BOLID SECURITY SYSTEMS

Orion ISS

ISO 9001

Access Controller

S2000-2

User's Manual

This User's Manual is intended to help for studying operability principles and maintenance of **S2000-2** or **S2000-2 rev.01 Access Controller** of version **1.11**.

The S2000-2 rev.01 access controller is equipped with twofold increased memory capacity for access keys (8192 keys), as well as event buffer capacity (4095 events) against the S2000-2 controller. All information presented in this Manual is applicable for both controllers taking this difference into account.

Please read the instructions completely before connecting, operating, adjusting or maintaining this product.

The following terms are used throughout the Manual

Zone: a minimal part of the security and safety installation that can be monitored and controlled independently. Depending on the context, the term 'zone' can imply an alarm loop, an addressable detector, a hardware component and so on.

Partition: A set of zones that can be user controlled as a whole. As a rule, zones fall into partitions depending on their location (e.g., one partition can involve all zones at one individual area)

Arm/Disarm means starting/cancellation monitoring of loop (zone, partition, system) conditions and signaling alarms in controlled zones

Network Address (Address): – a unique number of the device (from 1 to 127) within the ISS Orion local RS-485 network

Table of Contents

FEATURES AND DESIGN

The S2000-2 access controller (hereinafter referred to as the controller) is designed to control access through one or two access points by means of reading presented access keys (Proximity cards, iButtons, PIN-codes and so on), verification of access rights and closing (opening) relay contacts that operate locking units (electromagnetic locks and strikes, turnstiles, swing-beam drives and so on). To read access keys one or two readers with Touch memory, Wiegand or ABA TRACK II output interface are to be connected to the S2000-2 controller.

The controller is designed to operate either as a part of a PC-based Orion integrated security system under the Orion 1.0 KD (version 7 or higher) or the Orion Pro (version 1.8 or higher) Workstation software, or as a part of an Orion integrated security system based on S2000 or S2000M control console, or standalone.

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

- Two Entrance Doors
- One Entrance/Exit Door
- Turnstile
- Swing-beam Barrier
- Two Sluice Doors

Moreover, access via any access point (controlled by a reader) can be switched to locked or free access mode.

In order to verify access rights of the presented key, the controller takes into account the following access restriction factors:

- The key is not locked
- Access rights of the key to the restricted access zone
- Duration of the key validity
- The key time schedule is active
- Anti-passback rules violation (preventing a key from being passed back for re-use)
- Access lockout by means of alarm loops of the controller

Two-factor authentication mode can be applied to a reader of the controller if the reader is physically designed to read not one but two different identifiers of a person, for example a combination of Proximity card and PIN code. For such a case memory capacity of the controller is twice decreased.

Both local and centralized strategies of access control can be implemented by an S2000-2 access controller, connected via RS-485 interface to a network controller — a PC under ARM Orion Workstation software. Local control means that access is granted or denied depending on access rights of the identifier (key), stored in the controller database, the current access mode and access violations previously made by this key. Centralized access control means that the presented key code is read and transferred to the network controller (the Orion Workstation), which grants or denies access (only for operation as a part of the PC-based Orion system).

To increase the level of authentication two- or three-person access rules can be assign to be applied for a group of access keys.

Besides the access control functions the S2000-2 access controller (except being in Swing-beam operation mode) can monitor for conditions of two alarm loops connected to its relevant inputs signaling loop alarms locally and transmitting loop event information via the RS-485 interface to a network controller (S2000/S2000M or ARM Orion). The controller provides arming and disarming of the alarm loops by presenting pre-programmed keys designed for arming/disarming to a reader of the controller, or by a relevant command of the network controller.

The S2000-2 controller provides light and sound indication of access conditions and violations as well as loop alarms by means of built-in LEDs and sounder, and by means of LEDs and sounder of the reader.

The controller view is shown in Figure 1. The green READY LED is designed to indicate S2000-2 operation conditions while the two red LEDs 1 and 2 are intended to provide access and arming/disarming indication.

The controller enclosure is equipped with a tamper switch which provides generating tamper alarms and transmitting them to a network controller.

The controller is intended for indoor installation and round the clock operation. The controller is not suitable for operation in corrosive and dusty environments, as well as in fire-hazardous and explosive areas.

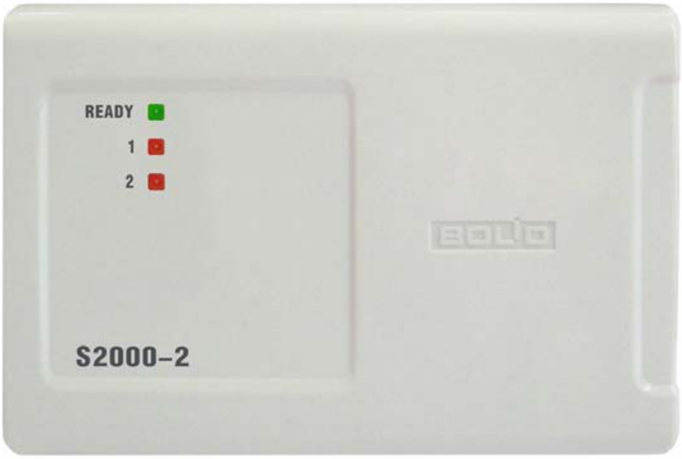


Figure 1

SPECIFICATIONS

➢ ***Doors Per Controller***	Up to 2
➢ ***Access Keys***	iButtons, Proximity cards, PIN-codes, etc.
➢ ***Readers Per Controller***	2
Output Interface	Touch Memory (1-Wire, µ-LAN), Wiegand, ABA TRACK II
LEDs	One or two single color LED, or one double color LED, controlled by logical +5 V CMOS levels
Sounder	Controlled by logical +5 V CMOS levels
➢ ***Memory Capacity***	4096 (S2000-2) or 8192 (S2000-2 rev.01) key codes
➢ ***Event Log***	2047 (S2000-2) or 4095 (S2000-2 rev.01) events
➢ ***Time Schedules***	16 separate time schedules each including 10 time zones active for entry and/or for exit (loop 1 and/or 2 arming/disarming). Each key can be assigned to one time zone for access and one time zone for arming/disarming
➢ ***Anti-Passback (APB) Modes***	5 (Hard, Soft, Timed, Zonal, Global)
➢ ***Indicators (LEDs)***	3 (READY, 1, 2)
➢ ***Built-in Sounder***	Yes
➢ ***RS-485 Communication Port***	Yes
➢ ***Power Input***	Bolid uninterrupted power suppliers of RIP-12 series are recommended
Input Voltage	10.2 ÷ 15V DC,
Current Consumption	120mA max
Input Power	2W max
➢ ***Door Inputs***	2
Detector Included	NC/NO dry contact, open collector, digit output (0 or 1 active with 5 V CMOS levels)
Passage Signal Time	50ms min

➢ ***Request-to-Exit Inputs***	2
➢ ***Alarm Inputs***	2 inputs to monitor intruder detectors' conditions (except for Swing-beam Barrier operation mode)
Wire Resistance	1 kOhm excluding termination resistance 8.2 kOhm
➢ ***Relay Outputs***	2 outputs to operate locking units or power relays
Commuting Voltage	30VDC
Commuting Current	7A
Commuting Power	100W
➢ ***Tamper Switch***	Yes
➢ ***Enclosure Protection***	IP 20
➢ ***Operating Temperatures***	–30 to +50°C
➢ ***Overall Dimensions***	157 × 107 × 36 mm
➢ ***Weight***	about 0.3 kg
➢ ***Average Lifetime***	8 years
➢ ***Readiness Period***	5 s max

OPERATING

ACCESS KEYS

To identify keys used to implement different functions of the access controller a variety of electronic keys can be suitable (Dallas iButtons, Proximity cards, PIN-codes) provided that this electronic keys can be read by readers with such output interfaces as Touch Memory, Wiegand, or ABA TRACK II. To do this up to two said readers are to be wired to the S2000-2 controller.

The controller operates two LEDs (one double-colored LED) of a reader to provide condition and alarm indication. Control levels correspond to logical +5 V CMOS levels. The controller keeps the current passing through the directly connected LEDs within 10mA.

The controller operates the sounder of a reader. Control levels correspond to logical +5 V CMOS levels.

The keys which are used to operate with the controller must be pre-programmed and stored either in the S2000-2 controller memory or in the ARM Orion database. All controller keys fall into four different classes (types):

- User keys used for access and arming/disarming
- Locking keys used to lock access via an access point (see Access Modes Section below)
- Unlocking keys used to open access via an access point (see Access Modes Section below)
- Master keys used to switch the computer to the mode of hardware programming of User keys

User keys can be mono-functional used only to gain access or to arm/disarm alarm loops, or combined used both for access and arming/disarming. To cause the controller to select arming/disarming functions some hardware or software methods are to be used (see Alarm Loops Section below).

Access rights of each key are defined by a set of pre-programmed parameters which can be divided on two parts, the first part being common for a group of keys and the rest being set individually for each access key. This provides optimal combination of programming flexibility and usability (see Access Rights Section below).

The following access rights and restrictions **are set as a whole** for a group of access keys called ‘the access group’:

- The right to gain access to zones controlled by the S2000-2
- The time periods when entry and/or exit via the access point controlled by the S2000-2 are allowed (see Time Schedules Section below)
- The anti-passback rules applied (see Anti-passback Rules Section below)
- Additional restriction related to two- or three-person access rules (see Passage Modes and Two or More Person Rule Access Control Section below)
- The right to arm and/or disarm the first and/or the second alarm loops of the controller

- The time periods when arming/disarming alarm loops of the S2000-2 are allowed (see Time Schedules Section below)

The following access rights and restrictions **are set individually** for each access key involved in an access group:

- The type of the key (is this key intended to be used as User, Locking, Unlocking or Master)
- The key lockout (a key be locked if necessary, e.g. if the key is lost or stolen)
- The additional code for the key or permission to use only main code in case of two-factor authentication (see Two Factor Authentication Section below)
- The validity period of the key

The access key can be preprogrammed either by hardware or software ways — see Key Programming Section of this Manual.

Moreover, access control based on five different key patterns can be implemented through the access point. In such a case the codes of presented keys are stored neither in the S2000-2 memory nor in ARM Orion database, but instead to gain access they must meet on of the controller key pattern (see Key Pattern Based Access Control Section below).

OPERATION MODES

The controller can operate in one of the following modes:

- Two Entrance Doors
- One Entrance/Exit Door
- Turnstile
- Swing-beam Barrier
- Two Sluice Doors

Two Entrance Doors Mode

In this mode the controller provides access via two independent access points (doors), with passing being controlled via key presenting for one direction (entry) and being free by EXIT button pressing for another (backward) direction.

Standard time to pass after access being granted is 10 seconds.

In this mode alarm loops are not involved in the access control strategy. Its can be used within the integrated security systems for intruder alarm purposes.

If door sensors are connected to the relevant terminals of the controller and the controller is programmed to use these ones, some extended features are available for the S2000-2 controller, among them:

- PASSAGE messages are generated and transmitted (when the S2000-2 operates on-line) to a network controller
- While access is granted, the relay can be activated not only for a time defined by its *Relay Activation Time* parameter (a constant), but also can be adjusted to cancel executive program just after door opening or closing (see ‘S*witch Off After…’* parameters, Relay Configuration Parameters Section of this Manual)
- Door Held or Forced Open events are monitored for
- While access is granted, the reader green LED lights for a time relevant to actual passage time. If door sensors are not in use, the reader green LED lights for a time defined by the *Relay Activation Time* parameter, but at least for two seconds, regardless of the time the passing actually takes

In order to pass in forward direction, a User key with the *Access* attribute set is to be presented to the reader mounted near the door.

If identification is completed successfully, the reader sounder generates two beeps, the green LED turns on, the door is opened (unlocked), and the ACCESS GRANTED message with the code of the presented key specified is generated.

If the reader is programmed to implement two-factor authentication its green LED starts flashing 5 times per second and access is granted only after the valid additional code having been presented.

If two or three person access rule is applied, while identifying the key access is granted after all participants of the access procedure having been identified.

After opening the door the reader LED enters its normal mode (is off or lit with red) and the PASSAGE message is generated with the code of the presented key specified.

In order to open the door passing in backward direction, it is necessary to press the EXIT button that is mounted near the door inside the premises. The reader sounder generates two beeps, the green LED turns on, the door is opened (unlocked) and the ACCESS GRANTED message is generated without specifying a key (impersonal). The door opening causes the impersonal PASSAGE message to be generated. Passing through the second door is implemented similarly.

One Entrance/Exit Door Mode

In this mode the controller provides access via one access point (door) with one common locking device control circuit, with access in both passage directions being controlled via key presenting to the readers installed both at entrance and exit.

EXIT buttons can also be used to provide access, e.g. for remote door opening from a guard post.

Standard passage time after access being granted is 10 seconds.

In such the operation mode the anti-passback rules can be applied because the identification is implemented for passages in both directions. However a regular door does not protect against tailgating.

If door sensors are connected to the relevant terminals of the controller and the controller is programmed to use these ones, some extended features are available for the S2000-2 controller, among them:

- PASSAGE messages are generated and anti-passback rules can be applied
- While access is granted, the relay can be activated not only for a time defined by its *Relay Activation Time* parameter (a constant), but also can be adjusted to cancel executive program just after door opening or closing (see ‘S*witch Off After…’* parameters, Relay Configuration Parameters Section of this Manual)
- Door Held or Forced Open events are monitored for
- While access is granted, the reader green LED lights for a time relevant to actual passage time. If door sensors are not in use, the reader green LED lights for a time defined by the *Relay Acti-*

vation Time parameter, but at least for two seconds, regardless of the time the passing actually takes

In order to pass in both directions, a User identifier with the *Access* attribute is to be presented to a reader mounted near the entrance/exit.

If the identification process is completed successfully, the reader sounder generates two beeps, the green LED lights, the door is opened (unlocked) and the ACCESS GRANTED message is generated with the code of key presented included.

If this reader uses two factor authentications, the reader green LED starts flashing 5 times per second and access is granted only after an additional code having been identified (see Two Factor Authentication Section of this Manual).

If two or three person access rule is applied, while identifying the key access is granted after all participants of the access procedure having been identified (see Passage Modes and Two or More Person Rule Access Control Section of this Manual).

After opening the door the reader LED enters its normal mode (is off or lit with red) and the PASSAGE message is generated with the code of the presented key involved.

The procedure of passing backward is similarly, except two factor authentication (which is adjusted for each reader separately) and two (three) person access rule applying (which is specified for each access group).

Turnstile Mode

In this mode the controller provides access via one access point (electromechanical turnstile) equipped with two control circuits for each passing direction separately, with granting access in each direction requiring presenting keys to the readers installed from the both sides of the turnstile.

EXIT buttons can also be used to grant access remotely, e.g. from a guard post.

Standard time to pass after access being granted is 10 seconds.

Anti-passback rules can be checked for such an operation mode, as identification is required for passing in both directions and only one person can pass when access is granted.

No passage detector (rotation sensor) can be used. But in this case no passage event is generated, so it is impossible to use anti-passback and time&attendance utilities of Orion workstation. Besides, in this case the minimal passage time is equal to two seconds (only after expiration of this time the next key can be taken into account by the controller). If passage sensors are in use, the turnstile capacity (pedestrian throughput) can be increased as the next key will be read and identified by the controller immediately after passing having been detected.

In order to pass in any direction, a User key with the *Access* attribute set is to be presented to a reader installed before the turnstile.

If identification is completed successfully, the reader sounder generates two beeps, the green LED lights, the turnstile is unlocked to provide one passage in specified direction, and the ACCESS GRANTED message is generated with the code of the presented key included.

If the reader uses two factor authentications, the reader green LED starts flashing 5 times per second and access is granted only after an additional code having been identified (see Two Factor Authentication Section of this Manual).

After opening the door the reader LED enters its normal mode (is off or lit with red) and the PASSAGE message is generated with the code of the presented key involved.

The procedure of passing backward is similarly, except two factor authentication which is adjusted for each reader separately.

Swing-beam Barrier Mode

In this mode the controller provides a bi-directional access via a single access point which is a swing-beam barrier with the same bar facility for both access directions. The relay 1 is used to lift the bar while the relay 2 is used to lower it down. To grant access in each direction requires presenting the relevant key to one of the controller's reader.

The standard time to pass after access being granted is 30 seconds.

In this mode anti-passback rules can be used as far as identification is required for passing (to be more precise, for driving) in both directions.

To increase the authentication level of a system, car presence detectors are to be connected to the alarm loop contacts of the controller. In such a case key presenting causes the controller to make access decisions only if there is a car near the reader actually.

Passage sensors in this operation mode are used not only to detect car passing but also to prevent swing-beam lowering down on a car located under the beam. While at least one of the sensors is activated, the swing-beam will not be lowered.

EXIT buttons can also be used to gain access remotely, e.g. from a guard post. In the Access Locked mode the swing-beam can be lifted only by means of the EXIT buttons. Pressing the buttons in the Free Pass mode is ignored.

If the access is granted after the ENTRY button, the green LED of the first reader and/or green light on the traffic control unit directed to the first reader is switched on. If the access is granted after the EXIT button, the green LED of the second reader and/or green light on the traffic control unit directed to the second reader is switched on.

When driving to the swing-beam barrier, a car is slowing down near the reader, the driver presenting its User key with *Access* attribute set on. If access is granted the green LED of the reader (green light on the traffic control unit) is switched on and the ACCESS GRANTED message is generated with the code of the presented key included.

If two factor authentication is used for this reader, the reader green LED starts flashing 5 times per second, and access is granted only after a valid additional code presenting (see Two Factor Authentication Section of this Manual).

After a car passage (after actuation of the first and then the second passage sensors) the green LED of the reader (green light of the traffic control unit) is switched off and the red LED of the reader starts flashing twice per second warning about swing-beam closing, and the PASSAGE message is generated with the code of the presented key included. In 5 seconds the red LED of the reader (red light of the traffic control unit) is switched on steady and the swing-beam is lowered down. If the car is staying under the swing-beam (none of the two passage sensors is recovered), the swing-beam is not lowered down and the red LED of the reader (red light of the traffic control unit) keeps flashing until the car drives off. The swing-beam is lowered in 5 second after the car has moved out.

The next access procedure (next identification) can be initiated starting from the moment, when the second passage detector has been activated, i.e. when the reader LED (traffic light) is switched from green to flashing red.

The procedure of driving in backward direction is similar keeping in mind that using two factor authentication is configured separately for each access direction (each reader).

When the controller is waiting for car driving out of the swing-beam barrier, the second (closing) relay can not be activated, and if the first relay activation time has not yet been expired, the first relay is kept active until the car driving off. Due to this, a swing-beam barrier is kept open without regard to it has one or two control circuits.

Two Sluice Doors Mode

In this mode the controller provides access via an access point, which is represented by two interlocked doors with a space between them (a sluice). Two readers are installed from each side of the sluice (outside the sluice). Two EXIT buttons are mounted inside the sluice near each door or at the guard post. In order to pass through the first door (enter the sluice), it is required to present an authorized key, while in order to exit the sluice it is sufficient to press the EXIT button. Access through a door can granted (the door is opened) only if the opposite door is closed.

The EXIT buttons can be located inside the sluice, which makes it possible to exit the sluice without security guard participation. Otherwise its can be located at the guard post, and then after a person have entered the sluice through a first door security guard can visually verify the key presented (for example, compare the person who entered with an image on the PC monitor) and then make an egress decision.

The standard time to enter the sluice after access being granted is 10 seconds.

The standard time to leave the sluice after the EXIT button being pressed is 10 seconds.

The doors must be equipped with door sensors.

Anti-passback rules can be being inspected in such the operation mode since identification is required for passing in both directions, appropriate sluice design and the monitoring performed by a security guard ensuring that only one person can enter when access is granted.

In order to enter the sluice, a User key with the *Access* attribute set is to be presented to a reader mounted near the first door. If identification is completed successfully, the reader sounder generates two beeps, the green LED is switched on, the first door is opened (unlocked) and the ACCESS GRANTED message is generated including the code of the key presented.

If two factor authentication is applied at this reader, the reader green LED starts flashing 5 times per second, and access is granted only after a valid additional code having been presented (see Two Factor Authentication Section of this Manual).

After entering the sluice and closing the first door it is necessary to press the EXIT button near the second door. This unlocks the lock of the second door to leave the sluice. The second door opening causes the PASSAGE message to be generated. The lock is opened and the access is granted only if the first door is closed.

From the moment of entering the sluice (first door closing) to the moment of pressing the EXIT button of the second door no more than 20 seconds have to be expired. If within this time period the EXIT button of the second door was not pressed, the sluice can be left only in backward direction, by pressing the EXIT button of the first door.

While the sluice is being passed it is regarded as occupied and no new passing in any direction is impossible.

If EXIT buttons are located not inside the sluice but at the security post, leaving the sluice is allowed or is not allowed by a security guard after additional control.

The procedure of passing in backward direction is similar, except for the usage of the two factor authentication is configured separately for each pass direction.

ACCESS MODES

In all the controller's operation modes (*Two Entrance Doors*, *One Entrance/Exit Door*, *Turnstile*, *Swing-beam Barrier*, and *Two Sluice Doors*) each of the two readers connected to the controller can operate in one of three following access modes:

- Controlled Access Mode
- Access Locked Mode
- Free Pass Mode

If the access is locked (the Access Locked mode) an access can be granted only by the EXIT button or by a remote network controller command.

