined by the parameter *Confirmation Timeout*. Within this time any of the CONFIRM buttons can be pressed opening the relevant door. If during this time neither of the CONFIRM buttons was pressed then the access procedure is considered to be incomplete while the mantrap is considered to be free. A person can be released from the mantrap after elapsing of Confirmation Timeout only via that door through which he has entered by pressing the CONFIRM button of this door. On the one hand, Confirmation Timeout must be selected enough for performing an additional identification. But on the other hand, if a person has presented a credential but has not entered into the mantrap then within this time a new access procedure cannot be started.

If the mantrap is equipped with an occupancy sensor and this sensor is connected to the BUSY input of the controller then no rigid time limitation is required and additional identification will be performed as long as required.

The doors have to be equipped with door open sensors (the parameter Passage Sensor is considered to be always set on).

In this operation mode antipassback rules can be applied because authentication is performed on passing in both directions while the relevant design of the mantrap and visual identification by a guard guarantee that a single access granting can be used only for a single passage.

2.5.2 The schematic for connecting the S2000-2 in the Mantrap operation mode is shown in Figure 16.

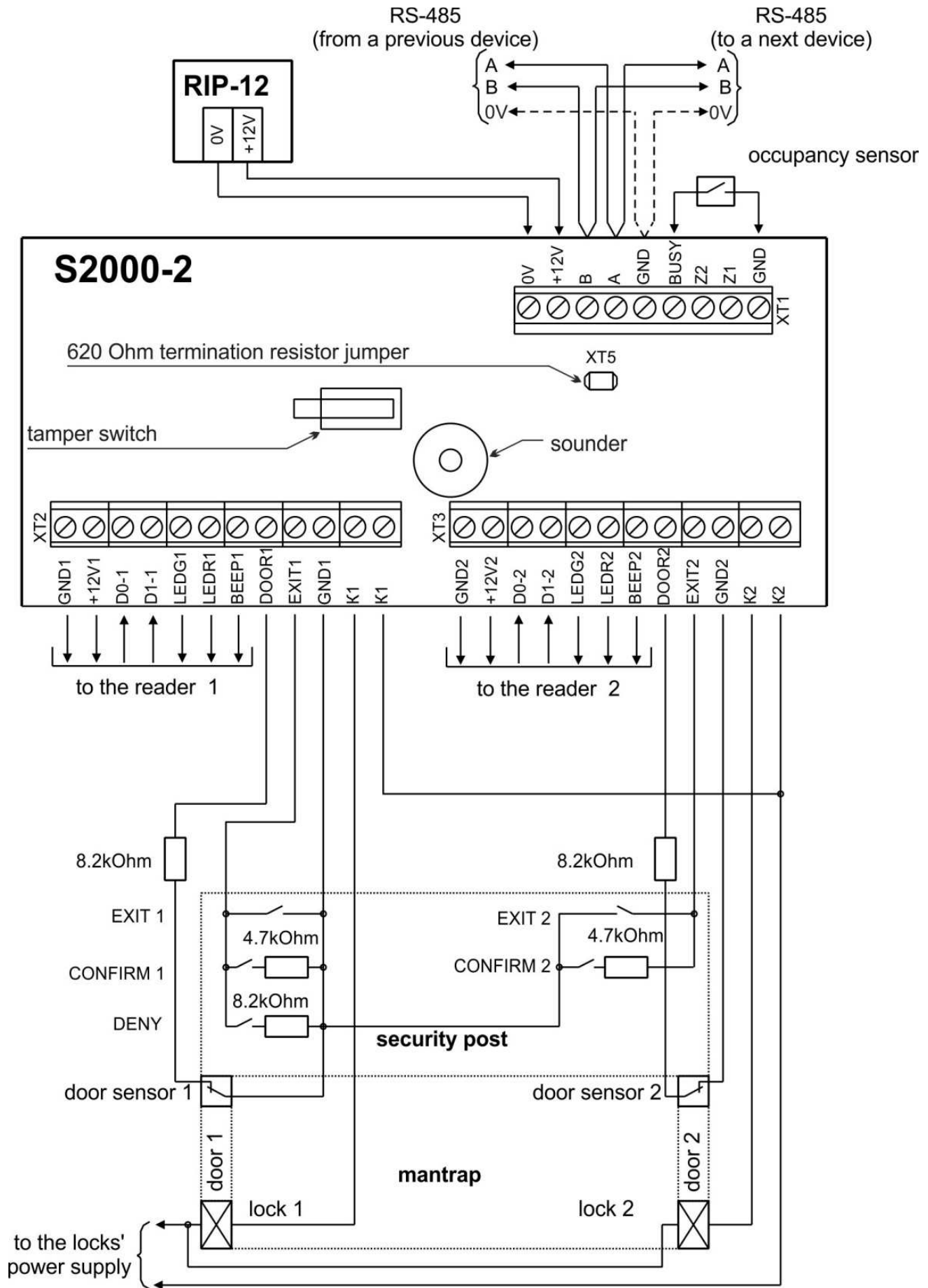


Figure 16. Connecting the S2000-2 for the Mantrap Operation Mode

In case of powering the locks and the controller by the same power supply, the input power circuits of the controller and input power circuits of the locks must be separate pairs of wires which are connected only at the power supply terminals.

If the lock is not equipped with a circuit for suppression of high-voltage pulses generated during commutation then a reverse switched diode must be connected at the lock terminals in parallel with the lock's winding (the admissible direct current of the diode must not be less than operating current of the lock).

If the readers are powered by a separate power supply then the circuits "GND" of the controller and the readers must be coupled.

2.5.3 Configuration Settings

- 1) Set the operation mode of the controller to the value "Mantrap".
- 2) Set the value of the Passage Timeout (10 s is advised).
- 3) Set the value of Confirmation Timeout. If no occupancy sensor is in use then the time shall be enough to identify a person additionally (the actual value depends on the specific procedure). If an occupancy sensor is in use than Confirmation Timeout can be set to a small value or even to zero provided that the occupancy sensor always responds by the time the door is closed after passing.
- 4) The Passage Sensor parameter in the Mantrap operation mode is considered to be always set on.
- 5) The PERMIT button is not used in the Mantrap operation mode and the relevant parameter is considered to be always set off;
- 6) If an occupancy sensor is in use then for both readers set the Receive BUSY parameters on.
- 7) For both readers set LED Quiescent Mode to "5 – Solid red light when BUSY".
- 8) If electric strikes are in use then for each relay set:
 - Control Program to the value 3 (Switch On for a Time);
 - Relay Activation Time to 1...5 seconds (the time enough for the strike to operate);
 - The relay parameter Switch Off When Door Is Open to the value "On" (for the strike to be latched correctly in case of a fast passage).

Otherwise, if magnetic locks are in use then for each relay set:

- Control Program to the value 4 (Switch Off for a Time);
- Relay Activation Time to the value of Passage Time (10 s is advised);

The parameter Switch Off When Door Is Closed can be not programmed because in the Mantrap mode it is considered to be set on always.

- 9) If Global Antipassback or Time & Attendance functions are in use then define correct values of Target Access Zones for both readers.

Other settings depend on the specific operation conditions.

2.5.4 Operation

To enter the mantrap, a User-type credential with Access attribute is to be presented to the reader before the door. If for the access level of the presented credential the Simple passage mode is programmed then the reader sounder beeps twice, the green LED starts illuminating, the first door is open (unlocked), and an Access Granted message is generated with the code of the presented credential. If the Confirmed Manually passage mode is programmed then the reader sounder beeps twice, the green LED starts pulsing, the first door is open (unlocked), and an Identification message with the code of the presented credential is generated.

If the access level of the credential implies two-factor authentication at this reader then the green LED of the reader starts pulsing five times per second and the door can be open only after presenting a correct extra code (see Section 1.5).

After entering inside the mantrap and closing the first door in case of the Simple passage mode the second door for exiting the mantrap opens (unlocked) immediately. After opening of the second door a Transaction message is generated.

In case of the Confirmed Manually passage mode a guard performs an additional verification of the incomer (by comparing with the photo on the screen of a PC, or by inspecting documents etc.) and makes a decision about granting or not granting access. Depending on the made decision the guard press one of the CONFIRM button and the DENY button.

When the CONFIRM button of the second door is pressed the door becomes open (is unlocked) and an Access Granted message is generated. After opening of the second door a Transaction message is generated.

If the CONFIRM button of the first door (through which the person entered the mantrap) is pressed then the door becomes open and no message is generated – access was not granted.

If the DENY button has been pressed then an Access Denied message is generated, and no door is open. A person then can be released only through the door through which he entered by pressing the relevant CONFIRM button.

If it is necessary to grant access to a person without a credential, the guard lets him go inside the mantrap by pressing the EXIT button of the relevant door. After the person has entered the access procedure is the same as said above for the Confirmed Manually passage mode.