In the Free Pass mode a door (turnstile, swing-beam barrier) is permanently open for free passing (without identification and passage detection).

In the Free Pass or Access Locked modes the S2000-2 controller takes into account only special keys (*Unlocking, Locking* or *Master*), as well as keys intended for loop and partition arming/disarming. Presenting an *Unlocking* or *Locking* key restores the Controlled access mode – see Controlled Access Mode Section below. Presenting a *Master* key to a reader switches the S2000-2 to the key programming mode (local key programming — see Key Programming section of this Manual).

The access mode for one S2000-2 reader (access to one direction) can differ from the access mode of another S2000-2 reader (access to another direction).

Access Locked Mode

Access can be locked for a reader by means of one of the following ways:

- by a Locking key presenting to the reader (with the key time schedule and validity being checked)
- by the relevant command of the network controller, received via the RS-485 interface
- by arming of an access locking alarm loop

Access Locked by a Locking Key or Network Controller Command

If access is locked by a *Locking* key or the remote network controller command, the LED of the relevant reader begins flashing with red color (one flash per second with short pauses), the sounders of the controller and the relevant reader, if enabled, playing four beeps.

In such a case an access is locked for all the keys stored in the controller memory (that is, local access is locked). Only centralized access or access by pressing the EXIT button (if exists) is possible. (Centralized access can be denied only by the network controller tools).

Switching to the *Controlled* mode can be implemented by:

- repeated presenting the *Locking* key, or
- presenting the *Unlocking* key, or
- the relevant command of the network controller, received via the RS-485 interface

Access Locked by Arming of Access Locking Alarm Loops

If access has been locked due to the alarm loops locking access are armed, then while presenting a combined key authorized to gain access and to disarm these loops the loops will be disarmed and the access will be granted at the same time. For other keys (authorized to access only or having no rights to disarm access locking loops) access will be denied.

Access locking due to alarm loops is canceled when the locking loops are disarmed.

Free Pass Mode

A reader can be switched to the *Free Pass mode* by the special *Unlocking* key or by the relevant command of a network controller received via the RS-485 interface. After that the reader LED starts flashing with green color (one flash per second with short pauses), the sounders of the controller and the reader, if enabled, playing the combination of one, two and two beeps.

In this mode a free passing is enabled to anyone without presenting any identifier.

In Free Pass mode, the controller sends opening signals to the relevant relay permanently (the relay stays switched on or off). Thus, **this access mode is not applicable for some locking units, such as electromagnetic strikes, for example**.

In the *Two Entrance Doors* and *Turnstile* operation modes each of the readers (access directions) can be switched to *Free Pass* mode independently. In other operation modes (*One Entrance/Exit Door, Swing-beam Barrier, Two Sluice Doors*) when one of the readers is switched to *Free Pass* mode, the other reader is automatically switched to the same mode.

Switching to the *Controlled* mode can be implemented by:

- repeated presenting the *Unlocking* key, or
- presenting the *Locking* key, or
- the relevant command of the network controller, received via the RS-485 interface

Controlled Access Mode

In the controlled mode the controller provides both local and centralized access.

Local access in controlled mode is granted for owners of those identifiers (keys) which:

- are stored in the controller database,
- are not locked currently,
- are authorized to access the specified zone,
- meet the access conditions (the required number of identifiers is presented),
- doesn't violate access rules (a permitted time schedule, an anti-passback rule, key validity),
- and in case of no access locking alarm loop is armed

Also an access can be granted similarly for owners of identifiers (keys) that are not stored in the controller database but meet the requirements of one of access key patterns (if used).

Centralized access is granted by the command of a network controller (the Orion Workstation) for the owners of the keys that are not stored in the controller database and do not meet requirements of any of access key patterns.

Hereinafter the local access will be meant while describing the controller operations unless except for the cases said explicitly.

OPERATING PRINCIPLES

The operating strategy of the S2000-2 controller is determined by actual parameters of the programmed operation mode (Two Entrance Doors, One Entrance/Exit Door, Turnstile, Swing-beam Barrier or Sluice — see below) and access mode (Free Pass mode, Access Locked Mode or Controlled Mode).

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

Access Granting

To have access granted (open a door, lift a swing-beam barrier, etc.), it is necessary to present (to swipe, to touch, etc.) a pre-programmed electronic key (Dallas iButton, Proximity card or PIN code) to the relevant reader of the controller. The key code should be stored in the controller memory, be of the *User* type and intended for access or access + loop arming/disarming (combined).

The S2000-2 controller verifies if the key presented is stored in its database, has relevant access rights, does not violate access rules and meets all required conditions to gain access.

If the presented key is registered by the controller and fit all pre-programmed access rights and limitations then the access will be gained. At that time:

- The sounders of the controller and the readers generate two beeps
- Green LED of the reader is turned on
- The relay is switched (on/off) to open the door (turnstile, swing-beam barrier)
- The ACCESS GRANTED message is generated

If the key code is stored in the controller database and no access rules are violated, but access granting conditions have not yet met (in case of two-factor authentication or two-person access rule, for instance), the controller waits for an additional or confirmation code to be presented:

- The sounders of the controller and the readers generate a beep
- The reader green LED starts flashing 5 times per second
- The relay is not switched
- If case of completed identification was (two-person access rule), the IDENTIFICATION message is generated

If the key code is stored in the controller database, but some access rules are violated (no access rights, a wrong time zone, an anti-passback rule is violated, the key validity period has already been expired, access locking loops are armed), access is denied as follows:

- The controller and reader sounders generate a long *Error* sound
- The red LED of the reader flashes three times and then lit steady;
- The relay is not switched to gain access
- An ACCESS DENIED message is generated.

If the key code is not stored in the controller database and communication with the network controller is lost (the S2000-2 operates standalone), access is denied as follows:

- The controller and reader sounders generate a long *Error* sound
- The red LED of the reader flashes three times and then lit steady
- The relay is not switched to gain access
- An ACCESS DENIED message is saved in the controller event buffer

If the key code is not stored in the controller database and the connection with the network controller is available:

- The controller and reader sounders generate a beep
- The key code is transmitted to the network controller for making an access decision
- The reader LED flashes with red and green alternately 5 times per second until the network controller makes an access decision (it may take from fractions of a second to several seconds).

The network controller can make one of the following decisions:

- To grant access
- To deny access (if the key is unknown for the network controller)
- To reject access (if the key is recognized but has no required access rights or violates some of access rules)
- To arm/disarm a partition (a set of loops) of the fire and intruder alarm system, the reader LED indicating the current partition condition: is lit steady with yellow if the partition is armed, is off if the partition is disarmed, of flashes with yellow once per second in case of a fire or intruder alarm.

Centralized granting, denying or rejecting access (in accordance with a network controller decision) is indicated by the same way as the local access.

In the partition arming/disarming mode the current condition of the partition is indicated by reader LED (yellow light, yellow flashes, or being off). Repeated key presenting inverts the partition condition (disarmed partition will be armed, and vice versa). The condition of the partition is indicated by the reader LEDs within 30 seconds or until another identifier is presented.

When the EXIT button is pressed, access is granted, but the ACCESS GRANTED message is generated without indicating a key code (impersonal).

If the door sensor (passage sensor) is actuated within the standard time to pass or within the relay activation time (whichever is longer), the PASSAGE message is generated, otherwise the access is considered to be not used, and the controller starts waiting for next access procedure to begin. In the both cases (actual passage detection or timeout expiration) the green LED is shut off and the reader LED is switched to the normal mode (which can be off, red light or loop condition indicating).

Alarm Loop Arming/Disarming

In order to arm/disarm alarm loops by a key intended only for this purpose (namely, a key of User type, assigned to an access group with Arming/Disarming flag set on and Access flag unset — see Access Group Parameters Section of this Manual), this key is to be presented to any reader of the controller.

The controller will check if the key record exists in the controller database, is authorized to control the loops, if key time zone is active for the current time and all access conditions are met (if two-factor authentication is applied to the reader an additional code also has to be presented).

If the key is authorized to control alarm loops of the controller, and all these alarm loops are disarmed, they will be armed. Otherwise these loops will be disarmed.

When the loop is being armed, the LED of the reader is switched on for 2 seconds (yellow color). When the loop is being disarmed the LED is switched off for 2 seconds.

In order to arm/disarm loops by means of combined keys (access + arming/disarming, access unlocking + arming/disarming, access locking + arming/disarming) the controller is to be preliminary switched to special *Ready to Arm/Disarm* mode. For this purpose the *Arming Request* button has to be pressed (see Figure 15) and held pressed for at least 1s, until the reader's LED starts flashing rapidly. Instead of using the Arming Request button, both terminals of the iButton reader can be coupled for the same time. After that, while the reader's LED is flashing (20s), the combined key will be interpreted by the controller as arming/disarming request.

If the reader has Touch Memory output interface, in order to arm/disarm loops it is sufficient to hold the combined key presented to the reader within a *Time to Hold Keys for Arming/Disarming* time period. In this case it is not obligatory to switch the controller to the Ready to Arm/Disarm mode. When the card, for example, is held near the reader, the LED flashes with yellow 4 times per second, and after this time has been expired the relevant loop is armed (reader LED is switched on for 2 seconds) or disarmed (reader LED is switched off for 2 seconds). If the card is taken from the reader before the *Time to Hold Keys for Arming/Disarming* time is expired, the main function of the combined card is realize: the access is granted, unlocked or locked.

ALARM LOOPS

In all operation modes except the *Swing-beam Barrier* one, two alarm loops with dry contact intruder alarm detectors brought can be connected to the relevant terminals and monitored by the S2000-2 controller. In the *Swing-beam Barrier* mode the sensors detecting a car located near the readers are included into the alarm loops instead.

Alarm loops are armed (that is the controller is caused to monitor loop conditions) or disarmed by one of the following ways:

- Centralized, by an arming/disarming command sent by a network controller via the RS-485 interface
- Locally, by means of presenting pre-programmed access keys (iButtons, Proximity cards, PIN-codes or its combinations) to a reader of the S2000-2 controller. The keys must be programmed so to have rights for this action and must be stored in the controller memory.

If the key programmed to arm/disarm alarm loops is presented to one of the readers of the controller the alarm loops controlled by this key will be armed if only all this loops were disarmed, or disarmed otherwise.

If the key is programmed not only to arm/disarm alarm loops but also to gain access (that is the key is combined) the controller has to be preliminary switched to the special mode called '*Ready to Arm-/Disarm*' (if not, such key presenting will be considered as an access request). For this purpose the special *Arming Request* button brought into a reader circuit have to be pressed (see Figure 15) and held pressed for more than 1s, until the reader's LED starts flashing at high frequency. Instead of pressing the Arming Request button, both contacts of the iButton reader can be coupled for the same time. After that, while the reader's LED is flashing, the controller will consider the combined key presenting as an arming/disarming request. The Ready to Arm/Disarm mode is valid only for one key reading and is disabled either after presenting the key to the reader, or upon expiration of 20 s, or after repeated pressing the Arming Request button (or coupling iButton reader contacts).

The S2000-2 controller can be programmed so that its loop arming causes the controller to lock local access via any reader's controlled area in accordance with one of the following ways (see *Lock Access If…* parameters, Reader Configuration Parameters Section):

- Do not lock access if the controller loops are armed
- Lock access if the loop 1 is armed
- Lock access if the loop 2 is armed
- Lock access if the loop 1 or the loop 2 is armed
- Lock access if the loop 1 and the loop 2 are armed

Access will be unlocked after disarming of access locking loops.

If one or two access locking alarm loops are armed (depending on *Lock Access If…* parameters setting), presenting a combined key (without entering the Ready to Arm/Disarm mode) will cause disarming the loop (loops) and access granting (of cause, if the key is authorized to disarm the access locking alarm loops). Therefore, in general, the Ready to Arm/Disarm mode has to be activated by pressing the Arming Request button only for arming the loops by means of combined keys, disarming being implemented automatically upon first access granting based on a combined key.

It is possible to arm/disarm alarm loops by means of combined cards (designed for arming/disarming and access) without switching the controller to the Ready to Arm/Disarm mode. For this purpose a non-zero value of the *Time to Hold Keys for arming/disarming* reader parameter has to be set. If the combined card is presented to a reader and keep it presented for the set time, the corresponding alarm loops will be armed/disarmed. If the card is presented for the short time, access will be granted (actual relay actuation and generation of access granted event will take place with insignificant delay, when the card is taken away from the reader). This way of arming/disarming can be used only for a reader with Touch Memory output interface. If the Time to Hold Keys for Arming/Disarming parameter is set to zero, this way of arming/disarming is disabled and the controller will grand access instantaneously.

Not only the User keys, but also Locking and Unlocking keys can be combined (designed for access + arming/disarming). All that is needed — to assign the keys with an access group which is designed to enable alarm loop arming/disarming. To control arming/disarming of the alarm loops by means of such combined keys the controller also has to be switched to Ready to Arm/Disarm mode or the key has to be held near the reader within Time to Hold Keys for Arming/Disarming.

Arming/disarming commands are delivered to the controller via the RS-485 interface the S2000-2 is controlled from a PC, from a S2000/S20000M control console or from one of Orion system devices by using partition arming/disarming mechanism. In particular, this S2000-2 controller can be used to control security and fire alarms in a system.

Transmitting a security system such events as intruder alarms, loop arming, loop disarming or loop arming fault is realized by sending them via the RS-485 interface to a network controller. Alarm messages dealt with alarm loops can be indicated by means of LEDs and sounders of the controller and its readers.

In order to activate sound indication of loop alarms, the relevant category of sound signals has to be activated for the controller or the reader respectively (see System Configuration Parameters and Reader Configuration Parameters Sections of this Manual).

In order to activate visual indication of loop alarms by means of the controller or reader LEDs, the *Indicate Loop Alarms* attributes have to be properly set for the reader (see Reader Configuration Parameters Section of this Manual).

Besides, reader's LEDs can display armed (red lighting) and disarmed (LED is off) conditions of the following loops combinations (defined by Normal Mode Condition parameter — see Reader Configuration Parameters Section of this Manual):

- Alarm loop 1 only
- Alarm loop 2 only
- Alarm loop 1 or alarm loop 2
- Alarm loop 1 and alarm loop 2

The controller provides any loop monitoring for breaking after the relevant arming command receiving only if the loop resistance (taking into account including the terminating resistor included) ranges between 5 kOhm ± 10% to 11 kOhm ± 10%.

No messages are generated by the controller if the loop has been shorted or opened within 50ms.

No messages are generated by the controller if loop resistance value slowly changes at the rate of at most 10% per hour and does not fall beyond the 5 to 11 kOhm range.

An alarm loop when armed is considered to be broken if its resistance is step-like changed by more than 10% or has been out of the 5 to 11 kOhm range for more than 70ms. In this case the controller generated an INTRUSION ALARM message for this alarm loop.

Leakage resistance between the loop wires or between each wire and ground must not be less than 20 kOhm.

TWO FACTOR AUTHENTICATION

Each of the two controller's readers can operate in such a mode when not one but two keys (for example, a Proximity card plus a PIN-code) are required to identify the same user — so called two factor authentication. This mode can be activated separately for each reader by setting the Two Factor Authentication flag (see the description of this configuration parameter in Reader Configuration Parameters Section of this Manual).

The main and additional keys are presented to the same reader of the S2000-2 controller, that is why combinations of different keys can be used only with special combined readers providing reading different keys and transmitting them to the S2000-2 controller in a single format (Touch Memory, Wiegand, or ABA TRACK II).

While an access or alarm loop arming/disarming is requested, the two factor authentication process starts with presenting the first key and reading the so called *Main code*. If the key is identified and there is no access violation, the controller is switched to the second code waiting mode. The reader LED starts flashing with green color 5 times per second. Within the subsequent 30 seconds the second identifier, so called *Additional code*, has to be presented.

If the presented code does not coincide with the Additional code, the controller generates the ACCESS DENIED message with ADDITIONAL CODE ERROR attribute. If the presented additional code is correct, the identification procedure is considered to be successfully finished and either the controller grants access — the green LED of the reader turns on, the lock opening relay is activated (deactivated) and the ACCESS GRANTED message is generated, or the access granted procedure is continued — the reader LED is lit with green for 2 s, the flashes 5 tome per second again and the IDENTIFICATION message is generated, or alarm loops which these keys is controlled by are armed/disarmed.

If the authentication procedure needs to be simplified for some of the keys, while using the two factor authentication for all other keys, it is necessary to set the *Without Additional Code* parameter for such keys. The Main code presenting will be sufficient to identify the keys in question (no additional code is required).

If the *Two Factor Authentication* mode is set for a reader, it will be applied not only for identification of *User* keys, intended for access and loop arming/disarming, but also for identification of special keys such as *Master, Unlocking, Locking*, if of cause the *Without Additional Code* parameter is not set for these keys.

NOTE: Taking into account that in two factor authentication mode the controller has to store in its memory two codes (main and additional) instead of single codes, the maximal number of keys being stored in the S2000-2 controller is twofold reduced (down to 2048), even if the two factor authentication mode is used only for one reader.

ACCESS RIGHTS

To simplify description of the access rights for each key as well as rights to arm/disarm the controller's alarm loops the *Access Group* category is used. Each access group is described as a set of rights and restrictions applied for a group of the keys (users). A process of setting the access rights for all the keys can be thus narrowed down to defining access groups and assigning the relevant access group number with each access key.

In order to define the access rights while adding a new key (user) it is only necessary to include it to the proper access group. Similarly, in order to modify the access rights of keys (users) included to an access group, it is sufficient only edit its descriptor.

Each access group descriptor involves the following set of access rights and restrictions:

- Passage modes to the zones controlled by the readers 1 and 2 (entry and exit modes)
- Time zones permitted for entry/exit or loop arming/disarming (see Time Schedules Section)
- Anti-passback mode (see Anti-passback Rules Section)
- Rights to arm and disarm the controller's alarm loops 1 and 2

Passage Modes and Two or More Person Rule Access Control

The passage modes for an Entry Zone (controlled by the reader 1) and Exit Zone (controlled by the reader 2) can be as follows:

- *Simple Access Control* (by user identifying only)
- Two-Person Rule Access Control
- Three-Person Rule Access Control
- *Confirmation* (to confirm entry or exit rights in cases of two(three)-person rule applying)
- *Locked* (no rights to access the zone controlled by the reader

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 keys with matched access groups to gain access. Implement this by doing the following:

- Activate the *Access* parameter of the access group
- Select the Two Person (Three Person) Access Rule passage mode
- Define the *Access Group 1 to Confirm Passage* parameter (the number of the access group required to be assigned with a first key which must be presented to confirm the passage in case of the two person access rule)

- Define if necessary the *Access Group 2 to Confirm Passage* parameter (the number of the access group required to be assigned with a second key which must be presented to confirm the passage in case of the three person access rule

If a two or three access rule is given for an access group of the presented, the IDENTIFICATION message is generated by the S2000-2 controller, the green LED of the reader starts flashing 5 times per second, and the controller waits during the next 30 seconds for the presenting the key (the keys) assigned with the access group (groups) required to confirm the access rights of the presented key.

If the next presented key is assigned with the unmatched access group and does not meet current access conditions, the controller generates the ACCESS DENIED message with CONFIRMATION ERROR attribute.

If, otherwise, the next presented key is assigned with the matched access group, but none of the keys meet access conditions (three person access rule), the IDENTIFICATION message is generated and during the next 30 seconds the controller waits for the third key to be presented.

If after the second or third key presenting the access conditions are met for at least one of these keys, access is granted. If the controller operates in *Two Entrance Doors* or *One Entrance/Exit Door* mode*,* ACCESS GRANTED messages will be generated for all the keys which meet the access conditions. In all other operating modes, the controller generates the ACCESS GRANTED message for the first key only.

If not all the persons, involved in the two (three) person ruled access procedure, are supposed to enter the restricted zone (for example: a security officer confirms access of another staff member), it is necessary to set the *Confirmation* passage mode for the access group of such the persons. The passage itself is not permitted for the owners of keys such passage mode and no ACCESS GRANTED and PASSAGE messages are generated for such the key during the two (three) person rule access procedure.

Two (three) person rule access control parameters is given for each reader (each passage direction) individually. For example, to entry a zone (to pass into a zone controlled by one of the readers) the two person rule is used, while to exit this zone (to pass into a zone controlled by another reader) the simple access mode (identification of one person only) is sufficient, and vice versa.

Modes of the passing to zones controlled by the first and the second readers of the controller (entry and exit modes) are given for each access group separately. Thus, for example, all members of one access group are accessed to a zone based on the two person rule, while the members of another access group are accessed to the same zone with the simple access mode (via the same reader).

If the two person rule access via one of the controller readers is set for an access group X and an access group Y is selected to be the *Access Group 1 to Confirm Passage* parameter value, then:

- If the two person rule access via the controller reader is set for the access group Y too and the access group X is selected to be the *Access Group 1 to Confirm Passage* for the group Y then access for owners the keys included by the access group X is granted only accompanied by an owner of the key included in the group Y, and vice versa
- If the simple passage mode is selected for the access group Y, then the such key holder is allowed as to confirm access by the access group X key, as to pass in specified direction (via this reader) by himself.