During a passage the mantrap is considered to be busy and no passing in this or opposite direction can be started.

If a person has happened to be within the mantrap while the mantrap is considered to be free (the door was unlocked but the person didn't exit or Confirmation Timeout has expired) then to release the person the CONFIRM button of the door which was unlocked last must be pressed.

The procedure of passing in another direction is similar provided that the mode of passage to this direction can differ from the mode of passage in forward direction for the same credential.

3.1.4 Test the controller in the following order:

- a) Check the package condition and unpack the controller;
- b) Check the delivery and the parts in accordance with Section 1.3;
- c) Ensure the controller case is not damaged;
- d) Shake the controller and ensure there are no foreign bodies within it;
- e) Ensure that the terminal blocks are fastened properly;
- f) Check that the serial number of the controller and its production date are the same as specified in documentation;
- g) Assemble the schematic in accordance with Figure 17.

3.1.5 Test the controller functionality:

- a) Apply power to the controller;
- b) The internal sounder shall play a short "Start" signal;
- b) Measure the current consumed by the controller and ensure that it doesn't exceed 120 mA;
- r) Observe how the S2000M panel displays events of recognizing the controller, resetting the controller, and tampering the controller.

3.1.6 Testing in Self-Diagnostic Mode

Before testing the controller in the Self-Diagnostic mode disconnect from it all the circuits to control locking devices which cannot be turned on during the diagnostic.

The Self-Diagnostic mode can be initiated by means of the tamper switch. To activate the mode, open the cover of the controller case and press the tamper switch three times for a short time and once for a long time.

Pressing for a long time here means holding the tamper switch down for at least 1.5 s. Pressing for a short time means holding the tamper switch down within 0.1 to 0.5 s. Pauses between presses should be no longer than 0.5 s.

If the controller is operating properly then the READY LED starts pulsing very fast and the controller's sounder beeps twice. Then "1" and "2" indicators in turns illuminate for a short time (1 s with red light and 1 s with green light). The contacts of the relay 1 are closed at the moment when the "1" LED turns on while the contacts of the relay 2 are closed when the "2" LED turns on.

3.1.7 Testing reader connection circuits:

- a) Present a credential unknown for the controller to the first reader of the controller;
- b) The LED "1" of the controller and the reader LED shall illuminate three times for a short time in red;
- c) The controller sounder and the reader sounder (if available and controlled by the S2000-2) shall issue a long Error signal;
- d) Repeat steps a) to c) for the second reader of the controller.

If the controller ignores the presented credential this can mean a mismatch between the reader data format and the programmed value of the **Output Interface** parameter (by default 1 – Touch Memory).

If no signal has been heard it can mean that this category of signals (Access) is disabled for the controller sounder and the reader sounder (enabled by default).

3.1.8 Testing alarm loops, door circuits, EXIT button circuits:

a) Read the value of the resistance of the alarm loop 1 by means of the S2000M panel. For doing so:

- In the *View Input Status* menu select the *Input ADC* command;
- Enter the RS-485 address of the S2000-2 (the factory value is 127) or select the device address in the list of connected devices with the help of the "◀" and "▶" buttons of the panel;
- Type the number of the input: "1".

The value of the alarm loop returned by the panel shall be $8.2 \text{ kOhm} \pm 10\%$.

b) Repeat the step a) for the alarm loop 2, the DOOR1 circuit ("alarm loop 3"), the DOOR2 circuit ("alarm loop 4"), the EXIT1 circuit ("alarm loop 5"), the EXIT2 circuit ("alarm loop 6"), the BUSY circuit ("alarm loop 8"). The values returned by the panel for all the "alarm loops" of the controller should be $8.2 \text{ kOhm} \pm 10\%$.

3.1.9 Testing the voltage of the battery of the real-time clock:

a) Read the value of the real-time clock battery voltage with the help of the S2000M panel by doing the following:

- In the *View Input Status* menu select the *Input ADC* command;
- Enter the RS-485 address of the S2000-2 (the factory value is 127) or select the device address in the list of connected devices with the help of the "◀" and "▶" buttons of the panel;
- Type the number of the input: "7".

The value of the battery voltage returned by the panel should be 2.7...3.4 V.

b) If the battery voltage is a lower value then the battery must be replaced. The type of the battery in use is CR2032 (3 Volt lithium button bell battery).

3.2 Annual maintenance works include:

- a) Ensuring the enclosure of the controller is not damaged and is mounted securely and wire terminals are fastened properly;
- b) Removing dust, debris, and corrosion from the contact connections and the controller enclosure;
- c) Testing functionality of the controller in accordance with the techniques discussed in Sections 3.1.6 – 3.1.9 of this Manual.

4 Marking

4.1 The marking of the controller must correspond to the set of design documentation and Russian Standard ГOCT 26828-86.

4.2 On the bottom of the controller base there is a plate with the following information:

- Logo or manufacturer name;
- Name or conventional name of the controller;
- Factory number;
- Two last digits of the year and the quarter the controller was made;
- Conformity mark.

4.3 On the front side of the controller case there are letterings near the relevant LEDs specifying their purposes.

4.4 The marking of the transport packaging corresponds to Russian Standard ГOCT 14192-77 and includes the handling marks N1 (“Fragile”), N3 (“Keep dry”), N11 (“Top”), base, additional, and information letterings.

5 Packaging

5.1 A final product is a controller with its documentation set and component items accepted by Quality Control Department and packed in a consumer packing.

5.2 Preservation of the controller is performed in accordance with Russian Standard ГOCT 9.014-78 for the product group III-3 with a variant of temporary anticorrosive protection B3-0.

5.3 The controller is to be packed into a consumer packing – a cardboard box of the type III-I of Russian Standard ГOCT 12301-81 and also the component kit is enclosed with the controller.

5.4 The boxes with the packaged controllers are packed into transport packages – boxes of the type II-I of Russian Standard ГOCT 5959-80 lined with ГOCT 515-77 saturated paper.

5.5 A packing list with the following information is to be enclosed into every box (or container):

- The name and conventional name of the controller, the number of the controllers;
- The month and the year of packaging;
- The signature or stamp of a person responsible for packaging.

5.6 The controllers can be packed within containers in accordance with Russian Standard ГOCT 9181-74.

5.7 The net weight should be 10 kg max.

5.8 The gross weight should be 15 kg max.

6 Storage

6.1 The controller in a consumer packing must be stored in accordance with Storage Ambients 1 of Russian Standard ГOCT 15150-69.

6.2 In the premises where the controller is stored there must not be any acid fumes, alkaline fumes and other aggressive gases and harmful impurities which can cause corrosion.

7 Transportation

7.1 Packed controllers should be transported by any covered vehicles in accordance with the local regulatory documents.

7.2 The transportation condition for the controller must be the same as Storage Conditions 5 in accordance with Russian Standard ГOCT 15150-69.

8 Certificates

8.1. Conformity Certificate № TC RU C-RU.ME61.B.00796 certifies that S2000-2 Access Controller meets the requirements of Technical Reglament of Custom Union TR CU 020/2011.



8.2. Production of S2000-2 Access Controllers is certified according to ГОСТ ИСО 9001 ISO 9001-2011 by a conformity certificate No.ПООС RU.ИК32.K00153.