Time Schedules

In order to implement time limitations on user access rights (to control access depending on date, day of the week or time) up to 16 different time schedules can be described for the S2000-2 controller, these time schedules being assigned to relevant access groups.

Each group can be assigned with two time schedules numbered from 0 to 16, the first used for passage limitation and the second used for time limitation of loop arming/disarming. Assigning the number 0 to a time schedule means that no time limitation is applied for this time schedule. Time schedules with the numbers of 1 to 16 are programmed while configuring the controller.

Each time schedule descriptor consists from a time zone list (up to ten time zones can be defined for a time schedule) and a list of holidays for one year.

Each time zone descriptor includes start and stop times of the zone (expressed in hours and minutes), the time zone activity flag for ‘entry’ (passage to the area controlled by the reader 1), the time zone activity flag for ‘exit’ (passage to the area, controlled by the reader 2), and the time activity flags for each day of the week as well as for holidays. If the time schedule is defined for arming/disarming the ‘entry’ and ‘exit’ activity flags mean enabling arming/disarming alarm loops from the first and the second S2000-2 reader respectively.

The ‘holiday list’ allows to reassign 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. At that the reassigned value of the day of the week may take one the following values: 1 (Monday), 2 (Tuesday), … 7 (Sunday), 8 (eighth day of the schedule), … 14 (fourteenth day of the schedule), 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 schedule. Thus, the holiday list allows:

- Announcing any day to be a holiday (that is the day with active time zones different from the zones 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 a ‘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 implement time limitations properly the controller clock has to be synchronized with the network controller. This is provided automatically when the S2000-2 controller operates as a part of the Orion system based on PC or the S2000M/S2000 control console of ver.1.20+, provided that the date and time are set for the PC or the control console. The controller is equipped with a non-volatile clock and calendar, thus the network controller turning off, the RS-485 interface communication fault and even the S2000-2 controller 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 controller operates standalone for a long time its clock can shift. That is why it is not recommended to use time schedules while the controller operates in standalone mode without a network controller: all time schedules for all access groups should have the number 0.

The S2000-2 controller backup battery provides power supply to the S2000-2 clock for at least 5 years.

Anti-passback Rules

Anti-passback rules are used to prevent anyone from repeated access to any access zone without exit from it (repeated access prohibition).

An anti-passback rule is considered by the S2000-2 to be violated if after logging a passage to the access zone of one S2000-2 reader the access to this zone is requested again with logging of the passage to the backward direction (i.e. the passage to the access zone of another S2000-2 reader). The controller behavior in case of an anti-passback rule violation depends on this anti-passback rule (which can be defined for each access group separately) and can be as follows:

- *None* (the S2000-2 controller is not checking any anti-passback rule)
- Hard
- Timed
- Soft

The *Hard Anti-passback* rule requires to prohibit a second passage to a zone up to the moment of logging the exit from it. If someone attempts to violate the rule, access is denied and the ACCESS DENIED message is generated with the *Anti-passback rule violation* attribute.

The *Soft Anti-passback* rule does not prohibit a second passage but in case of its violation the ACCESS GRANTED and PASSAGE messages are generated with the *Anti-passback rule violation* attribute.

The *Timed Anti-passback* rule uses an additional *Anti-passback Lockout Reriod* parameter. During this time period since passing to an access zone the S2000-2 controller is operating as for *Hard Anti-passback* rule (repeated access requests to the zone without exiting it are rejected and ACCESS DENIED messages are generated). After expiration of the specified time the S2000-2 controller is operating as for *Soft Anti-passback* rule (second access is granted, but the ACCESS GRANTED and PASSAGE messages are generated with the *Anti-passback rule violation* attribute).

If the S2000-2 controller operates as a part of an *Orion* system, it checks anti-passback rules taking into account all passages to the access zone registered by other controllers of the system (the *Global* anti-passback rule is implemented). So, if an access zone has several access points (for example, several gate houses to enter/exit from the company premises or several turnstiles operating in parallel) equipped with S2000 controllers, entering the zone via one of the access points will lock the access to the zone through other access points and unlock the access from this zone. Vice versa, leaving the zone via one of the access points will lock exit from the zone and unlock entry to it (of course, if the anti-passback rule checking is programmed for the key presented).

Anti-passback rules will operate properly at an access point between two zones only if two following requirements are met:

- Authorized passing from one zone to another is only possible via the access points controlled by S2000-2 controllers
- Each the access point has to be equipped with two readers providing identification both for entry and for exit as well as a passage sensors.

For the Global anti-passback mode to operate properly all readers controlling entry to a zone must be programmed with the same *Access zone number*. Checking anti-passback rules each S2000-2 controller takes into account a passage registered by any other S2000-2 controller of the Orion system if the passage is relevant to the two access zones which are assigned with the S2000-2 in question. Passages relevant to zones not assigned with the S2000-2 controller are ignored.

An anti-passback rule can be made stronger by setting the *Zonal Anti-passback* ('Entry/Exit Control'). If this parameter is set for an access group the S2000-2 controller takes into account all passages of key owners assigned to the access group to all the access zones programmed within the system. If an access is requested at one of the controller readers then the anti-passback rule requires that the last passage for this key owner was that to the zone which is requested to exit from, that is at the another reader of this S2000-2 controller.

Thus, for example, if the controller is located on the bound between *Zone 1* and *Zone 2* and entering the *Zone 2* is registered followed by entering the *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 Anti-passback* parameter is set, the anti-passback 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 Anti-passback* parameter is not set, the anti-passback 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 Anti-passback* parameter is taken into account only if one of the anti-passback modes (hard, timed or soft) is used. If the *Zonal Anti-passback* is meaningless.

In order to prevent the possibility of simultaneous access of several persons by means of sequential presenting of the same identifier at closely located readers (for example, opening several adjacent turnstiles to pass) after the access is granted until the actual passage is detected, short anti-passback lockout is applied for this identifier at other reader. Namely, if the access is granted for the owner of the key presented at one of the readers and no passage has yet been logged, any attempt to present the same identifier on any other reader (a reader of another controller) will violate the anti-passback rule. If the hard or timed anti-passback mode is used for the reader, the access for this identifier owner will be denied. As soon as the actual passage 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 owner of the specified identifier is possible only through the lane controlled by the reader where the identifier was presented for the last time or through any other lane controlled by a reader where anti-passback rules are not applied for this identifier.

This must be taken into account while designing the access control system at the installation. If some access points exist not far from the access point where anti-passback 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 access granting) 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).

CENTRALIZED ACCESS CONTROL AND ALARM LOOP ARMING/DISARMING

If the S2000-2 controller operates as a part of an *Orion* system, it provides not only local but centralized control for all its operation modes (*Two Entrance Doors*, *One Entrance/Exit Door*, *Turnstile*, *Swing-beam Barrier* and *Two Sluice Doors*). Local control means that codes of keys are stored in the controller memory, so a key owner can gain access only through this local access point or/and only arm/disarm alarm loops of S2000-2 which ‘knows’ the key code. Centralized control means that key codes are stored not in the memory of a S2000-2 but in the memory of a network controller. When the Orion system operates under *ARM Orion Workstation* the owner of any key stored in *Orion* database can gain access through any system access point that is permitted for this key or arm/disarm any permitted alarm loop in the system. If the system operates under C2000/C2000M controller only centralized arming/disarming is enabled.

Similarly to local stored keys centralized control keys can be combined, that is used both for access gaining and partition arming/disarming. Besides, local access can be combined with centralized partition arming/disarming (the *Access* attribute must be set for the access group descriptor of a key in the controller memory to implement such operation).

If an identifier is presented to one of the controller readers and this identifier is unknown to the controller, the code of the identifier is sent to the network controller. The reader LED starts flashing with red and green alternately 5 times per second until the answer from the S2000/S2000M or PC is received (this may 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 (*ARM Orion*) makes the decision to grant access, the centralized access is granted by the same way as the local one.

If the presented key is authorized to arm/disarm a system partition, the current partition status will be displayed by the reader LED as shown in Table 1. Repeated presenting of the key will initiate arming (provided the partition is disarmed) or disarming (in all the other cases) of the partition. Each subsequent presenting of the identifier will initiate activity, which is contrary to previous one, i.e. if the second presenting of the key initiates the partition disarming, the third presenting of the key would initiate the partition arming, etc. If rights assigned to the key are limited, for example, only arming is authorized, the repeated (as well as all the subsequent) presenting of the key will initiate only the authorized action (arming) regardless of the current state of the partition.

If the presented identifier is unknown to the network controller or the identifier has no relevant access rights, the controller indicates access denying so as the controller and reader sounders initiate the long sound signal (Error), the reader LED flashes three times and then lights red steady.

Table 1 Partition Status Indication

Partition Status	Reader Indicator Behavior	Indication Color
Disarmed	Off	–
Armed	On	Yellow (green + red)
Intrusion Alarm Fire Alarm Fire Prealarm Arming Failed	Blinks 2 times per second	Yellow (green + red)
Trouble (in a fire partition)	Flashes once for a second	Yellow (green + red)

If the key unknown to the S2000-2 is presented to one of its readers when the communications between the controller and the network controller is lost, the ACCESS DENIED message is generated. This message (as well as the other ones) is kept in non-volatile memory of the S2000-2 controller, being sent to the network controller as soon as the connection is restored.

If a combined key (for centralized access + partition control or local access + partition control) is presented, it is considered as the key for access request (see below). In order to arm/disarm partitions (alarm loops) remotely by means of this key presenting, the controller has to be switched to Ready to arm/disarm mode, similarly to it is performed when combined keys are used for the local arming/disarming of alarm loops (see Alarm Loop Arming/Disarming and Alarm Loops Sections of this Manual).

The centralized access and partition control are disabled upon the RS-485 communication faults.

If the *Orion* system operates under an *ARM Orion Pro Workstation* of versions 1.11+, such features as two-factor authentication and two (three) person rule access are supported for the centralized access.

KEY PATTERN BASED ACCESS CONTROL

In order to provide identification for a wide range of individuals whose access keys need not or cannot be stored in the S2000-2 or network controller memory (for example, if there are too many keys) the key pattern based access control mode can be implemented by the S2000-2. To make it possible all the key codes which are supposed to be identified by the S2000-2 based on key pattern must meet some specific rule (for example, start from the same numerical sequence).

Each pattern is represented by a base code and a mask that ‘opens’ certain positions of the base code. Only the digits in ‘opened’ positions have a meaning in identifications process. When the digits of the code of a presented key match for ‘opened’ positions with the relevant digits of the base code, access to the key owner is granted with access rights specified for the pattern. The values of other (not ‘opened’) digits of the presented key code are ignored.

In order to limit access rights of all the keys meeting a pattern, each pattern is assigned to a specific access group and specific validity period. Granting access for a person presenting the key which meets to rules of any pattern is equivalent to that for the key which is stored in a controller memory, has access rights of the pattern access group and pattern validity period, except for the following limitations:

- The key can be only of User Type and cannot be Locking, Unlocking or Master
- Anti-passback rules are not monitored (for the keys that are not stored in the controller memory passage events are not logged)
- Two-factor authentication cannot be implemented (neither main nor additional key codes are stored in the controller memory)

When a key is presented to a reader of the S2000-2 controller the controller first checks if the presented key code is stored in its database. If the key code is not found in the controller memory, it is checked against the first access key pattern, then against the second one, etc. So if the code is stored in the controller database, the access rights set for this specific key will be applied. Otherwise, if the code is not stored in the controller memory, but meets at least one key pattern, access rights set for this specific key pattern will be applied (for the first of the key patterns, if the code meets several key patterns simultaneously).

NOTE: It should be kept in mind that the keys that are used for centralized access and/or arming/disarming must neither be stored in the controller memory no meet any access key pattern programmed.

Up to five different key patterns can be programmed for the S2000-2 controller. By default, all the five patterns are locked, that is the key pattern based access control mode is disabled. In order to enable identification based on a key pattern it is necessary to unlock one of the available patterns, enter the base code of the pattern (type manually or read by presenting to a reader one of the keys which code meets the pattern) and specify the pattern mask (its ‘opened’ positions) which will be allied to codes of presented keys. Finally, the access group and validity period must be specified for the pattern (see Access Key Pattern Configuration Parameters Section of this Manual).

A typical example of key pattern based identification is an access control to an ATM for bank clients, when the access is granted only for those cardholders whose bank card serial numbers start with the specified numerical sequence.

LIGHT AND SOUND ALARMS

The S2000-2 controller transmits signals to its built-in LEDs and sounder, as well as to LEDs and sounders of the readers.

READY LED indication is shown in Table 2.

The indication of reader LEDs is similar to that of the 1 and 2 controller LEDs and is shown in Table 3.

The behavior of reader sounders is similar to the behavior of the S2000-2 sounder and is shown in Table 4.

Table 2 READY LED Indication

S2000-2 Condition/Event	READY LED Behavior
Quiescent mode	On
Power fault (the supply voltage is out of normal range)	Flashes twice per second
Programming a Master key	Double short flashes with long pauses
Test mode	Flashes 5 times per second

Table 3 Reader LED and Controller 1 and 2 Indication

Condition/Event		Lighting Mode	Color
Quiescent mode (controlled access mode with no alarms)	LED standby mode – **1** (off)	Off	–
	LED standby mode – **2** or **3** (loops are armed)	On if the loops are armed Off if they are disarmed	Red
	LED standby mode – **4** (red lit)	On	Red
Access Locked mode		On with short pauses	Red
Free Pass mode		On with short pauses	Green
Access is granted and a passage is expected		On	Green
A Main code is recognized, no access violations, an Additional code reading is expected		Flashes 5 times per second	Green
A Confirmation code reading is expected (two person access rule)		Flashes 5 times per second	Green
Access is denied		Three rapid flashes	Red
The key presented is not known to the S2000-2 controller and the decision of the network controller is expected		Flashes with red and green alternately 5 times per second	Red/Green
Loop alarm*		Flashes twice per second	Red
Loop arming fault*		Flashes twice per second	Green

Condition/Event	Lighting Mode	Color
Centralized partition control, the partition is armed	On	Yellow (Red + Green)
Centralized partition control, the partition is disarmed	Off	–
Centralized partition control, an alarm within the partition	Flashes twice per second	Yellow (Red + Green)
The pause after a car has passed before the swing-beam barrier is lowered down	Flashes twice per second	Red
The door is expected to be closed after entering or exiting the sluice	Flashes 5 times per second	Red
Programming access keys	Flashes with red and green alternately twice per second	Red/Green alternately
Programming a Master key	Double flashes with red and green alternately	Twice red/Twice green
* – the condition is indicated only if this loop's alarm indication is permitted for this reader		

Table 4 C2000-2 Sounder and Reader Sound Signaling

Condition/Event	Category	Sound Signaling
Quiescent mode	–	Off
Access is granted	Access	Two beeps
Access is denied	Access	Long sound (Error)
A main code is recognized under two factor authentication condition	Access	A beep
A first key is presented under two-person rule access condition	Access	A beep
For the Turnstile, Swing-beam Barrier, and Two Sluice Doors operating modes, while requesting the access to one direction a key for the access to another direction is presented	Access	Two short and one long sounds ('Please wait')
Access is opened by a special key	Access	Short + 2 short + 2 short sounds ('Access is opened')
Access is locked by a special key	Access	Long + 4 short signals ('Access is locked')
Controlled access mode recovery by a special key	Access	2 short + 2 short + short sounds ('Access is controlled')

Condition/Event	Category	Sound Signaling
Forced open (the door is open without access granted)	Door Held or Forced Open	Interrupted sounds 4 times per second
Held open (the door is open for more than a specified time, 20 s by default)		
Loop Alarm	Loop Alarms	Interrupted sounds 2 times per second
Entering the User key programming mode	Programming	Three pairs of short sounds ('Programming')
Exiting the User keys programming mode	Programming	3 short + long sounds ('Programming is finished')
Entering the Master key programming mode	Programming	'Master Programming' melody
A Master key is programmed	Programming	The final part of the 'Master Programming' melody
A key is added or modified while the controller being in key programming mode	Programming	Two short sounds ('Code saved confirmation')
Presenting an existing key while the controller being in key programming mode	Programming	A short sound ('The key has already been enrolled')

NOTE: Sound alarms can be disabled for any signal category (Access, Door Held or Forced Open, Programming, or Loop Alarms) both for the C2000-2 built-in sounder and each sounder of the readers individually. It can be done while programming the relevant parameters of S2000-2 by means of the UProg Configuration Tool — see S2000-2 Programming Section of this Manual.

DATA COMMUNICATIONS VIA RS-485 INTERFACE

The S2000-2 controller connected to an Orion network via RS-485 interface transmits condition and trouble messages to the network controller, enabling remote alarm and trouble indication. These messages are displayed by the network controller and can be redirected to other devices of the Orion system, such as indicator modules or relay modules, for external alarm devices or executive modules switching on as well as remote notification via a dedicated channel, phone line, GSM, Internet and so on.

Condition Message Transmission

The S2000-2 controller is designed to send automatically condition and trouble messages to a network controller through RS-485 interface line, among them:

IDENTIFICATION	RIP-12 RS power has just been turned up
ACCESS GRANTED	Upon two-person or three-person rule passage mode identifying of first key is completed
PASSAGE	Passage of a person is detected after access granted
ACCESS DENIED	Access is denied for the presented access key
ILLEGAL CODE	The unknown access key is presented to the reader after the S2000-2 with the network controller communications have been lost (the message is stored in the S2000-2 memory)
ACCESS CLOSED	Access through the walkway, doorway or lane is locked
ACCESS FREE MODE	Access control is deactivated
ACCESS NORM MODE	Access control has just been activated
DISARMED	The alarm loop has just been disarmed and is not being monitored
ARMED	Monitoring for the alarm loop conditions has just been activated
ARM FAILED	Arming has failed because the loop is still disturbed
INTRUSION ALARM	
USER’S CODE ENTR	A loop arming/disarming identifier has been submitted to the reader
DOOR LEFT OPEN	The door is open too long (for more than a specified time)
DOOR FORCED	The door is forced open without access granted

DOOR CLOSED	The door has just been closed after being propped open or forced open
TAMPER ALARM	S2000-2 enclosure has just been opened
TAMPER RESTORE	S2000-2 enclosure has just been closed
POWER FAILED	The device input voltage is out of range
POWER RESTORED	The device power supply has just been repaired after a failure
BATTERY FAILED	The voltage of the controller clock battery has dropped or the battery is removed
BATTERY RESTORED	The voltage of the controller clock battery has just been restored
PROGRAMMING	The controller is switched to the programming mode by means of a Master key or Master key re-programming

S2000-2 controllers provide buffering of events that should be transmitted to a network controller. 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 internal S2000-2 clock.

The event buffer capacity is 2047 events for a S2000-2 or 4095 events for a S2000-2 rev.01.

Remote Control via RS-485 interface

The S2000-2 controller responds to commands received via RS-485 interface line from a network controller or supervisory Orion application software, such as S2000(M) console, ARM Orion (Pro), or UProg Configuration Tool. These commands include:

- The S2000-2 with a net controller clock synchronization
- Remote S2000-2 programming
- Remote network address assigning
- Remote alarm loop arming/disarming
- Remote access control, as well as remote access locking/unlocking
- Remote reading the list of programmed key codes
- Remote key descriptor adding/editing/deleting
- Remote requests for reading alarm loop resistance values in ADC units.

INSTALLATION

STANDARD DELIVERY

Find the following when unpacking the S2000-2 controller:

- S2000-2 Access Controller
- This User’s Manual
- Six 8.2 kOhm Terminating Resistors
- Three Woodscrews
- Three Wallplugs
- DIN 7982 Flat Head Tapping Screw with Cross Drive 2,2x6,5

S2000-2 MOUNTING

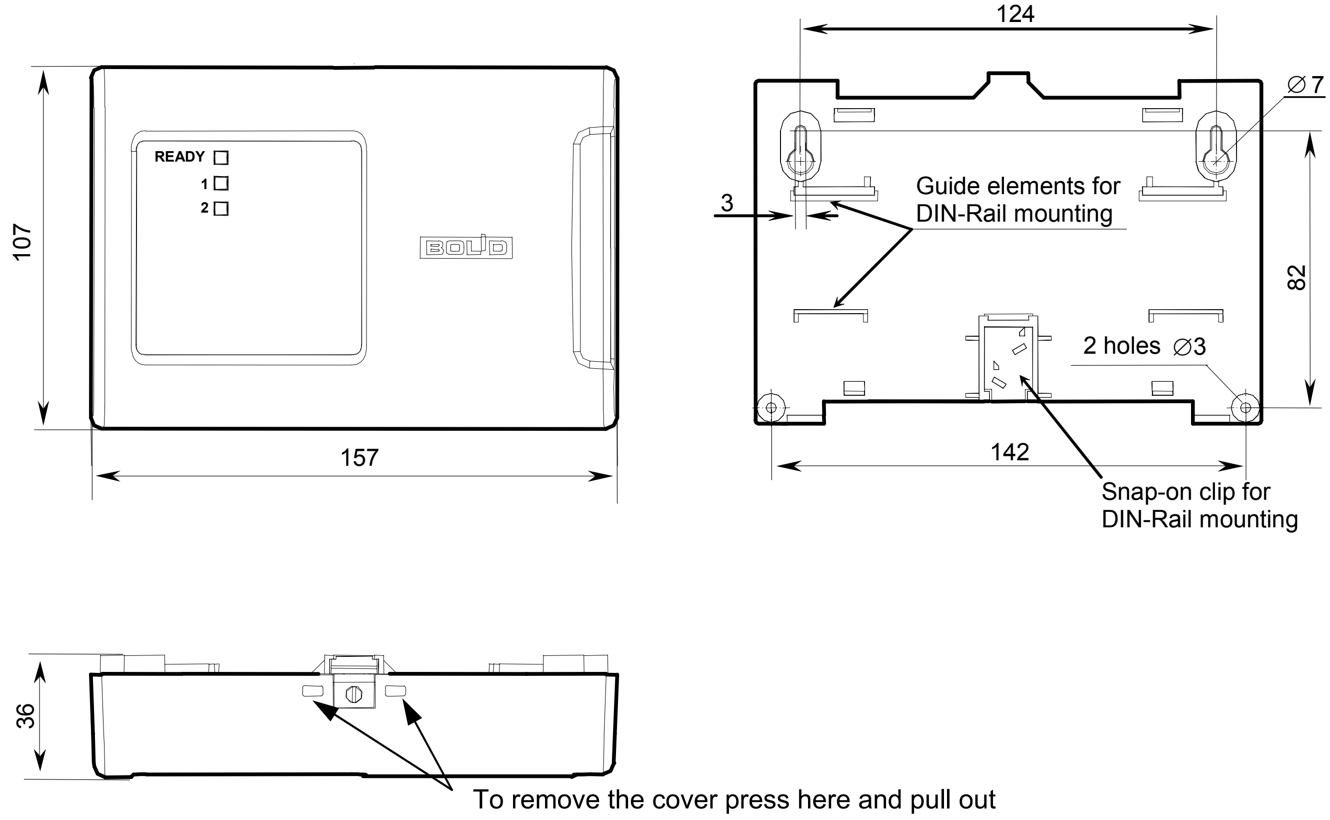

124
∅7
READY
1
2
107
157
3
Guide elements for DIN-Rail mounting
82
2 holes ∅3
142
Snap-on clip for DIN-Rail mounting
36
To remove the cover press here and pull out

Figure 2. S2000-2 Overall and Mounting Dimensions

The S2000-2 controller is to be mounted on walls and other constructions within remises which are protected against atmospheric fallouts, mechanical damage and unauthorized access.

S2000-2 overall and mounting dimensions are shown in Figure 2.

S2000-2 PCB LAYOUT

The layout of the S2000-2 access controller PCB is shown in Figure 3.

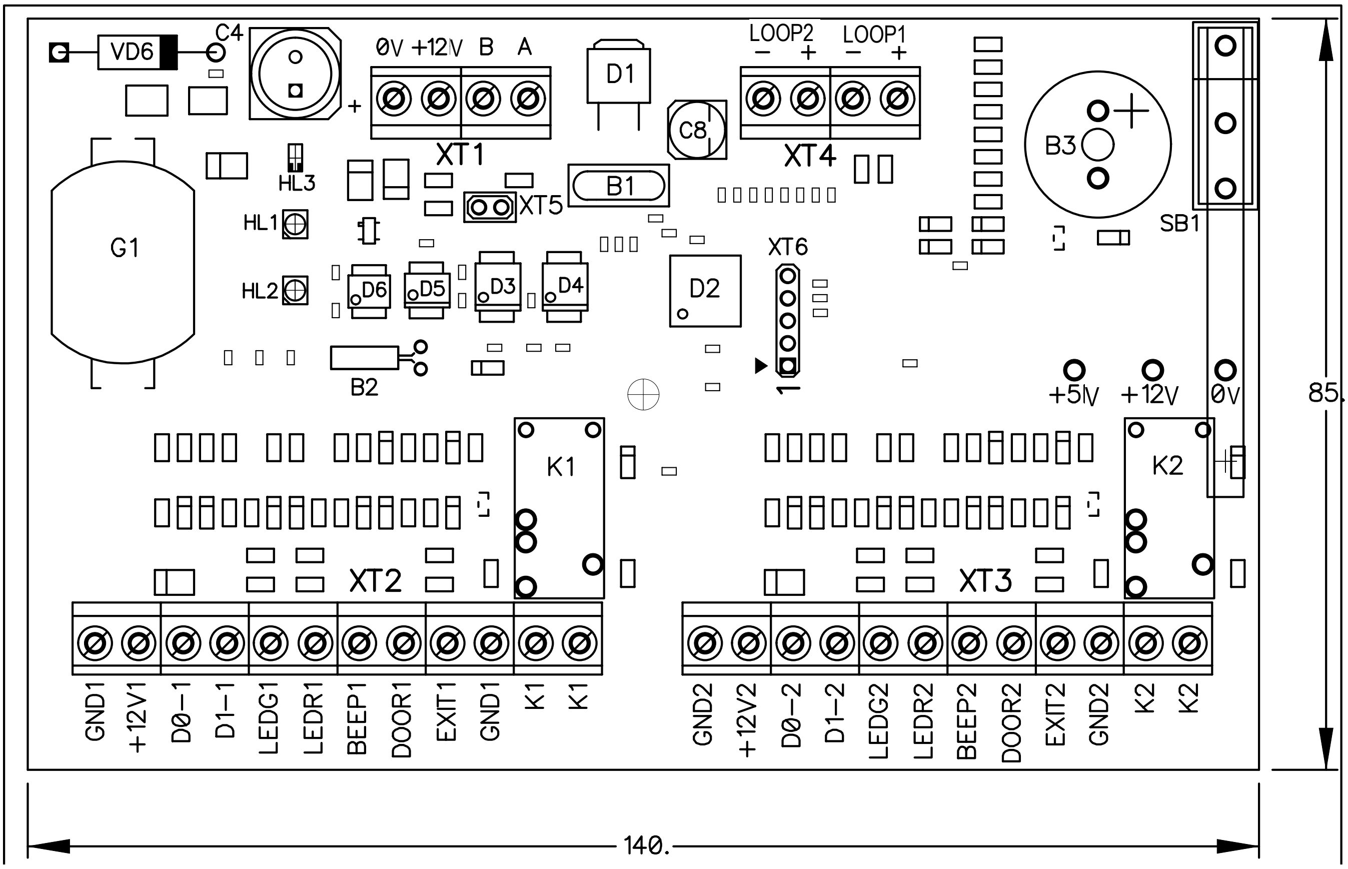


Figure 3. S2000-2 PCB Layout

WIRING THE S2000-2 FOR TWO ENTRANCE DOORS MODE

Figure 4 shows the wiring diagram for a S2000-2 controller operating in the *Two Entrance Doors* mode. In this operating mode alarm loops are not involved in access strategy and are not shown in the connection diagram. However they can be used as intruder alarm loops in the Orion system in which the S2000-2 controller operates on-line (see Alarm Loops Section of this Manual).

The first door equipment (the reader, the lock, the EXIT button, the door sensor) are connected to the controller terminals marked with digit 1 at the end. The second door equipment is to be connected, accordingly, to the terminals marked with digit 2 at the end.

Electromagnetic locks (strikes) can be powered by the same power supply as the controller, or by the separate one. If its are powered by the same power supply, power circuits of the controller and the lock must be wired separately and be connected only at the power supply terminals.

Please note that Free Pass Access mode can not be implemented for an access point if the electric strike is used as a locking unit.

If the readers are suitable for input current consumption more than 100 mA or they are located far from the controller (100m and above), to power them the separate pair of wires must be used which leads directly to the power supply (against the case shown on the scheme when the readers are powered via the controller terminals).

If a reader is powered by a separate supply, the GND circuits of the controller and the reader must be coupled, i.e. the terminal +12V1 of the XT2 terminal block (terminal +12V2 of the XT3 terminal block) is not to be connected to the reader, while terminal GND1 (GND2) is always connected to it.

When passing through the doors in backward direction the lock is opened by EXIT button pressing.

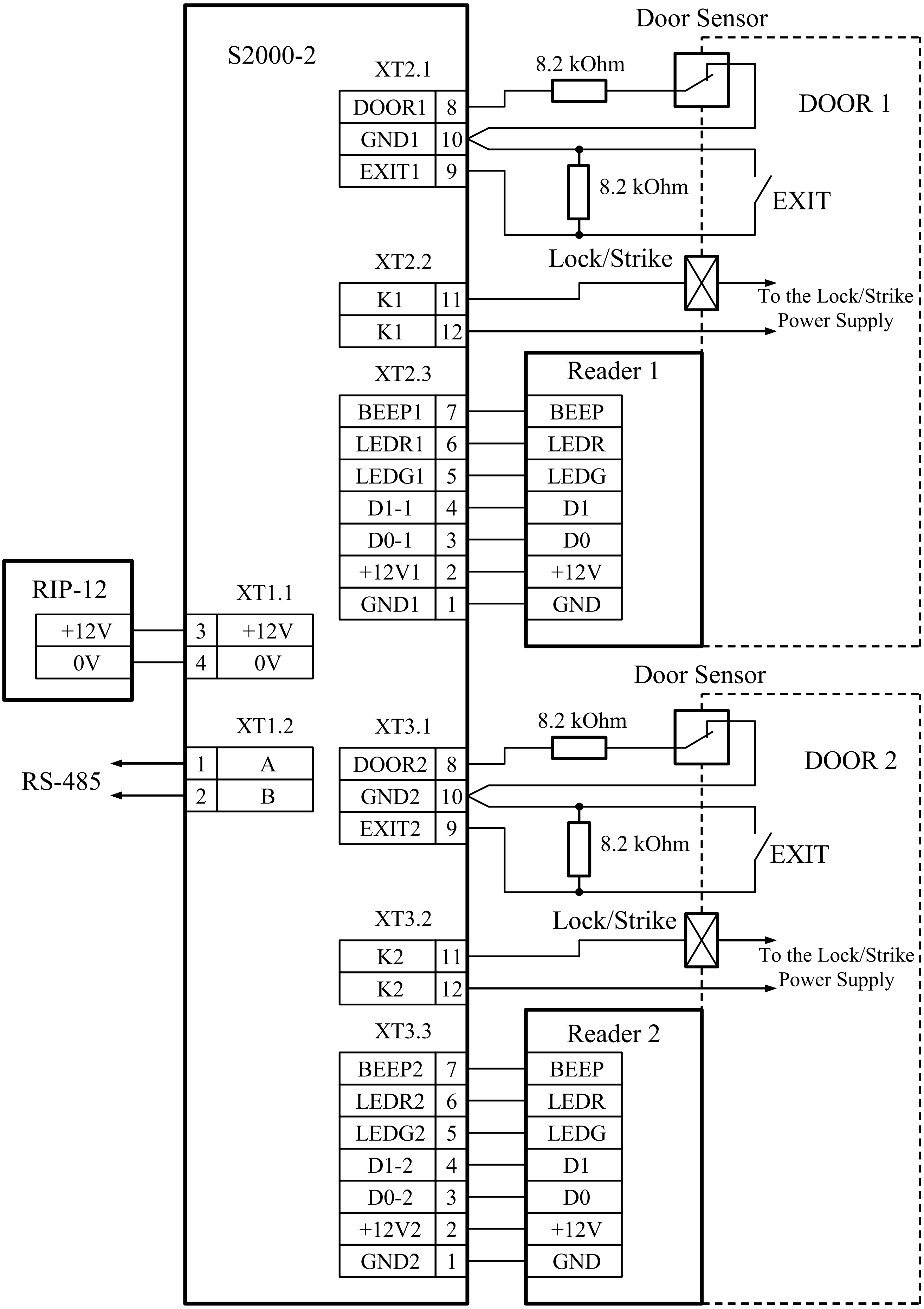


Figure 4. S2000-2 Wiring for the Two Entrance Doors Operation Mode

WIRING THE S2000-2 FOR ONE ENTRANCE/EXIT DOOR MODE

Wiring diagram for a S2000-2 controller operating in the *One Entrance/Exit Door* mode is given in Figure 5. In this operation mode alarm loops are not involved in access strategy and are not shown in the connection diagram. However they can be used as intruder alarm loops in the Orion system in which the S2000-2 controller operates on-line (see Alarm Loops Section of this Manual).

In order to control a lock and monitor for door sensor condition the first channel of the controller is used. Neither second relay nor second door sensor is used in this operation mode.

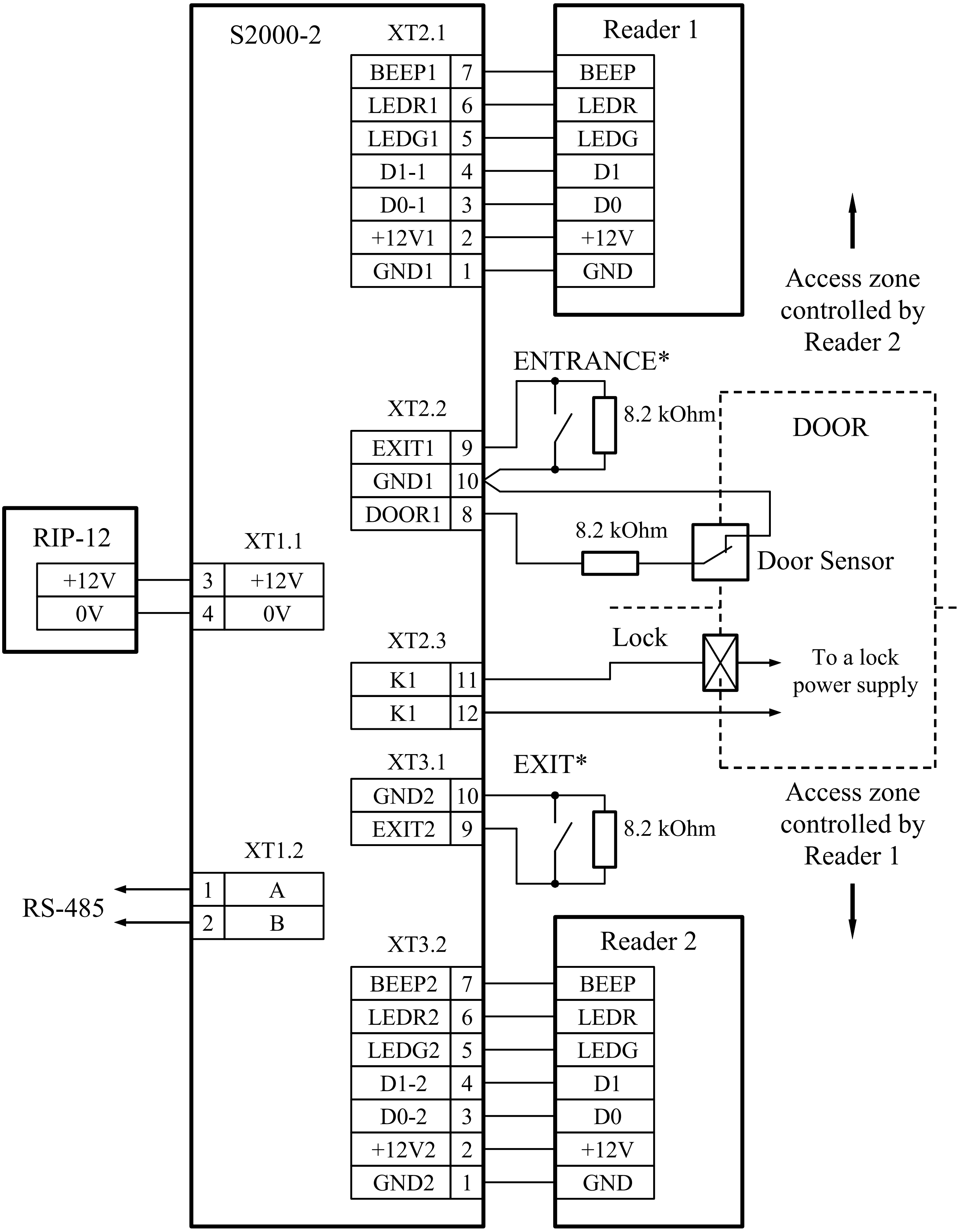
ENTRANCE and EXIT buttons along with the 8.2 kOhm terminating resistors are connected if necessary, e.g. to grant access from a guard post.

Electromagnetic locks (strikes) can be powered by the same power supply as the controller, or by the separate one. If its are powered by the same power supply, power circuits of the controller and the lock must be wired separately and be connected only at the power supply terminals.

Please note that Free Pass Access mode can not be implemented for an access point if the electric strike is used as a locking unit.

If the readers are suitable for input current consumption more than 100 mA or they are located far from the controller (100m and above), to power them the separate pair of wires must be used which leads directly to the power supply (against the case shown on the scheme when the readers are powered via the controller terminals).

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



* – ENTRANCE and EXIT buttons are used if required

Figure 5. S2000-2 Wiring for the One Entrance/Exit Door Operation Mode

WIRING THE S2000-2 FOR TURNSTILE MODE

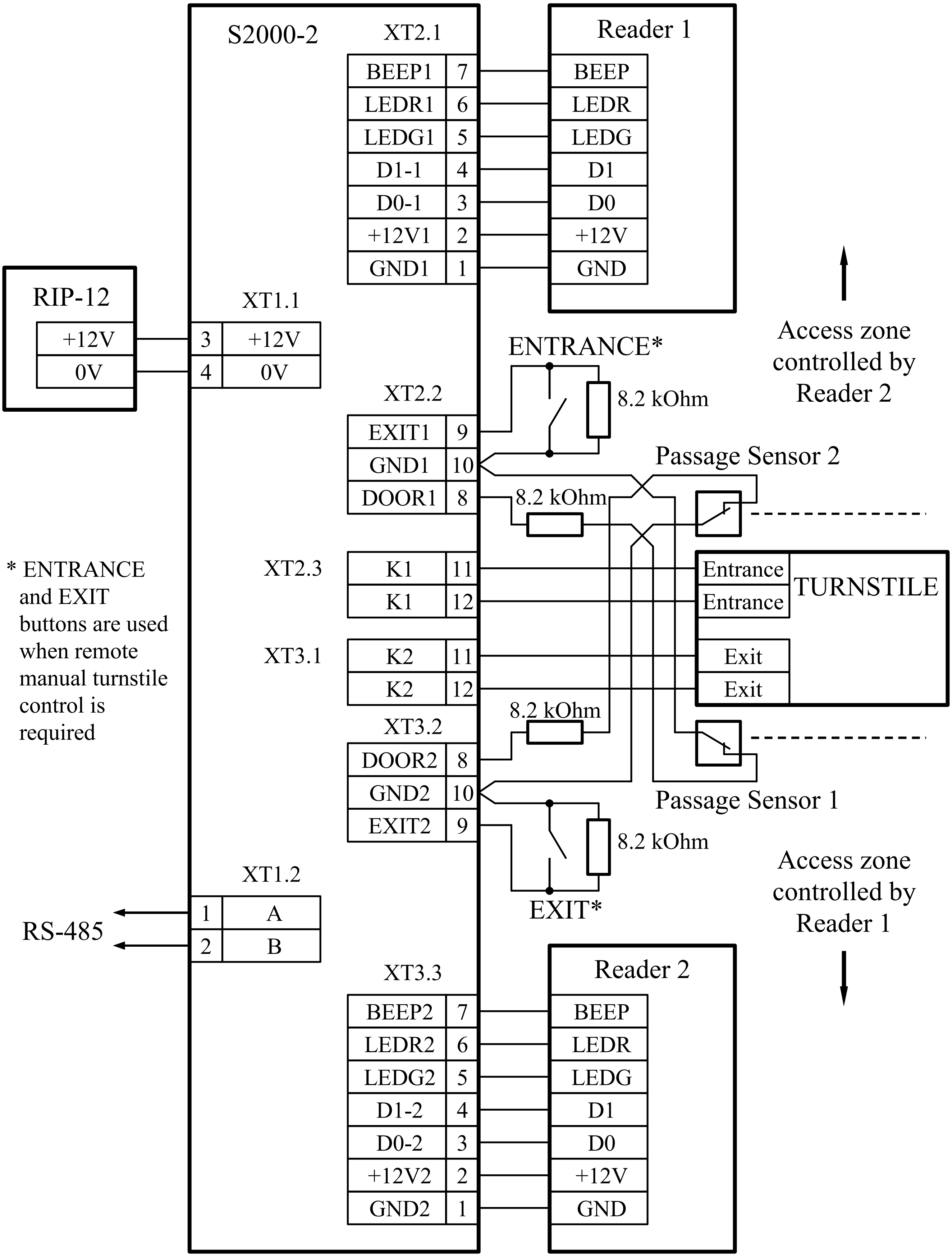


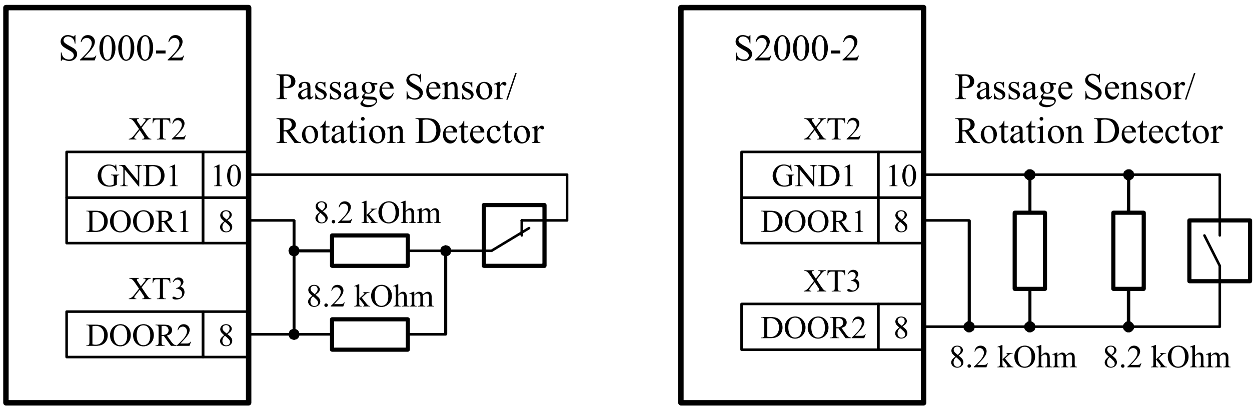
Figure 6. S2000-2 Wiring for the Turnstile Operation Mode

Figure 6 shows wiring diagram for a S2000-2 controller operating in the *Turnstile* mode. In this operation mode alarm loops are not involved in access strategy and are not shown in the connection diagram. However they can be used as intruder alarm loops in the Orion system in which the S2000-2 controller operates on-line (see Alarm Loops Section of this Manual).