9 Manufacturer Data

The Bolid Company, Russia

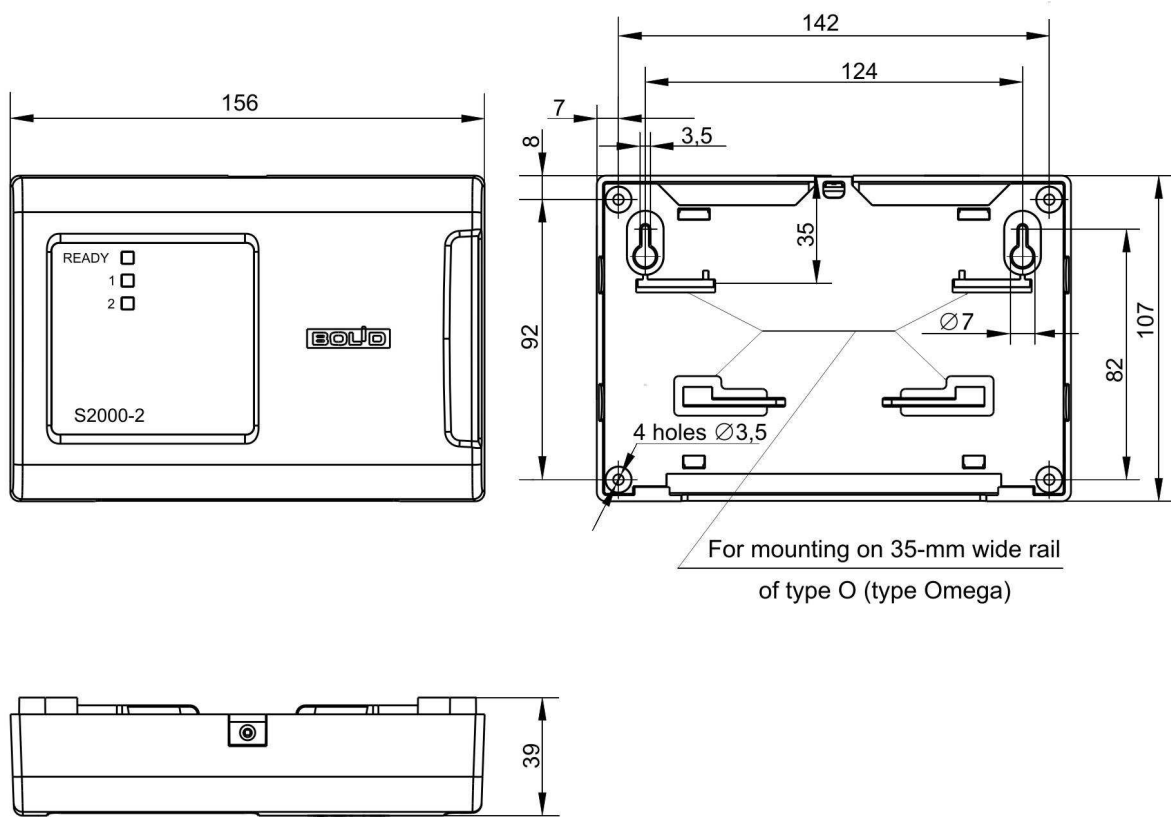
Address: 4 Pionerskaya Str., Korolev 141070, Moscow Region, Russia

Tel./fax: +7 (495) 775-71-55 (multi-channel), +7 (495) 777-40-20, +7 (495) 516-93-72

E-mail: info@bolid.ru; Technical Support: support@bolid.ru; <http://bolid.ru>

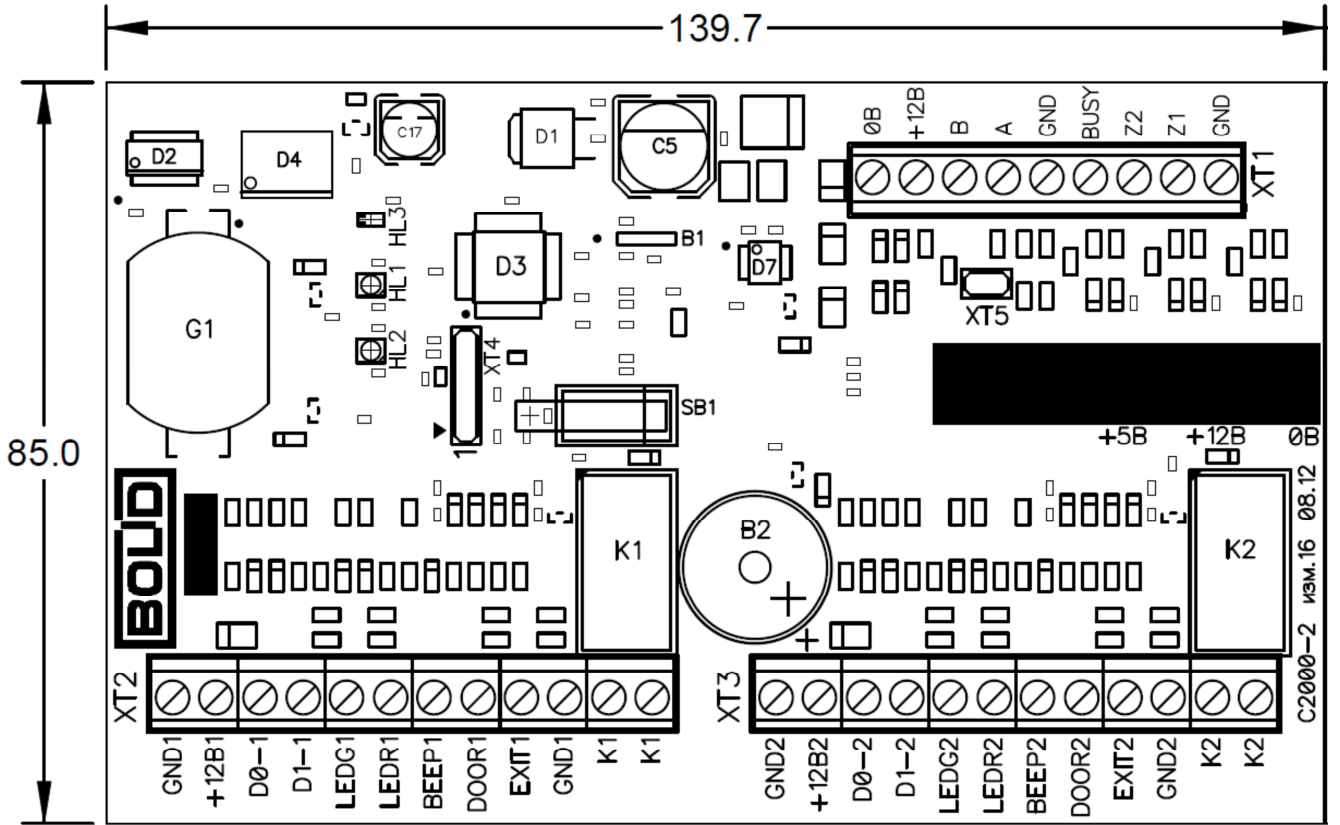
Appendix A

Overall and Mounting Dimensions of the S2000-2 Controller



Appendix B

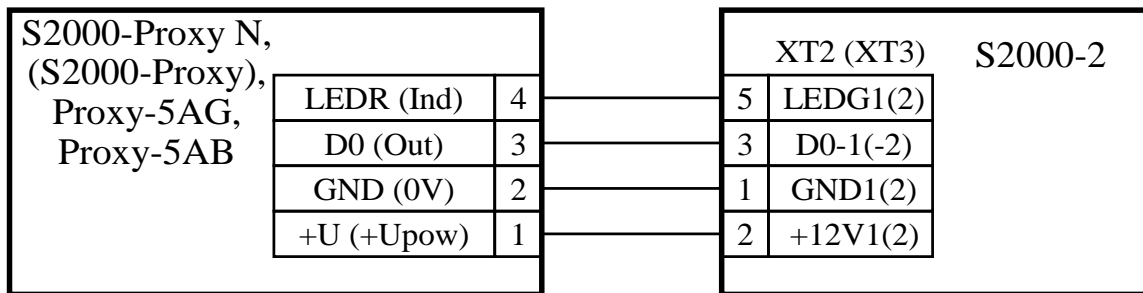
PCB Layout



Appendix C

The Schematics for Connecting Readers to the S2000-2 Controller

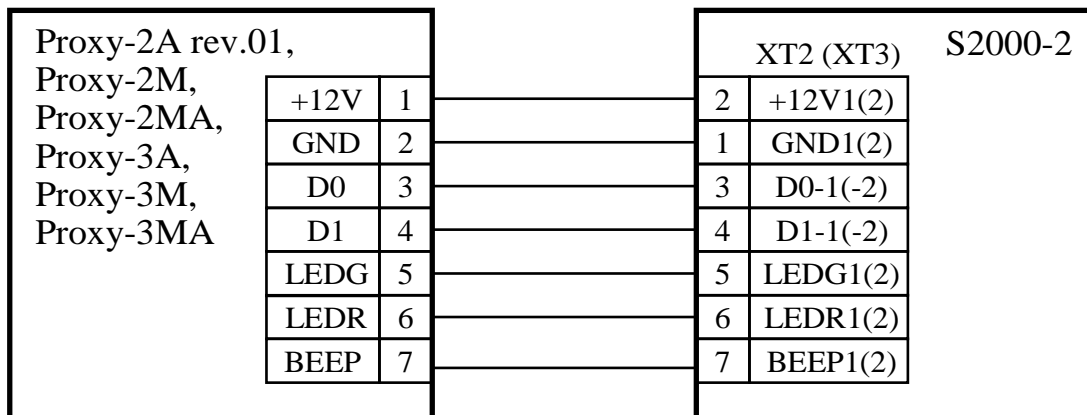
The Schematic for Connecting S2000-Proxy, S2000-Proxy N, Proxy-5AG, Proxy-5AB



S2000-2 Configuration Parameters:

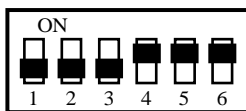
Output Interface	1: Touch Memory
LED Control Polarity	Direct (active "1")