This diagram implies that gaining access for entry and exit is performed by closing the relevant pairs of the turnstile contacts, designated as the *Entrance* and *Exit* in Figure 6.

The diagram shows wiring dry contact passage sensors with NC output (that are being opened to gain access). Wiring passage sensors or turnstile rotation detectors of other output type is considered in Connecting Door or Passage Sensors Section of this Manual. These can be either single sensors or outputs of a turnstile control system.

If the turnstile is equipped with a single bi-directional rotation sensor, which detects passages in each direction, it is connected in parallel across the relevant inputs of both control channels of the controller, as shown in Figure 7.



Wiring of a normally closed sensor

Wiring of a normally opened sensor

Figure 7. Passage Sensor/Rotation Detector Wiring Diagram

In order to control the turnstile manually any buttons connected to the EXIT1 and EXIT2 terminals of the controller can be used. The events about manual access granting by key pressing followed by subsequent passing are registered by the controller and saved in the event log of the ARM Orion Workstation or the C2000/C2000M console. If the remote control provided with the turnstile is used for manual access gaining, the facts related to access granting without S2000-2 participation are not logged.

If the readers are suitable for input current consumption more than 100 mA or they are located far from the controller (100m and above), to power them the separate pair of wires must be used which leads directly to the power supply (against the case shown on the scheme when the readers are powered via the controller terminals).

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

WIRING THE S2000-2 FOR SWING-BEAM BARRIER MODE

Figure 8 shows the wiring diagram for a S2000-2 operating in the *Swing-beam Barrier* mode.

In this mode the first relay is used to lift the swing-beam, while the second relay is used to lower it down. ENTRY and EXIT buttons are used to grant access remotely, e.g. from a guard post.

It is implied in this diagram that lifting the swing-beam is implemented by closing swing-beam barrier control unit contacts denotes as ‘Lift’, while lowering the swing-beam down is implemented by closing swing-beam barrier control unit contacts denotes as ‘Lower’. If swing-beam barrier control requires switching of voltage more than 30V, or electric current more than 7A, or power more than 100W, power relays has to be connected to the controller relay outputs. In such a case the controller relay will switch the contacts of the power relay, while the power relay contacts will in turns switch the contacts of the swing-beam barrier electric drive.

If only the opening relay is required to control the swing-beam barrier (with lowering being implemented automatically after cancellation of the open command) then the first S2000-2 relay is to be used. The Relay Activation Time in such a case is set to value no less than standard passage time (30s), preventing a car from swing-beam being lowered down on it (the relay 1 will be activated until the car has driven off the swing-beam barrier).

Car presence detectors causing the controller to make access decisions only if there is a car near the reader when a key is presented to it are to be connected to the alarm loop contacts of the controller.

Passage sensors are used for such an operation mode not only to detect a passage but to prevent the swing-beam from lowering down on a car. If at least one of the sensors is activated, the swing-beam will not be lowered. For this reason the sensors (generally, optical beam sensors) are located from both sides of the swing-beam barrier, so that any car located under the swing beam causes at least one car presence detector to actuate.

The diagram shows how to wire NC output dry contact passage sensors that are opened when the access is being granted. Wiring passage sensors of another output type is considered in Connecting Door or Passage Sensors Section of this Manual.

Instead of two passage sensors located at the both sides of the swing-beam barrier it can be possible to use a single sensor located strictly under the swing-beam (near the swing-beam). In such a case it is wired in parallel across the relevant inputs of both control channel of S2000-2 as shown in Figure 7.

Along with the LEDs of the readers (or instead of them) two traffic lights operated by +5 V CMOS logic signals can be connected to the LEDG1, LEDR1 and LEDG2, LEDR2 terminals of the controller.

In order to control the swing-beam barrier manually from a guard post, the buttons connected to the EXIT1 and EXIT2 terminals of the controller are used. If the swing-beam barrier is lowered down, pressing any of the buttons will lift the swing-beam, and if it is lifted up, pressing any button lowers it down, even if the current procedure has not been competed.

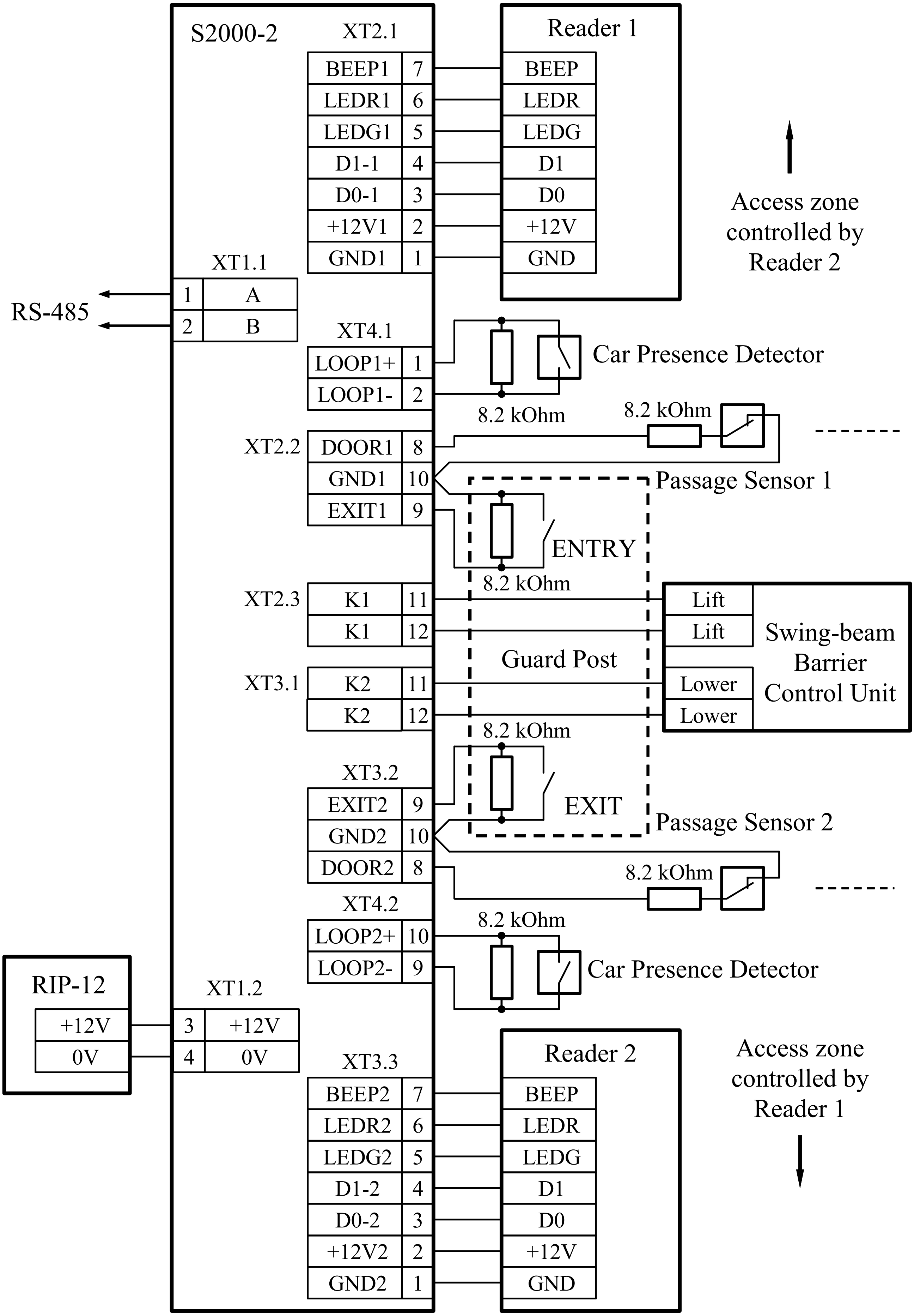


Figure 8. S2000-2 Wiring for the Swing-beam Barrier Operation Mode

If access is granted by ENTRY button pressing, the green LED of the first reader and/or green light on the traffic control unit directed to the first reader is switched on.

If access is granted by EXIT button pressing, the green LED of the second reader and/or green light on the traffic control unit directed to the second reader is switched on.

In the Access Locked mode the swing-beam barrier can be lifted only with the help of ENTRY and EXIT buttons. Pressing these buttons in the Free Pass mode is ignored.

If car presence detectors are used, all reader identifications are ignored when no car is staying near the reader (more strictly, near the car presence detector). The diagram shows connection of the car presence detectors with NO contacts (closed in the presence of a car). Connection of detectors with NC contacts is shown in Figure 9. If no car presence detectors are used, the LOOP1+, LOOP1–, LOOP2+ and LOOP2– terminals of the controller are left unconnected.

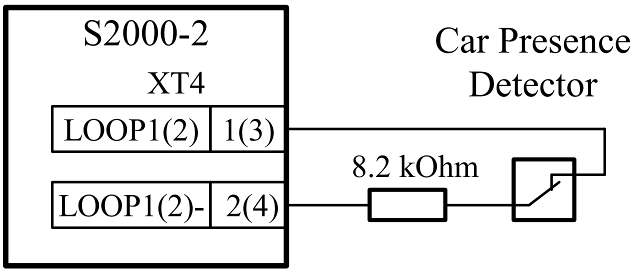


Figure 9. NC Car Presence Sensor to LOOP1 and LOOP2 S2000-2 Terminals Wiring Diagram

If reader current consumption exceeds 100 mA or the readers are located far from the controller (100m and more), they must be wired directly to the power supply (the connection diagram shows the readers are powered via the controller terminals).

If a reader is powered by a separate power supply, the GND circuits of the controller and the reader must be coupled.

WIRING THE S2000-2 FOR TWO SLUICE DOORS MODE

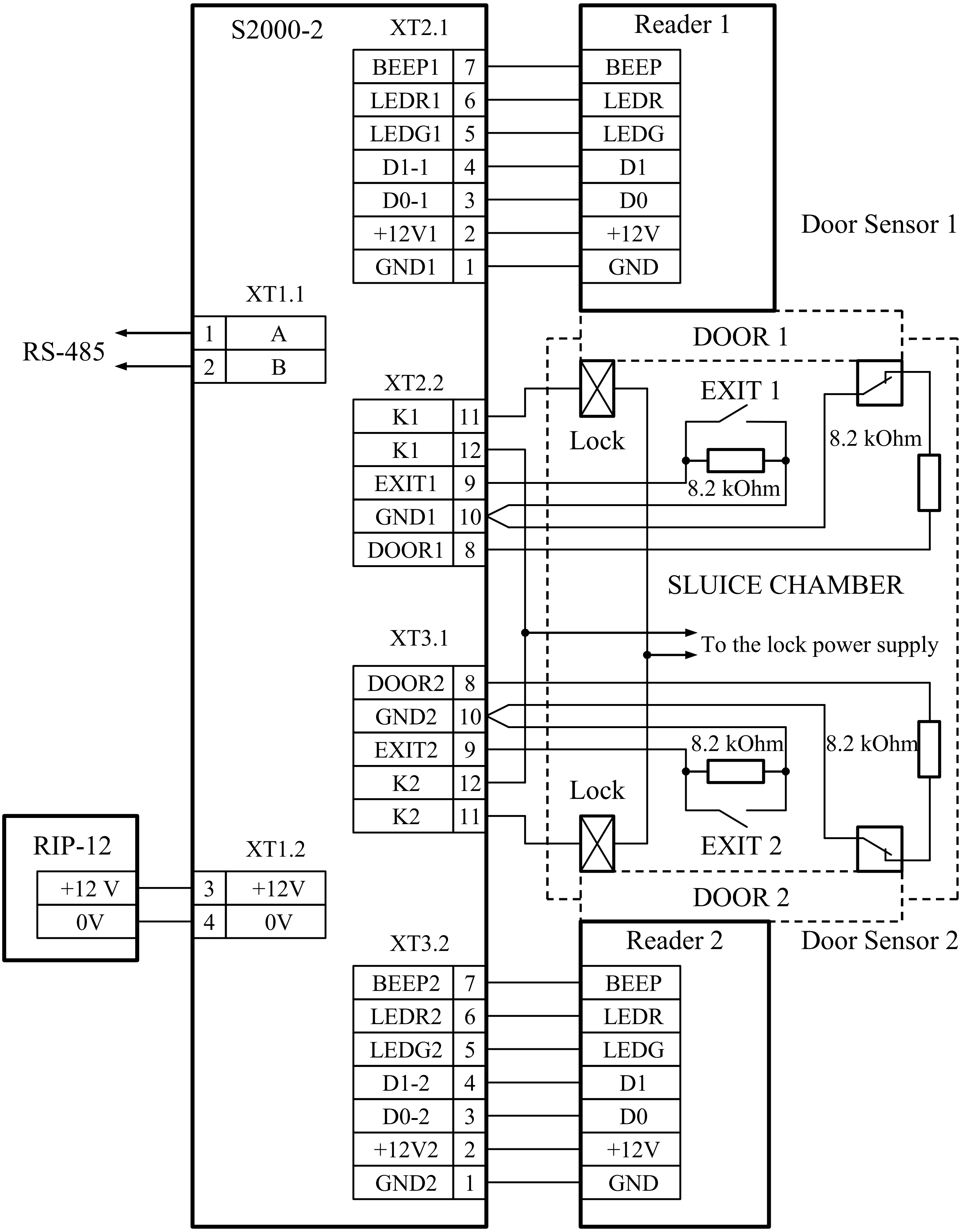


Figure 10. S2000-2 Wiring for the Two Sluice Doors Operation Mode

Wiring of a S2000-2 controller operating in *Two Sluice Doors* mode is shown in Figure 10. In this operation mode alarm loops are not involved in access strategy and are not shown in the connection diagram. However they can be used as intruder alarm loops in the Orion system in which the S2000-2 controller operates on-line (see Alarm Loops Section of this Manual).

Installing at a guard post switches disabling EXIT buttons inside the sluice (as shown in Figure 11) makes it possible to control the way to leave the sluice which can be either ‘Automatically’ (without an additional control of a security guard) or ‘Confirmation’.

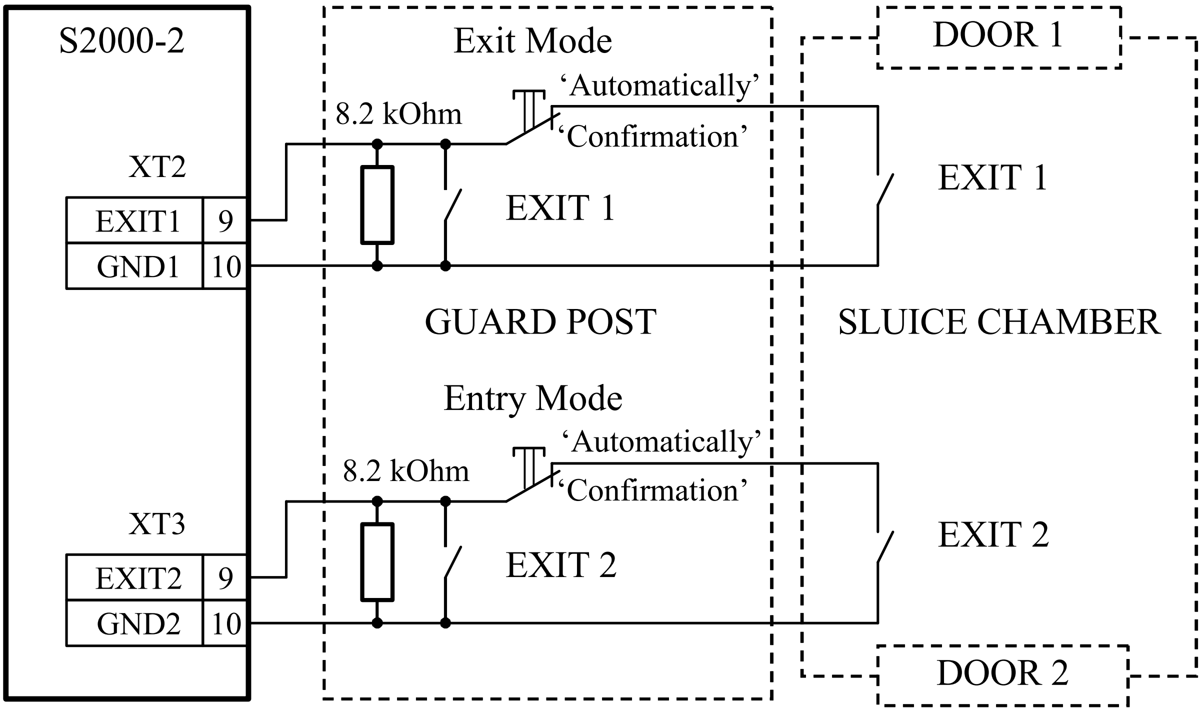


Figure 11. Sluice Leaving Mode Switches Applying

Electromagnetic locks (strikes) can be powered by the same power supply as the controller, or by the separate one. If they are powered by the same power supply, power circuits of the controller and the lock must be wired separately and be connected only at the power supply terminals.

If the readers are suitable for input current consumption more than 100 mA or they are located far from the controller (100m and above), to power them the separate pair of wires must be used which leads directly to the power supply (against the case shown on the scheme when the readers are powered via the controller terminals).

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

Wiring door sensors (door open detectors) in such the operation mode is obligatory.

CONNECTING READERS

In order to identify users, two readers with Touch Memory, Wiegand or ABA TRACK II (magnet cards) output interface are to be connected to the S2000-2 controller. The S2000-2 terminals used to connect the first and the second reader are similar and described in Table 5.

Table 5. S2000-2 Terminals to Connect a Reader

Terminal Designation		Input or Output	Assignment
D0	Touch Memory	Input/output	Reader's data
	Wiegand	Input	D0 data
	ABA TRACK II	Input	DATA data
D1	Touch Memory	–	Unused
	Wiegand	Input	D1 data
	ABA TRACK II	Input	CLOCK signal
LEDG		Output	Controls the green LED of a reader
LEDR		Output	Controls the red LED of the reader
BEEP		Output	Control the sounder of a reader

NOTE: The number 1 or 2 at the end of the terminal designation points the 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.

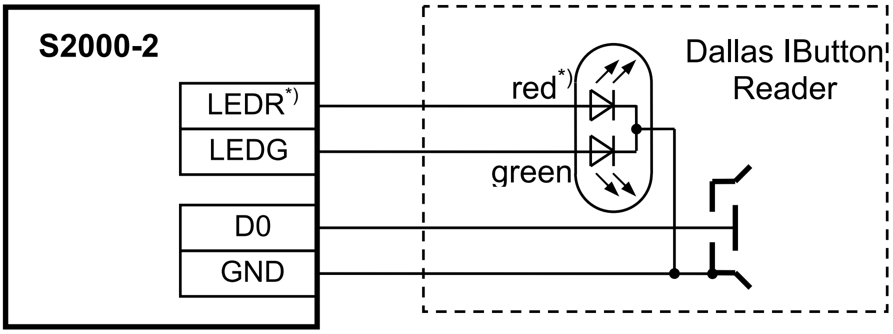
When designing an access control system it is required to follow the recommendations given below.

If readers with different interface types (Touch Memory, Wiegand-26, Wiegand-44, etc.), designed for operating with identifiers of the same type are connected to various S2000-2 controllers of the Orion system, the code of an identifier presented to one reader can differ with the code of the same identifier presented to another reader. For instance, the code of a Proximity card presented to a reader with the Wiegand-26 interface is not equal to the code of the same card presented to a reader with the Wiegand-44 or the Touch Memory interface. Respectively, a PIN code, entered to a reader with the Wiegand-6 or Wiegand-8 interfaces (each entered number is sent to the controller apart from another), will differ from the same code entered to a reader with the Wiegand-26 or Touch Memory interface (all code numbers are sent to the controller as a whole).