The Schematics for Connecting Proxy-2A rev.01, Proxy-2M, Proxy-2MA, Proxy-3A, Proxy-3M, Proxy-3MA

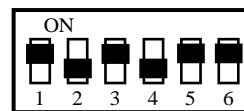


Variant 1: The Touch Memory interface

Variant 2: The Wiegand interface



Reader DIP Switch Positions

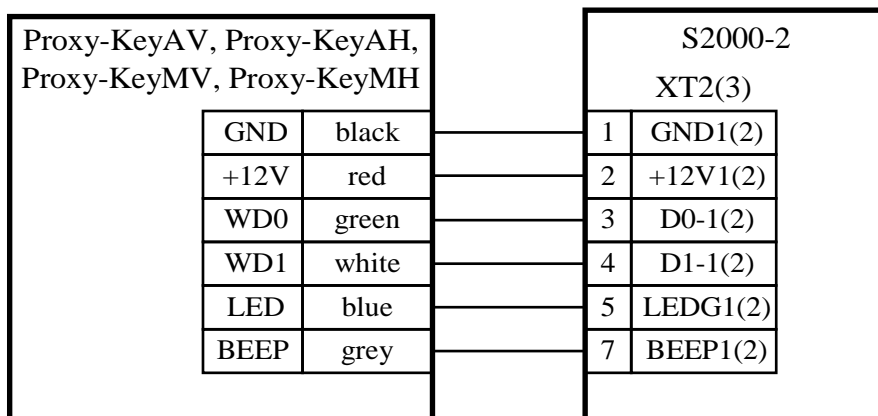


Configuration Parameters of the S2000-2:

Output Interface	1: Touch Memory
LED Control Polarity	Direct (active "1")
Sounder Control Polarity	Direct (active "1")

Output Interface	2: Wiegand
LED Control Polarity	Inverse (active "0")
Sounder Control Polarity	Inverse (active "0")

The Schematic for Connecting **Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH**

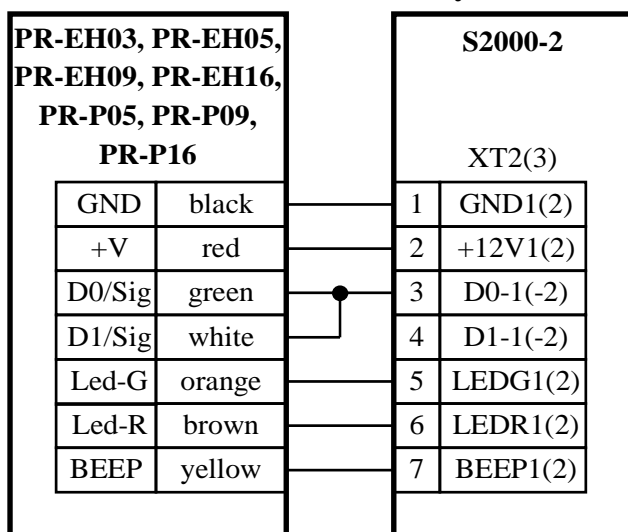


S2000-2 Configuration Parameters:

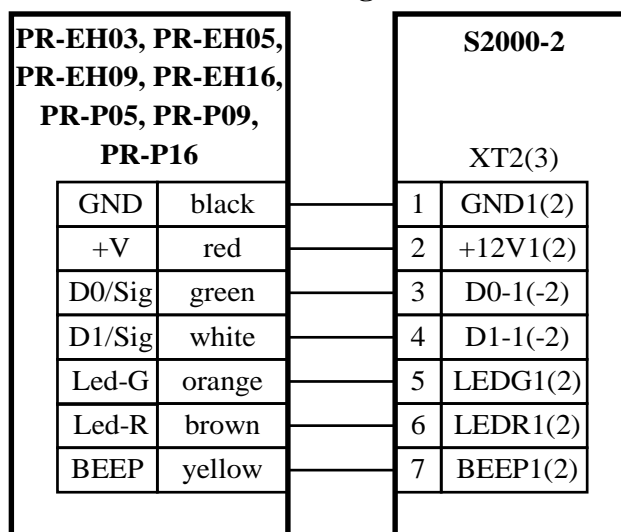
Output Interface	2: Wiegand
LED Control Polarity	Inverse (active "0")
Sounder Control Polarity	Inverse (active "0")

The Schematic for Connecting
PR-EH03, PR-EH05, PR-EH09, PR-H16, PR-P05, PR-P09, PR-P16