So it is advisable to use readers with the same format of output data in a system. Also it is advisable to use compatible formats for readers with different interfaces. For example, the 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.

Wiring diagrams for some models of readers are shown in the Appendix.

Connecting Dallas IButton Readers



*) If a Dallas IButton Reader is equipped with a single color LED it must be connected to the S2000-2 LEDG contact without regard to actual lighting color

Figure 12. Dallas IButton Reader Wiring Diagram

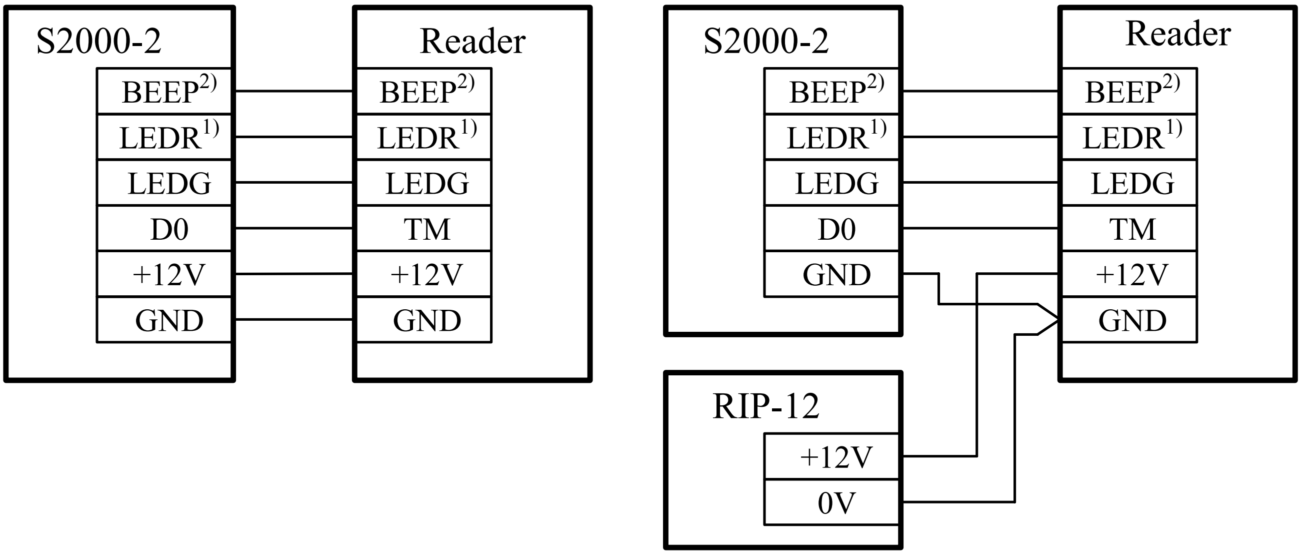
Connecting Readers with Touch Memory Output Interface

Variant 1

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

Variant 2

is intended for readers with high current consumptions or far from the controller more than 50m



1) If a reader is equipped with a single LED control circuit this circuit is to be connected to the LEDG terminal of S2000-2, with LEDR terminal being left unconnected

2) If a reader is equipped with no built-in sounder the BEEP terminal of the S2000-2 controller is to be left unconnected

Figure 13. Reader with Touch Memory Output Interface Wiring Diagram

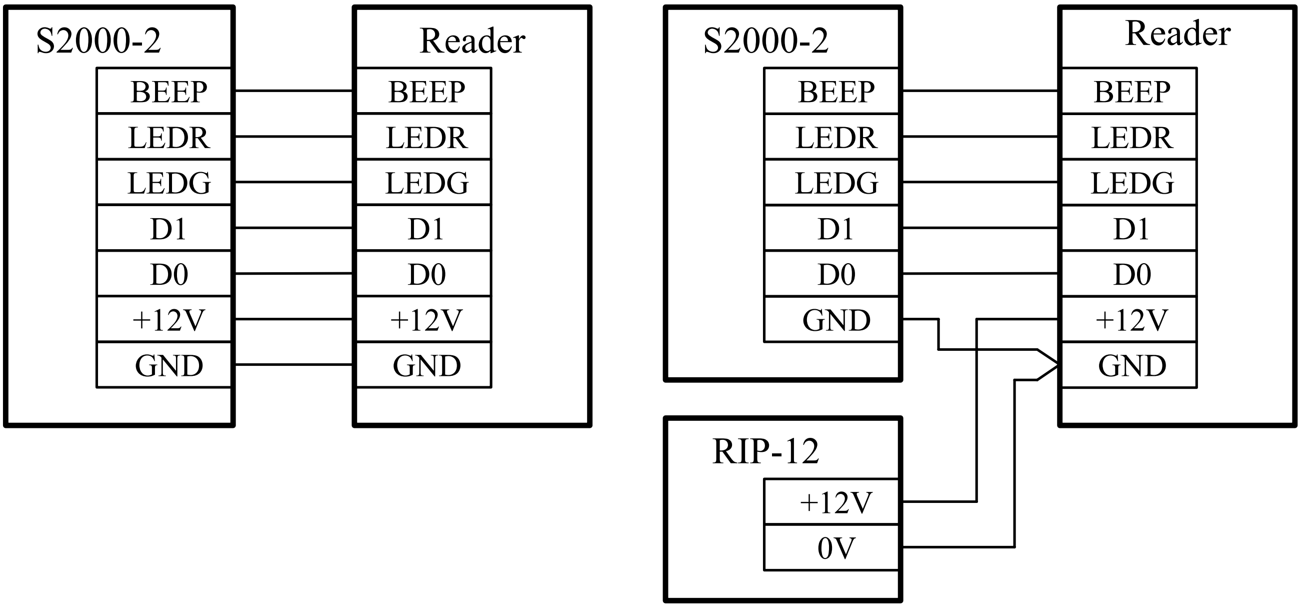
Connecting Readers with Wiegand Output Interface

Variant 1

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

Variant 2

is intended for readers with high current consumptions or far from the controller more than 50m



1) If a reader is equipped with a single LED control circuit this circuit is to be connected to the LEDG terminal of S2000-2, with LEDR terminal being left unconnected

2) If a reader is equipped with no built-in sounder the BEEP terminal of the S2000-2 controller is to be left unconnected

Figure 14. Reader with Wiegand Output Interface Wiring Diagram

Connecting Readers with ABA TRACK II Output Interface

Readers with the ABA TRACK II magnet cards interface are connected similarly to the readers with the Wiegand interface. The DATA output of the reader is connected to the D0 input of the controller and the CLOCK output of the reader is connected to the D1 input of the controller.

Connecting an Arming Request Button

If combined keys designed both for access and arming/disarming are supposed to be presented to a reader the Arming Request button is to brought to the reader circuit as shown in Figure 15.

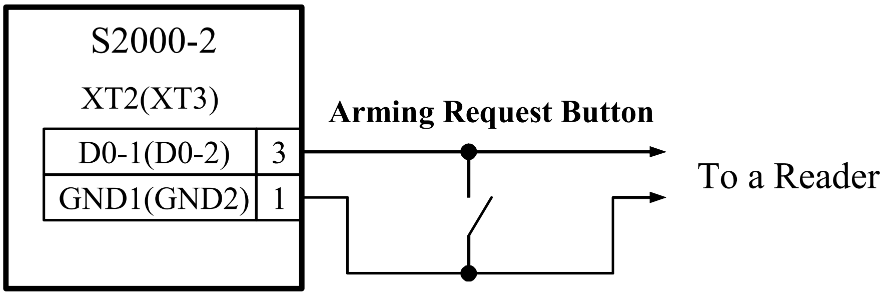


Figure 15. Arming Request Button Wiring Diagram

CONNECTING DOOR OR PASSAGE SENSORS

DOOR1 and DOOR2 terminals of the C2000-2 controller (see Figure 3) are intended to connect door sensors (or door open detectors, or door contacts) as well as various passage sensors or turnstile rotation detectors. These sensors are used for implementing extended S2000-2 functions, such as PASSAGE messages generating and transmitting them to a network controller, monitoring doors for being forced or held open, anti-passback rules checking, time&attendance monitoring, relay activation while door being open/closed and so on.

If none of these functions is required these circuits can be out of use and the relevant terminals are to be left disconnected only if the S2000-2 controller operates in the Two Entrance Doors, One Entrance/Exit Door and Turnstile modes. In the Swing-beam Barrier and Two Sluice Doors modes using DOOR1 and DOOR2 circuits and connecting passage sensors are obligatory.

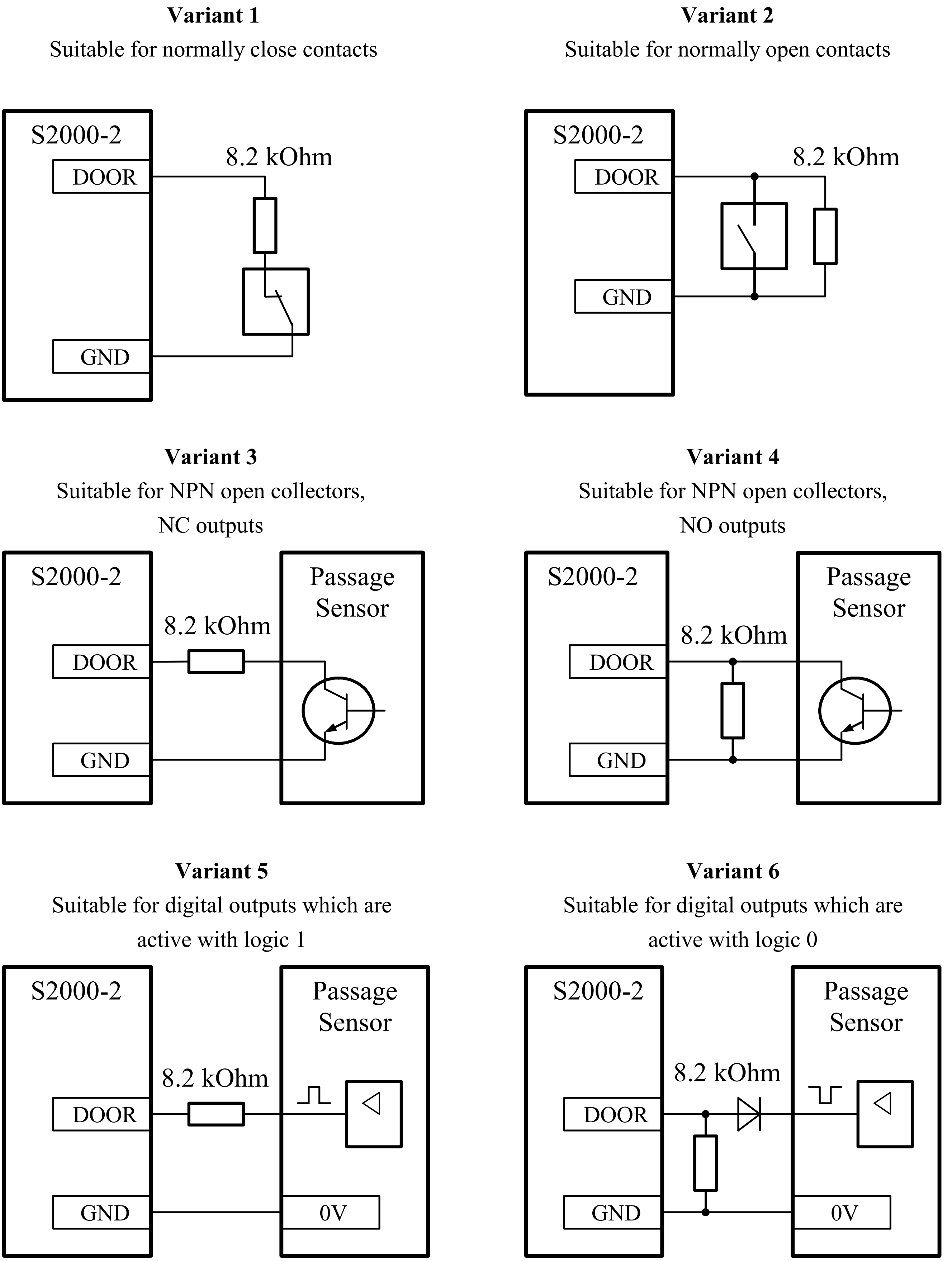
The following detection devices can be brought into the DOOR circuits:

- Magnetic contacts
- Optical passage sensors
- Turnstile rotation sensors
- Optical car passage sensors

These detectors can be equipped with both NC and NO outputs, open collector outputs, as well as digital outputs (active 0 or active 1 with +5V CMOS levels).

Figure 16 shows wiring diagrams for connecting passage sensors (door sensors) to the S2000-2 controller. For all the diagrams it is supposed that in normal conditions (the door is closed, the turnstile is in home position, no car is located near the swing-beam barrier) a 8.2 kOhm terminating resistor is included between the DOOR…and the GND circuits (the voltage on a DOOR… terminal relative to GND is about 2.9V). When a passage sensor has been activated, the terminating resistor circuit is either open (voltage at a DOOR… terminal is about 5.0V) or short circuited (voltage at a DOOR… terminal is about 0V).

A passage sensor must generate a signal of at least 50 ms length, it is necessary for the controller to detect a passing event.



Variant 1

Suitable for normally close contacts

Variant 2

Suitable for normally open contacts

Variant 3

Suitable for NPN open collectors, NC outputs

Variant 4

Suitable for NPN open collectors, NO outputs

Variant 5

Suitable for digital outputs which are active with logic 1

Variant 6

Suitable for digital outputs which are active with logic 0

Figure 16. Wiring Diagrams for Door and Passage Sensors

CONNECTING ALARM LOOPS

In all S2000-2 operation modes except the *Swing-beam Barrier* (see above) LOOP1 and LOOP2 terminals of the S2000-2 controller are used to connect intruder alarm loops (see Alarm Loops Section of this Manual).

Figure 17 shows how to bring detectors with normally closed and normally open contacts into a S2000-2 alarm loop.

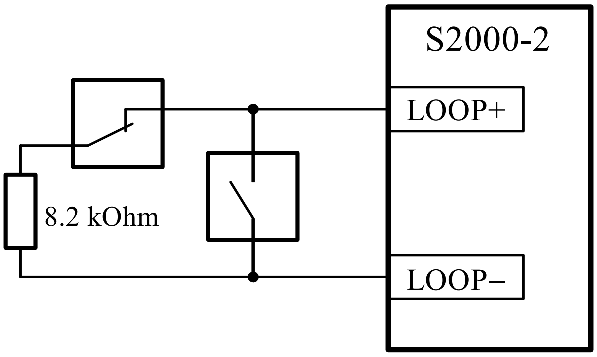


Figure 17. NO and NC Intruder Detectors to the S2000-2 Connection Diagram

Resistance of the loop wires must not exceed 1 kOhm, excluding the terminating resistor.

Leakage resistance between the loop wires or between each wire and ground must not be less than 20 kOhm.

The S2000-2 controller provides arming a loop if the resistance of this loop including terminating resistance 8.2 kOhm ranges from 5 kOhm ± 10% to 11 kOhm ± 10%.

S2000-2 PROGRAMMING

The S2000-2 configuration parameters are to be modified by ***UPROG Configuration Tool software of 4.0.0.821 version or later*** which operates on a PC under the Windows-98 and higher. Programming all the parameters of the controller (including the key serial number length, access templates and possibility to program up to 8192 keys in the S2000-2 rev.01) are provided via the ***UPROG Configuration Tool software of 4.0.0.915 version or later***. The configuration of the S2000-2 is stored in the S2000-2 non-volatile memory.

The controller can be connected to the COM-port of the computer through the following: the PI-GR Interface Converter, the S2000-PI Interface Converter/Extender, the S2000-USB Interface Converter, and the S2000 Console (version 1.20 and higher) or the S2000M Console.

The most up-to-date version of UPROG.EXE can be found on the web site of the Bolid Company at the address www.bolid.com, in DOWNLOAD section.

The S2000-2 controller has eight groups of configuration parameters:

- System configuration parameters
- Parameters of readers
- Parameters of alarm loops
- Parameters of relays
- Parameters of access groups
- Parameters of time schedules
- Parameters of keys
- Parameters of key patterns

SYSTEM CONFIGURATION PARAMETERS

System parameters of the controller's configuration are given in the Table 6.

Table 6 System Configuration Parameters

Parameter	Description	Range	Default value
Network Address	The unique number of S2000-2 within the address space of a network controller	1…127	127
Operation Mode	The fundamental parameter which define the controller operation strategy and its destination	1 (Two Entrance Doors) 2 (One Entrance/Exit Door) 3 (Turnstile) 4 (Swing-beam Barrier) 5 (Two Sluice Doors)	1

Parameter		Description	Range	Default value
Maximum PIN-code Length		Maximal number of the PIN-code digits for readers that have the Wiegand interface and send the PIN-code to the controller as one digit at a time	1…12	6
Key Serial Number Length		Limits the number of significant bits in a serial number to be read while reading the key codes. Required to insure identity of a key code received from readers of different type	16…48 bits (4 12 digits)	48 bits (12 digits)
Sound Alarms	**Access**	Enables the built-in controller sounder signaling for access events, door being forced and held open, loop breaking, and key programming mode entering respectively	On/Off	On
	Door Forced/ Held Open		On/Off	On
	Loop Alarms		On/Off	On
	Programming		On/Off	On

The ***Network Address*** parameter is used for communicating data between the S2000-2 controller and an Orion network controller via RS-485 interface. A unique address must be assigned to the controller while connecting it to the network (the Orion system).

When one of the readers connected to the controller is a keypad with Wiegand output interface which sends to the controller the codes of pressed keys one by one, then a PIN-code is considered to be completely entered when the number of entered symbols has reached the ***Maximum PIN-code Length*** value. To complete entering of a shorter PIN-code the keypad button # (with the hex code 0B) should be pressed after the last symbol.

The codes of the keys 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 key. The **Key Serial Number Length** parameter enables limiting the size of the significant part of the key serial number. This can be suitable for a system where readers with different output interfaces are used to read keys 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 an Orion system, to regard these codes to belong to the two different cards. If however the value of the **Key Serial Number Length** parameter is set to 24 bit (6 hexadecimal digits), while receiving a code of the card from any reader the controller will set the high-order bits (from 25 to 48) of the card code to 0, and the code will be the same regardless of the type of the reader.

Decreasing the **Key Serial Number Length** value (to less than 48 bits) can be used while importing a key database from any other system to an Orion system in the case if the keys were stored with shortened serial numbers. In such the case the **Key Serial Number Length** is to be selected according to the quantity of known digits of the key serial numbers.

If no one of the reviewed tasks is set, it is not advisable to modify the **Key Serial Number** parameter (let it be 48 bit on default).

If this parameter is being modified for the controller which stores some previously entered keys in its memory the UProg Configuration Tool generates a prompt asking the permission to correct existing key codes (set high-order bits to zeros and recount the keys' CRC). This action is irreversible, i.e. if the **Key Serial Number Length** will be increased afterwards the key is to be newly entered into the controller (for example, to be loaded from the previously saved file).

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

READER CONFIGURATION PARAMETERS

Both readers of the controller have similar sets of the configuration parameters given in Table 7.

Table 7. Reader Configuration Parameters

Parameter	Description	Range	Factory Value
Output Interface	The way to transmit the read code of the presented key to the S2000-2	1 Touch Memory 2 Wiegand 3 ABA TRACK II	1 (Touch Memory)
Time to Hold Keys for Arming/Disarming	Time needed the combined key to be held at the reader in order to arm/disarm alarm loops (for Touch Memory output interface readers only)	0…32 s	0 (off)
Access Zone Number	The number of the access zone passing to which is controlled by means of the reader	0…65535 (65535 means an undefined zone)	65535
Two Factor Authentication	The mode of identification when each key involves codes of two different types (for combined readers only)	On/Off	Off
Passage Sensor	A sensor detecting door opening, passing or car presence, is connected and used for an access strategy	On/Off	Off

Parameter		Description	Range	Factory Value
Forced Open Monitoring[1]		Activates monitoring the time of the door being open	On/Off	Off
Held Open Monitoring[1]		Activates monitoring for the time the door is open for	On/Off	Off
Held Open Timeout[1]		The time needed to expire for the door which has just been opened is considered as held open	1…255 s	20 s
Lock Access If Any Loop Is Armed	**LP 1**	Specifies alarm loops of the controller that will lock access when any of them are armed (locking based on OR rule)	On/Off	Off
	LP 2			Off
Lock Access If All Loops Are Armed	**LP 1**	Specifies alarm loops of the controller that lock access when all of them are armed (locking based on AND rule)	On/Off	Off
	LP 2			Off
LED Control Polarity		Provides selecting the active logic level to turn the LED of the reader on	Forward (1 active) Reverse (0 active)	Forward (1 active)
LED Quiescent Mode		Defines the way the LED lights in quiescent mode	1 — off 2 — red if any of the specified below loops is armed, otherwise the LED is off 3 — red if all the specified below alarm loops are armed, otherwise the LED is off 4 — red	2
Indicate Armed Loops	**LP 1**	Specifies alarm loops which being armed causes the LED to be lit (for 2nd and 3rd LED Quiescent Mode – see above)	On/Off	On
	LP 2			On
Indicate Loop Alarms	**LP 1**	Specifies alarm loops of the controller which breaking causes the LED indication	On/Off	On
	LP 2			On
Sounder Control Polarity		Provides selecting the active logic level to turn the sounder of the reader on	Forward (1 active) Reverse (0 active)	Forward (1 active)
Sound Alarms	**Access**	Enables the reader sounder signaling for access events, door being forced and held open, loop breaking, and key programming mode entering respectively	On/Off	On
	Door Forced/ Held Open		On/Off	On
	Loop Alarms		On/Off	On
	Programming		On/Off	On

[1] *The parameter is valid only if the Passage Sensor parameter is set*

Output Interface parameter (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 controller.