Variant 1: The Touch Memory Interface



Variant 2: The Wiegand Interface

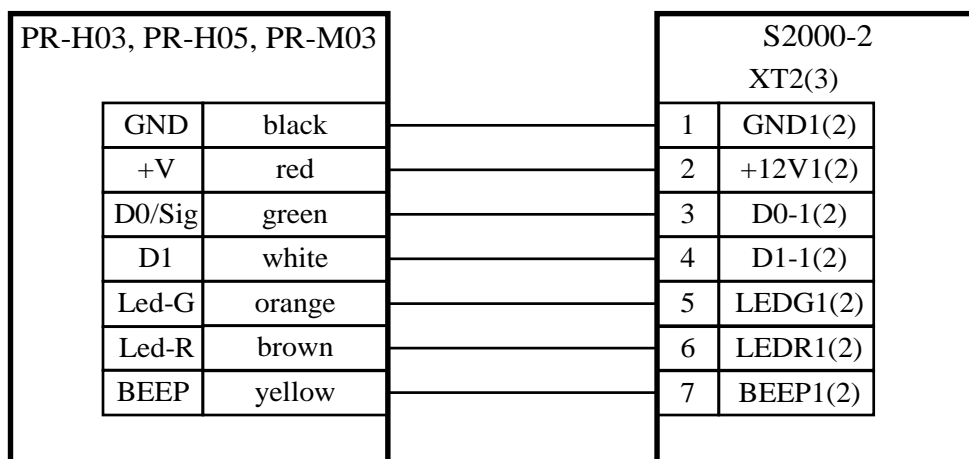


S2000-2 Configuration Parameters:

Output Interface	2: Touch Memory
LED Control Polarity	Direct (active "1")
Sounder Control Polarity	Direct (active "1")

Output Interface	2: Wiegand
LED Control Polarity	Inverse (active "0")
Sounder Control Polarity	Inverse (active "0")

The Schematic for Connecting Readers **PR-H03, PR-H05, PR-M03**



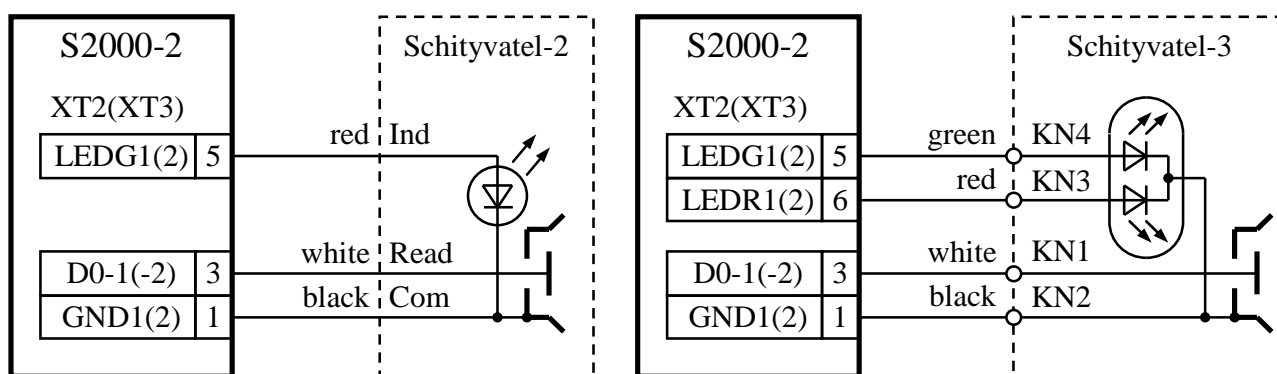
Variant 1: The Touch Memory interface

S2000-2 Configuration Parameters		Reader Jumpers	
Output Interface	1: Touch Memory	Red	Open
		Yellow	Open
LED Control Polarity	Direct (active "1")	Orange	Open
Sounder Control Polarity	Direct (active "1")	Green	Open

Variant 2: The Wiegand interface

S2000-2 Configuration Parameters		Reader Jumpers	
Output Interface	2: Wiegand	Red	Close
		Yellow	Open
LED Control Polarity	Inverse (active "0")	Orange	Close
Sounder Control Polarity	Inverse (active "0")	Green	Close

The Schematic for Connecting iButton Readers "Schityvatel-2" and "Schityvatel-3"



S2000-2 Configuration Parameters:

Output Interface	1: Touch Memory
LED Control Polarity	Direct (active "1")