If a reader with the Touch Memory interface is in use then the **Time to Hold Keys for Arming/Disarming** parameter makes it possible to arm/disarm alarm loops by means of the combined key (both to access and to arm/disarm) without preliminary switching the controller to the Ready to Arm/Disarm mode. In order to arm/disarm loops the key has to be held near the reader for more than the specified period of time. In order to gain access, the combined key has to be presented to the reader for a shorter time interval (actually the relay will be actuated with a short delay — while taking off the key). By default the value of the **Time to Hold Keys for Arming/Disarming** parameter is equal to zero, and this way of loop arming/disarming is disabled, and an access, while a combined key is presented, is granted instantaneously (after presenting, not after taking off the key).

Access zone number is an arbitrary 16-bit number that identifies a zone, access to which is controlled by the programmed reader (that is *the zone* access to which is implementing by means of presenting a key to *this reader*). To give access zone numbers for each reader is required for the controller to operate as a part of an access control system. These numbers are included in all the messages due to passages, access denying and granting which are generated by the controller. Taking into account access zone numbers provides implementation of:

- Global Anti-passback rule checking
- Time&Attendance monitoring
- Detection of personnel location.

For these features to operate properly it is required to set the same **Access Zone Number** for all the readers of the access control system which are installed at the entrance of an access zone and control the entry to this zone**.**

Maximal allowed number of an access zone (65535) indicates that the zone is undefined. The Global Anti-passback rule will not be check and the Time&Attendance will not be monitored for such a 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 without anti-passback rule and time&attendance monitoring. This makes it possible to unload the RS-485 interface which in turns increases interface capacity and decreases message delivery time).

Setting the **Two Factor Authentication** parameter means that to identify one user (one key) will require not one but two identification codes (see Two Factor Authentication Section). If this parameter is set for at least one reader of the S2000-2, the available number of keys to be stored in the controller memory will be twice lower (down to 2048 for a S2000-2 or down to 4096 for a S2000-2 rev.01).

The **Passage Sensor** parameter being set indicates that a device sensing a passage through the access point is in use. In this case:

- For Two Entrance Doors, One Entrance/Exit Door and Turnstile modes, after granting the access the controller is waiting for a passage to be detected (the door to be open, the turnstile to be rotated and so on) for the Relay Activation Time, but at least for 10 seconds. Before sensing the passage or this time having been expired the controller ignores all attempts to present identifiers to the reader again
- When the sensor has just actuated the PASSAGE message is generated by the controller
- Monitoring the door for held or force open has been available (see the description of the **Forced Open Monitoring** and **Held Open Monitoring** parameters)
- The relay which controls the lock can be switched off lock before the **Relay Control Time** having been expired (see the description of the **Switch Off After Door Being Opened** and **Switch Off After Door Being Closed** parameters)

If the **Passage Sensor** parameter is unset, the mentioned above functions are unavailable, passing is not expected and in the Two Entrance Doors, One Entrance/Exit Door and Turnstile modes the system indicates the fact of access granting by means of the reader LED, which is switched on for the Relay Activation Time**,** but at least for 2 seconds.

If the **Forced Open Monitoring** parameter is set, door opening preceded by no access granting will cause the DOOR FORCED alarm message to be generated and the light and sound alarms to be activated.

If the **Held Open Monitoring** parameter is set, door being opened for more than **Held Open Timeout** will cause the DOOR LEFT OPEN alarm message to be generated and the light and sound alarms to be activated.

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

It is advisable to set this parameter to

- ➢ *Forward* (1 active) for IButton readers and for most readers with Wiegand interface,
- ➢ *Backward* (0 active) for most readers with Touch Memory interface (except iButton readers)

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

It is advisable to set this parameter to

- ➢ *Forward* (1 active) for most readers with Wiegand interface,
- ➢ *Backward* (0 active) for most readers with Touch Memory interface

The **Sound Alarms** switches enable reader sounder turning on for each category of the alarms available (see Light and Sound Alarms Section of this Manual)

If readers with different interface types (Touch Memory, Wiegand-26, Wiegand-44, etc.), designed for operating with identifiers of the same type are connected to the S2000-2 controllers of the Orion system, the code of an identifier presented to one reader unit may not coincide with the code of the same identifier presented to another reader.

For instance, the code of a Proximity card presented to a reader with the Wiegand-26 interface can differ from the code of the same card presented to a reader with the Wiegand-44 or the Touch Memory interfaces.

Similarly, a PIN code, entered to a reader with the Wiegand-6 or Wiegand-8 interfaces (each entered number is sent to the controller apart from another), will differ from the same code entered to a reader with the Wiegand-26 or Touch Memory interface (all the PIN code numbers are sent to the controller as a whole).

So when designing and operating an access control system it is necessary to follow the recommendations given below:

If possible, use readers with the same format of output data.

If possible, use compatible formats for readers with different interfaces. For example, the 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.

If the reader formats are incompatible, a **Key Serial Number Length** should be limited by a value that is the length of the shortest serial number to be generated by readers of the system. As a rule, it is the readers with the Wiegand-26 interface that generate the shortest serial numbers (24 bit).

If key codes are entered remotely by means of a reader, connected to another controller, data format of this reader has to be compatible with data format of readers connected to the programmed controller.

PIN-codes entered from readers with the Wiegand-6 or Wiegand-8 interface (each entered number is sent to the controller apart from another) are of the same format as if they were entered from computer keyboard (by means of the UProg or the Database Administrator of the ARM Orion Workstation). Thus, when programming the S2000-2 controller with such readers being connected to, it is possible to use PC keyboard (the UProg software) to enter PIN codes. As for the PIN code readers with other format of output data, while programming keys, a code should be entered solely from the reader keyboard.

ALARM LOOP CONFIGURATION PARAMETERS

Each of the two controller's loops has the same configuration parameter, **Arming Delay**. In all the controller operation modes, except for the Swing-beam Barrier mode, this parameter defines the delay time for starting alarm loop condition monitoring after the Loop Arming command has been received. In Swing-beam Barrier operation mode loops 1 and 2 can not be used for security aims since they are used in access control strategy (sensors detecting a car presence are connected to them), so for this operation mode the value of this parameter is ignored.

The arming delay is set in seconds within 0 — 255s range. Default value (the factory setting) is 0 for both loops.

RELAY CONFIGURATION PARAMETERS

Configuration parameters for each of the two controller's relays are given in Table 8.

Table 8. Relay Configuration Parameters

Parameter	Description	Range	Default Value
Executive Program	Defines a way the relay is controlled if access is granted	3 - Switch On for a Time 4 – Switch Off for a Time	3
Relay Activation Time	Maximal time of transmitting the relay control signal (program) if access is granted	0.125…8192s (0.125s… …2h 16min 32s)	5 s
Switch Off After Door Being Opened	Causes the selected relay executive program to be interrupted when the door is being opened (when the passage has been detected) before the Relay Activation Time has been expired	On/Off	On
Switch Off After Door Being Closed	Causes the selected relay executive program to be interrupted when the door has just been closed after user passing	On/Off	Off

The **Executive Program** parameter defines the way to control a relay automatically while granting access. The executive program 3 (Switch On for a Time) is used to control normally open electromechanical locks and strikes, turnstiles, swing-beam barrier openers, gates drives and so on. Initially the relay contacts are opened (the relay is switched off). When the access has been granted the relay contacts are closed (the relay is switched on) for a given time. The executive program 4 (Switch Off for a Time) is used to control normally closed electromagnetic locks. Initially the relay contacts are closed (the relay is switched on) and when the access has been granted the relay contacts ear opened (the relay is switched off) for a specified time (see below).

The maximum time of the relay activation while granting access is given by the **Relay Activation Time** parameter. The maximum relay activation time can reach 2h 16min 31.875s, the incremental step being 0.125s.

For all the controller operation modes a standard time period is provided for passing after access is granted. If no passage is detected within this time (the door sensor in the door control circuit was not activated) the access will be regarded as not used and the identification procedure has to be repeated. If the Relay Activation Time has not expired to the moment of expiration the passage time, the passage time is prolonged up to the moment when the relay returns to its initial condition. So the maximum time the system waits for a passage can be prolonged if the Relay Activation Time exceeds the standard passage time (of cause if the locking unit being in use supports applying such a long opening signal).

If the **Switch Off After Door Being Opened** attribute is set for the relay and access is granted, the relay will return to its initial condition immediately after the door has been opened (the passage sensor has actuated) before elapsing the Relay Activation Time.

If the **Switch Off After Door Being Closed** attribute is set for the relay and access is granted, the relay will return to its initial condition after the door is open and then has been closed again (the passage sensor has been restored) before elapsing the Relay Activation Time.

If none of these attributes is set, the relay will always be switched on (off) strictly for the Relay Activation Time (except for the Swing-beam Barrier operation mode — see Swing-beam Barrier Mode Section of this Manual).

ACCESS GROUP PARAMETERS

The significant part of access rules for each access key are specified by means of assigning this key to a relevant access group number. Access rights and limitations defined for the access group are extended to all the keys assigned to this group. Up to 32 different access groups can be described for the S2000-2 controller. The parameters of an access group are listed in Table 9.

The **Access** attribute is set for an access group if the keys assigned with it are supposed to be used for access.

The **Time Schedule** for access represents a number of time schedule defining intervals of time when access can be granted for these keys. If this parameter is equal to 0, access is granted at any time. Parameters of all other available 16 time schedules are programmable (see Time Schedules Section of this Manual).

The **Antipassback Mode** and **Zonal Anti-passback Rule** define the controller's reaction on the anti-passback rule violation (see Anti-passback Rules Section of this Manual).

The Timed Anti-passback rule uses an additional **Anti-passback Lockout Period** parameter. During this time period since key owner passing to an access zone the S2000-2 controller is operating as for Hard Anti-passback rule and after expiration of the time the S2000-2 controller is operating as for Soft Anti-passback rule.

Table 9. Access Group Parameters

Parameter	Function Description	Value Range
Access	Defines that keys assigned with the access group configured are designed to gain access	On/Off
Time Schedule (Access)	The number of a time schedule specifying the time zones when the access is permitted for the owners of keys included in the access group programmed	0…16
Anti-passback Mode	Defines the controller access policy in case of anti-passback rule violation	None (not checked) Hard Timed Soft
Anti-passback Lockout Period	The period of time in HH:MM format used for the Timed Anti-passback mode. Before this time expiration since user passage to a zone is monitored in accordance with Hard Anti-passback rules while after expiration of this time in accordance with Soft Anti-passback rules	0
Zonal Anti-passback Rule	Specify to check anti-passback rules taking into account passages between different zones of a system (provides implementing of full entry/exit control)	On/Off

Parameter	Function Description	Value Range
Entry Mode	Defines the rules to access the zone with the specified number (zone controlled by the first reader of the S2000-2) for owners of the keys of the programmed access group	Locked Simple Confirmation Only Two-person Rule Three-person Rule
Exit Mode	Defines the rules to access the zone with the specified number (zone controlled by the second reader of the S2000-2) for owners of the keys of the programmed access group	Locked Simple Confirmation Only Two-person Rule Three-person Rule
First Access Group to Confirm Entry	The number of an access group assigned with the key which must be presented after the presenting the key of programmed access group in order to confirm access rights if the Entry Mode is set to Two-person Rule	0…32
Second Access Group to Confirm Entry	The number of an access group assigned with the key which must be presented after the presenting of two relevant keys (see above) in order to confirm access rights if the Entry Mode is set to Three-person Rule	0…32
First Access Group to Confirm Exit	The number of an access group assigned with the key which must be presented after the presenting the key of programmed access group in order to confirm access rights if the Exit Mode is set to Two-person Rule	0…32
Second Access Group to Confirm Exit	The number of an access group assigned with the key which must be presented after the presenting of two relevant keys (see above) in order to confirm access rights if the Exit Mode is set to Three-person Rule	0…32
Arm/Disarm	Defines that keys assigned with the access group configured are designed to arm and disarm the alarm loops of the S2000-2 controller	On/Off
Time Schedule (Arming/Disarming)	The number of a time schedule specifying the time zones when the arming/disarming is permitted for the owners of keys included in the access group programmed	0…16
Arm Loop 1	Setting of these switches on permits arming of the specified alarm loops of the S2000-2 for all the keys included to the access group	On/Off
Arm Loop 2		On/Off
Disarm Loop 1	Setting of these switches on permits disarming of the specified alarm loops of the S2000-2 for all the keys included to the access group	On/Off
Disarm Loop 2		On/Off

Entry Mode (Exit Mode) parameter defines conditions necessary for access to the zone controlled by the first reader (the second reader) to be granted.

For the *Simple* entry (exit) mode it is sufficient to present only one user access key.

If the *Confirmation Only* entry (exit) mode is selected for the all keys included in the access group such the keys are used only to confirm access rights for keys of another access groups and cannot be used to gain access by itself.

If the *Two-person* or *Three-person Rule* passage mode (see Passage Modes and Two or More Person Rule Access Control Section of this Manual) is selected for an access group, then to gain access owners of the keys of this access group must present their keys followed by presenting one more key (two keys) assigned with the other access group (groups). The numbers of these groups are specified by values of **First Access Group to Confirm Entry (Exit)** and **Second Access Group to Confirm Entry (Exit)** parameters. If for example the Two-person Rule is selected as entry mode the controller after successful identification of the key of programmed access group will be waiting for presenting a key assigned with the access group specified by **First Access Group to Confirm Entry**. If otherwise the Three-person Rule is selected, the controller first verifies the access rights of the key of the programmed access group, then verifies that the next presented key has the group number specified by **First Access Group to Confirm Entry**, and finally requires the presenting of a third key included in **Second Access Group to Confirm Entry**. The exit modes are implemented similarly.

If the **Arming/Disarming** parameter is set the keys contained in this access group can be used to arm and disarm alarm loops of the S2000-2 controller. The **Arm Loop 1**, **Arm Loop 2**, **Disarm Loop 1**, **Disarm Loop 2** parameters defines specific actions which are permitted for owners of keys included in the access group.

The **Time Schedule** for arming/disarming represents a number of time schedule defining intervals of time when arming/disarming alarm loops is permitted for the keys. If this parameter is equal to 0, arming/disarming is enabled at any time. Parameters of all other available 16 time schedules are programmable (see Time Schedules Section of this Manual).

If the both attributes **Access** and **Arming/Disarming** are set on for the keys included in the access group these keys are called *combined* (that is, multifunctional). The combined keys can be used for:

- Access and loop arming/disarming (if the keys are assigned with the *User* type)
- Unlocking/restoring Controlled Access mode and loop arming/disarming (if the keys are assigned with the *Unlocking* type)
- Locking/restoring Controlled Access mode and loop arming/disarming (if the keys are assigned with the *Locking* type)

In order to control the loop arming/disarming by a combined key the controller has to be preliminary switched to Ready to Arm/Disarm mode or the key has to be held near the reader within the specified time (see Alarm Loops Section of this Manual).

ACCESS KEY CONFIGURATION PARAMETERS

Up to 4096 key descriptors (8192 for the S2000-2 rev.01) can be stored in the controller database. The keys can be Dallas iButtons, Proximity cards, PIN-codes and so on. Each key is described by a set of parameters which is shown in Table 10.

Table 10. Key Configuration Parameters

Parameter Name	Function Description	Range
Key Type	Defines functions of the key	User Master Unlocking Locking
Key Is Locked	This attribute provides temporary blocking the key	On/Off
Without Additional Code	No additional code is necessary to identify the key while the Two Factor Authentication mode is set for a reader which the key is presented to (see Two Factor Authentication Section of this Manual)	On/Off
Access Group	A number of an access group which defines common access rights and limitations which are applied to this key and are common for all keys assigned to this access group	0…32
Validity Limitation	Defines key activity limitations depending on date	On/Off
Validity Period	Defines the period of dates when the key is active	01.01.2000 … … 31.12.2255

The **Key Type** parameter defines the destination of the key.

User keys are intended to access or to arm/disarm loops.

Master keys are intended to switch the controller into the programming mode for hardware programming (adding) new keys. All keys programmed by hardware with the help of a Master key will be of User type.

Unlocking key is intended to open access (to implement free pass mode) and restore the Controlled Access mode (see Access Modes Section) and also to arm/disarm alarm loops.

A *Locking* key is intended to lock access and restore the Controlled Access mode (see Access Modes Section) and can be also used to arm/disarm loops.

The **Key is locked** switch setting prohibits operation for a key of any type. It is used to lock a key temporary (e.g. if the key is lost) with possibility of its subsequent recovery.

The **Without Additional Code** parameter is intended to simplify identification of several keys if the Two Factor Authentication mode is used for other keys (see Two Factor Authentication Section of this Manual). If the Two Factor Authentication mode is not used (neither at entry, nor at exit) this key parameter is ignored.

The **Access Group** (the number of the access group) defines the access rights and restrictions for the *User* key, as well as its rights to arm/disarm loops (see Access Rights Section of this Manual). The *Master* key access group is inherited by all the keys programmed by hardware (see Key Programming Section of this Manual).

If the **Validity Limitation** parameter is set, the date of the key validity starting and validity expiration are set by the **Validity Period** parameter. Otherwise the key never expires. The validity limitation is used for all the key types.

ACCESS KEY PATTERN CONFIGURATION PARAMETERS

In order to gain access for key owners that are not stored in controllers' memory it can be possible to program up to 5 different key patterns which are used for key identification. Each key pattern is described by a set of parameters shown in Table 11.

Table 11. Key Pattern Configuration Parameters

Parameter Name	Function Description	Range
Pattern Is Locked	This attribute provides disabling the key pattern	On/Off
Key Pattern Type	Destination of all the keys fitting the key pattern	User
Base Code	A base code the specified digits of which must be equal to relevant digits of all codes of the keys fitting the key pattern (see below)	
Code Mask	A set of code positions in digital sequence of a presented key, digits in these positions must be identical with the relevant digits of the base pattern code (see above)	
Access Group	A number of an access group which defines common access rights and limitations which are applied to this key and are common for all keys assigned to this access group	0…32
Validity Limitation	Defines key activity limitations depending on date	On/Off
Validity Period	Defines the period of dates when the key is active	01.01.2000 … … 31.12.2255

The **Pattern is locked** switch setting on disables a key pattern. By default this parameter is switched on for all five key patterns disabling the possibility to gain user access based on access key patterns.

The **Pattern Type** parameter describes what operation the key met the pattern requirements is destined to. All keys fitting to any pattern can only have the *User* type and cannot be *Unlocking*, *Locking*, or *Master*.

The **Base Code** parameter represents a base key code which will be covered by the **Code Mask** while identifying keys based on the pattern. Digits of the base code which positions match with the 'opened' mask positions must be equal to relevant digits of all the keys fitting the pattern. The base code is not stored in the controller memory on the contrary to codes of individual keys. The base code can be typed manually or read by presenting to a reader a key fitting the pattern.

The **Code Mask** parameter specifies digits of the base code which are significant while presented keys being identified (that is ‘opened’ digits which values must be equal both for the base and the presented key) and are mindless and ignored by the controller (that is can differ for different keys). ‘Opening’ and ‘closing’ of digits are implemented by double click of the mouse left button on the relevant digits of the pattern base code in the Pattern Base Code field, on the Key Pattern tab of the UProg Configuration Tool for the S2000-2 controller. ‘Opened’ digits in base code are showed by black while ‘closed’ digits which will be ignored are shown by light gray color.

The **Access Group** (the number of the access group) defines the access rights and limitations for the *User* key, as well as its rights to arm/disarm loops (see Access Rights Section of this Manual). The *Master* key access group is inherited by all the keys programmed by hardware (see Key Programming Section of this Manual).

If the **Validity Limitation** parameter is used, the dates between which the key pattern is valid have to be set by the **Validity Period** parameter. Otherwise the key pattern never expires.

KEY PROGRAMMING

If the S2000-2 controller operates as a part of a PC-based Orion system, codes of iButtons, Proximity-cards and other identifiers are saved to the S2000-2 database (into the controller non-volatile memory) with the help of the *Orion Database Administrator* utility *of the Orion Workstation* software.

If the S2000-2 controller operates as a part of an Orion system based on the S2000/S2000M control console or the S2000-2 operates standalone, access keys are programmed by means of UProg Configuration Tool software (**uprog.exe**) installed on a personal computer (PC). This software facilitates adding and deleting keys, setting and modifying key attributes, saving the list of programmed keys to a file, loading a key list from a file to the controller memory, etc.

Moreover, the keys can be programmed by hardware without PC, with the help of one or more Master keys. Any identifier can be used as a Master key if the Master key type is set for it. Presenting Master key turns on the key programming mode. New keys presented to one of the controller readers in this mode are enrolled to the controller memory with User type, inherit access group of the Master key and have unlimited validity.

Also a single Master key with access group #0 can be programmed by hardware only, without PC. To do this remove the cover of the controller enclosure and then press the tamper switch for three times. First pressing has to be prolonged (longer than 1.5s), the second one has to be short (less then 0.5s), and the last one has to be prolonged again. Pauses between pressings should not exceed 0.5s. The sounders of the controller and the first reader will play special '*Master Programming*' melody, the READY indicator and the LED of the first reader will start double flashing synchronously, the LED of the reader double flashing with red and green color alternately. If the first reader is busy (the last access procedure has not yet been finished), the Master key programming mode indication will be activated on the second reader. After that the key to be programmed has to be presented to those reader which indicates Master programming mode, within 30s after the mode being switched to. Sounders of the controller and the reader will play ending of the 'Master Programming' melody and the READY indicator and reader LED will start to light continuously.

WARNING! **Programming the Master key with a tamper switch deletes all the previously programmed keys that are stored in the controller memory** (while Master keys programming by means of the uprog.exe software has no effect on previously programmed keys).

Master keys of other (non-zero) access groups have to be preliminary programmed using the uprog.exe software.

To enter the hardware key programming mode for User key programming, it is necessary to present a Master key to one of the controller readers. Three pairs of short sound signals will be generated by the sounders of the reader and the controller, and the LED of this reader will flash alternately with red and green colors. In this mode the presented identifiers are saved to the controller memory and assigned with access group number of the Master key. If a new key code is successfully stored in the

S2000-2 database, or the access group descriptor of an existing key is modified, the sounder will sound two short signals, and the LED of the reader will be switched on for 2s (green color). Single short sound and 1s long lighting of the green LED mean that the key belonging to the access group of the Master key has already been saved in the S2000-2 memory. Long sound and triple blinking of the red reader LED mean that key code saving was failed (the memory is full).

If 2 Factor Authentication is used by the reader, after receiving the main key code the controller will ask to present an additional code, the reader LED starting flashing green 5 times per second. Afterwards a key (key code) presented to the reader within next 30s will be saved as the additional code for the key that was presented before.

To exit key programming mode it is necessary to present the same Master key which was used to activate the programming mode. Besides, the keys programming mode will be finished automatically if no key is presented at the reader within 30s. The controller and reader sounders will generate three short sounds and one long sound (the 'Programming is finished' melody), and the READY indicator and the reader LED will start to light continuously.

If the keys of different access groups are to be added, programming keys of the second access group (presenting a next Master key to a reader) must be started only after exiting keys with the first access group programming mode. Otherwise the second Master key presented to a reader will be reprogrammed as a User key of the first access group.

The hardware key programming (without the UProg Configuration Tool) has restricted by the following:

- It is impossible to program Unlocking, Locking, or Master keys with a non-zero access group
- Validity of the programmed key can not be restricted
- Using 2 Factor Authentication, it is impossible to program a simplified key without an additional code

If keys are programmed with the help of the UProg Configuration Tool software all limitations mentioned above are not exist. Moreover, any key can be deleted or temporary locked. The possibility to accompany key descriptors with text comments (owners names, for example) and save this information in the PC files (text comments are not saved in the controller memory) considerably simplifies key handling process.

In order to arm/disarm loops by means of a Proximity card or iButton, the card or the iButton must be registered in the controller memory, included in the access group with the *User* attribute and specifying the alarm loops which are allowed to be armed/disarmed by means of this access group key presenting (see Access Group Parameters Section below).

PROGRAMMING THE CONTROLLER DEPENDING ON ITS OPERATION MODE

Two Entrance Doors Mode Programming

In order to program the S2000-2 controller for operating in Two Entrance Doors mode by means of UProg Configuration Tool:

1. Select the 'Two Entrance Doors' value in Operation Mode field on the Device tab.
2. If door sensors are in use set the relevant Passage Sensor flags on, else unset them.
3. If any mechanical or electrical buttons, as well as any other equipment, are used to open the lock without participation of the controller, the Forced Open Monitoring and Held Open Monitoring parameters are to be unset in order to avoid false alarms.
4. If electric strikes are in use as locking units, set for each relay (the Outputs tab)

   - 'Switch On for a Time' in Executive Program field
   - 1 ÷ 5s in the Relay Activation Time field (the time sufficient for the strike to be actuated)
   - 'Switch off after door being opened' flag (for the strike to be cocked properly upon quick passing)

   Please note that Free Pass Access mode can not be implemented for an access point if the electric strike is used as a locking unit.

   If magnet locks are in use as locking units, set for each relay (the Outputs tab)

   - 'Switch Off for a Time' in Executive Program field
   - 5 ÷ 20s in the Relay Activation Time field (maximum passage time)
   - 'Switch off after door being opened' or 'Switch off after door being closed' flag (for the lock to be secured just after a passage detection)
5. For all access groups (the Access Groups tab) Anti-passback Mode field must be set to 'None'.
6. Entry Mode parameters on the Access Groups tab in the UProg is interpreted by the controller as the mode for passing in forward direction via the first door, Exit Mode being interpreted as the mode for passing in forward direction via the second door.
7. Programming time zones on the Time Zones tab in UProg, select Entry and Exit interval activity considering an entry interval to be the interval to gain access in forward direction via the first door and an Exit interval to be the interval to gain access in forward direction via the second door.

Other configuration parameters are adjusted depending on specific user needs and desires.

One Entrance/Exit Door Mode Programming

In order to program the S2000-2 controller for operating in One Entrance/Exit Door mode by means of UProg Configuration Tool:

1. Select the ‘One Entrance/Exit Door’ value in Operation Mode field on the Device tab.
2. If a door sensor is in use set the first Passage Sensor flag on, else unset it.
3. If an electric strike is in use as the locking unit, set for the first relay (the Outputs tab)

   – ‘Switch On for a Time’ in Executive Program field
   – 1 ÷ 5s in the Relay Activation Time field (the time sufficient for the strike to be actuated)
   – ‘Switch off after door being opened’ flag (for the strike to be cocked properly upon quick passing)

   Please note that Free Pass Access mode can not be implemented for an access point if the electric strike is used as a locking unit.

   If a magnet lock is in use as the locking unit, set for the first relay (the Outputs tab)

   – ‘Switch Off for a Time’ in Executive Program field
   – 5 ÷ 20s in the Relay Activation Time field (maximum passage time)
   – ‘Switch off after door being opened’ or ‘Switch off after door being closed’ flag (for the lock to be secured just after a passage detection)
4. If Global Anti-passback or Time&Attendance features are to be implemented within a security system (the S2000-2 operates as a part of networked system) pay attention the access zone numbers for both readers to be given correctly.

Other configuration parameters are adjusted depending on specific user needs and desires.

Turnstile Mode Programming

In order to program the S2000-2 controller for operating in Turnstile mode by means of UProg Configuration Tool:

1. Select the ‘Turnstile’ value in Operation Mode field on the Device tab.
2. If passage sensors (a turnstile rotation detector) are in use set the relevant Passage Sensor flags on, else unset its.
3. Set the Forced Open Monitoring and Held Open Monitoring parameters on.
4. Select the Outputs tab and set the Executive Program to ‘Switch On for a Time’ value for both the controller relays

5. Set the Relay Activation Time parameter to a 0.25 ÷ 1s value (which is sufficient to unblock the turnstile when one person is passing)
6. If Global Anti-passback or Time&Attendance features are to be implemented within a security system (the S2000-2 operates as a part of networked system) pay attention the access zone numbers for both readers to be given correctly.

Other configuration parameters are adjusted depending on specific user needs and desires.

Swing-Beam Barrier Mode Programming

In order to program the S2000-2 controller for operating in Swing-beam Barrier mode by means of UProg Configuration Tool:

1. Select the 'Swing-beam Barrier' value in Operation Mode field on the Device tab.
2. The Passage Sensor flags are always active (set on) for this operation mode.
3. Unset the Forced Open Monitoring and Held Open Monitoring parameters.
4. Select the Outputs tab and set the Executive Program to 'Switch On for a Time' value for both the controller relays
5. Set the Relay Activation Time parameter value for the Relay 1 as 5 ÷ 20s (which is sufficient to lift the swing-beam). If the swing-beam barrier is controlled by the single relay or if the standard passage time value (30s) must be increased then set the Relay Activation Time parameter for the Relay 1 to a value more than 30s.
6. Set the Relay Activation Time parameter value for the Relay 2 as 5 ÷ 20s (which is sufficient to lift the swing-beam).

Other configuration parameters are adjusted depending on specific user needs and desires.

Two Sluice Doors Mode Programming

In order to program the S2000-2 controller for operating in Two Sluice Doors mode by means of UProg Configuration Tool:

1. Select the 'Two Sluice Mode' value in Operation Mode field on the Device tab.
2. If Global Anti-passback or Time&Attendance features are to be implemented within a security system (the S2000-2 operates as a part of networked system) pay attention the access zone numbers for both readers to be given correctly.
3. The Passage Sensor flags are always active (set on) for this operation mode.
4. If electric strikes are in use as the locking units, set at the Outputs tab

   - 'Switch On for a Time' in Executive Program field for both the relays

- 1 ÷ 5s in the Relay Activation Time fields (the time sufficient for the strike to be actuated)
- ‘Switch off after door being opened’ flag (for the strike to be cocked properly upon quick passing)

Please note that Free Pass Access mode can not be implemented for an access point if the electric strike is used as a locking unit.

If magnet locks are in use as the locking units, set at the Outputs tab

- ‘Switch Off for a Time’ in Executive Program field for both the relays
- 5 ÷ 20s in the Relay Activation Time fields (maximum passage time)
- ‘Switch off after door being opened’ or ‘Switch off after door being closed’ flag (for the lock to be secured just after a passage detection)

Other configuration parameters are adjusted depending on specific user needs and desires.

MAINTENANCE

TECHNICAL INSPECTIONS

To make sure your S2000-2 controller keeps proper operability it must be inspected by a competent specialist at least on receipt and annually. The inspection algorithm shall include:

- Visual checking S2000-2 for contaminations and mechanical damage
- Verifying S2000-2 for secure mounting and wire connection conditions
- Inspection of S2000-2 operability in accordance with the techniques shown below

The S2000-2 controller must be tested under the following ambient conditions:

- Temperature 25° ± 10°C
- Relative humidity 45 ÷ 80 %
- Atmospheric pressure 630 ÷ 800 mm Hg

WARNING! Disconnect the S2000-2 controller power supply before wiring and unwiring the device while testing

NOTE: Technical readiness period of the S2000-2 does not exceed 5s

The wiring diagram for the controller operability inspection is shown in Figure 18**.**

S2000-2 Operability Inspection

Inspect the controller operability by doing the following:

1. Remove the controller cover and power the controller on.
2. Ensure the controller makes a sound
3. Measure the consumed current value; it must not exceed 120mA.
4. Ensure the network controller displays the event of controller being found.

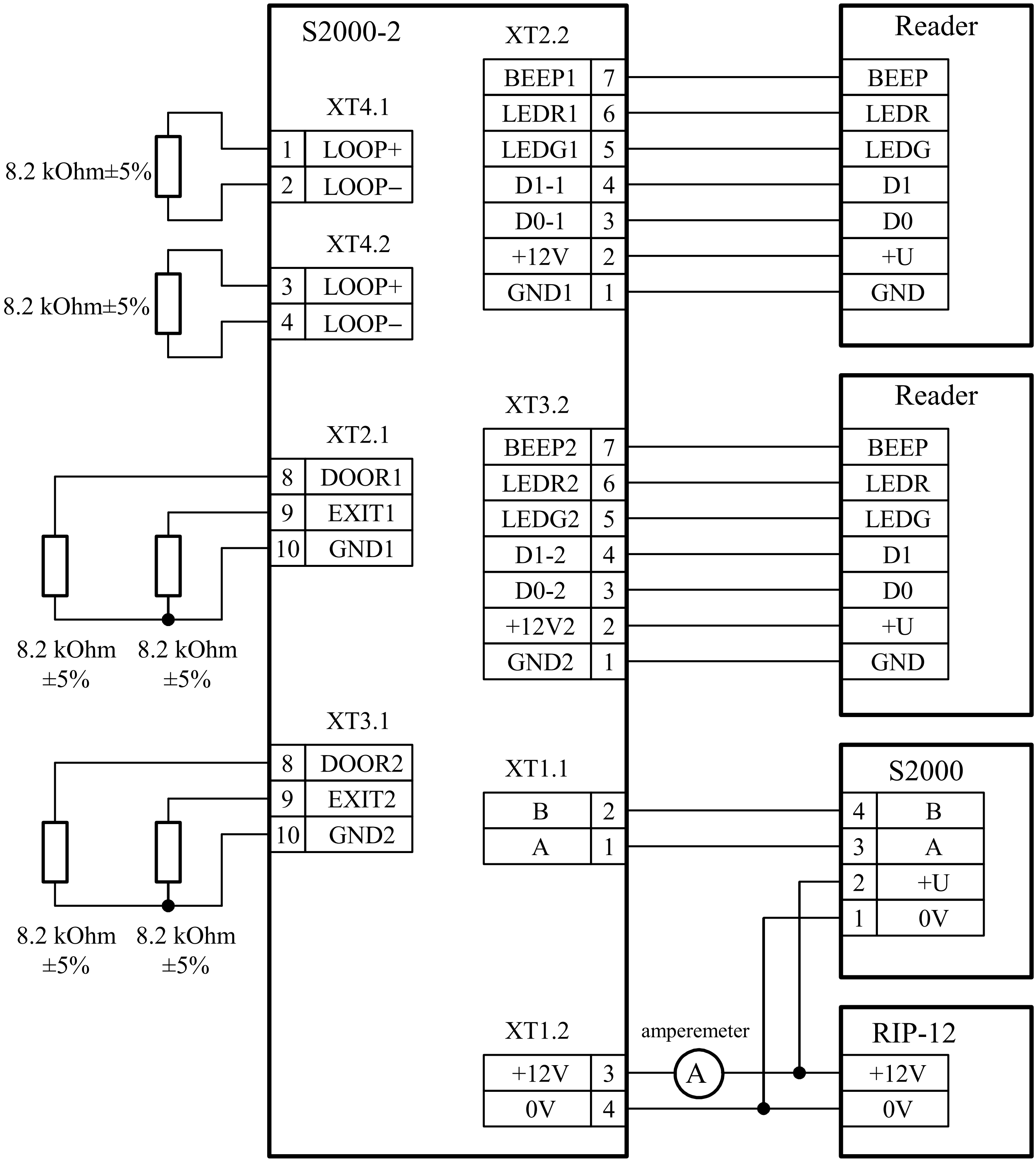


Figure 18. Wiring the S2000-2 Controller for Operability Inspection.

Self-Diagnostic Test

WARNING! Disconnect if necessary all locking units before testing the S2000-2 controller in self-diagnostic mode

To start self-diagnostic test remove the top cover of the controller enclosure and make three short and one long pressing on the tamper switch. 'Short pressing' means 'press and held the tamper switch pressed for 0.1 - 0.5s', while 'long pressing' means 'press and held the tamper switch pressed for at least 1.5s'. Pauses between pressings must not exceed 0.5s.

The test outcome is considered as success if the sequence pressings said above causes the controller behavior as follows:

- The READY indicator flashes rapidly
- The controller sounder plays two beeps
- The LED 1 and LED 2 of the controller lights in turns with red for 1s and green for 1s.
- The contacts of the relay 1 are closed together with LED 1 switching on, the contacts of the relay 2 being closed together with LED 2 switching on.

Condition Inspection of Readers' Connection Circuits

Inspect the condition of readers' circuits by doing the following:

1. Present an unknown access key to the first reader of the S2000-2. The red LED 1 of the S2000-2 and the red LED of the reader must flash three times. The internal sounder of the S2000-2 and the reader sounder, if used and controlled, must play long 'Error' beep each.
2. Repeat the said procedure for the second reader of the S2000-2.

If the S2000-2 controller doesn't respond upon a key presenting it can be caused by mismatching of the reader data format and the set value of reader's *Output Interface* type (which is *Touch Memory* by default – see Reader Configuration Parameters Section of this Manual).

If a long beep is not heard it can indicates that the sound signaling is disabled for the controller or the reader (it is enabled by default – see Reader Configuration Parameters Section of this Manual).

Condition Inspection of LOOP, DOOR and EXIT Circuits

To inspect the conditions of electrical circuits, connected to the LOOP, DOOR and EXIT terminals of the S2000-2 controller, request its ADC readings **using the S2000(M) console** by doing the following:

ENTER CODE:_	Power on the S2000(M) console and enter your PIN-code
⬍ 5 REQUEST INFO	Select REQUEST INFO command by ◀ or ▶ console button and press ENTER, or use 5 console button as the hot key
⬍ 51 ZONE ADC	Select ZONE ADC command by ◀ or ▶ console button and press ENTER, or use 2 console button as the hot key
ADDRESS:_	Enter the S2000-2 network address or select the valid value by ◀ or ▶ console button and press ENTER
ENTER LOOP#:_	Enter gradually the numbers from one to six (or select the proper value by ◀ or ▶ console button and press ENTER) and compare the responded values with the reference values shown below

Table 12. Normal Value Ranges for Some S2000-2 Readings

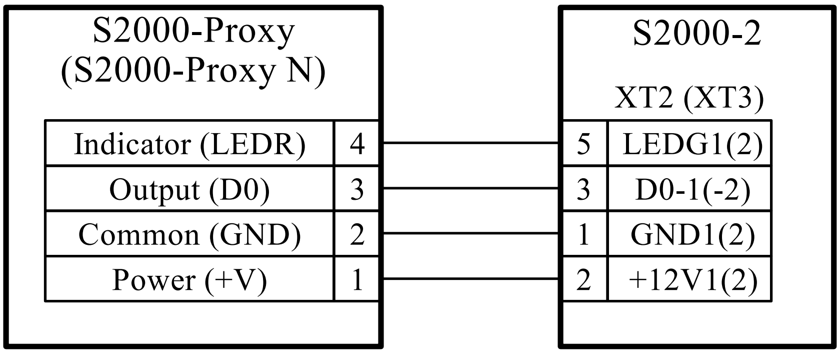
#	The Circuit Identified by This Number	Reference Value Range
1	LOOP1	115…127 (8.2 kOhm)
2	LOOP2	115…127 (8.2 kOhm)
3	DOOR1	145…160 (8.2 kOhm)
4	DOOR2	145…160 (8.2 kOhm)
5	EXIT1	145…160 (8.2 kOhm)
6	EXIT2	145…160 (8.2 kOhm)

Each of the circuits mentioned above is considered to be in good condition if the value returned for the request with the specified number is within the specified range.

Appendix

Connecting Some Models of Readers to the S2000-2 Controller

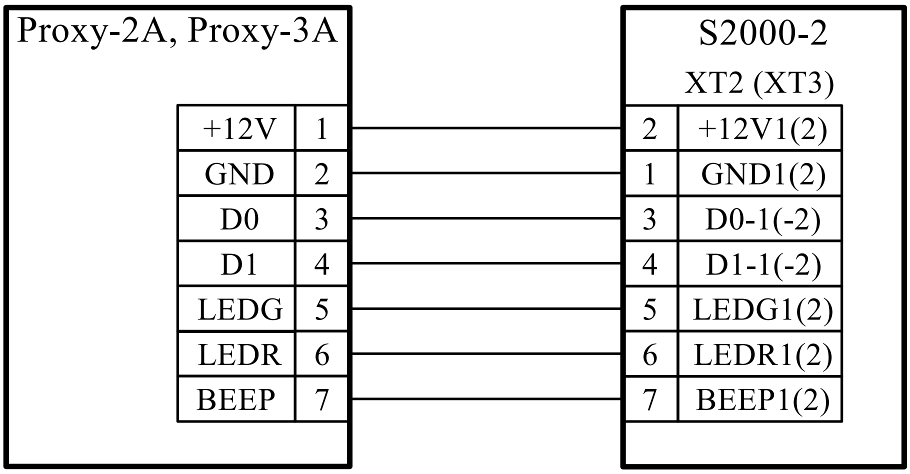
BOLID S2000-PROXY / S2000-PROXY N READER CONNECTION



S2000-2 Configuration Settings

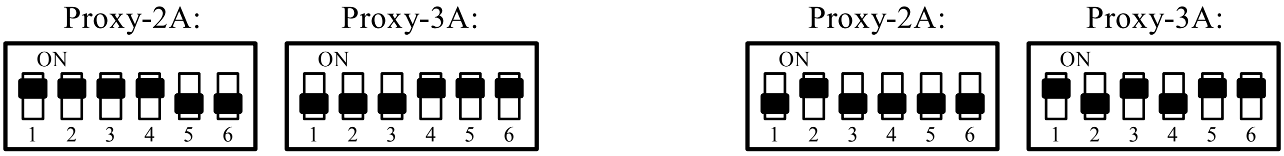
Reader Output Interface	1 – Touch Memory
LED Control Polarity	Forward (1 active)

BOLID PROXY-2A / PROXY-3A READER CONNECTION



Variant 1 –Touch Memory Interface **Variant 2 – Wiegand** Interface

Reader DIP Switches Positions



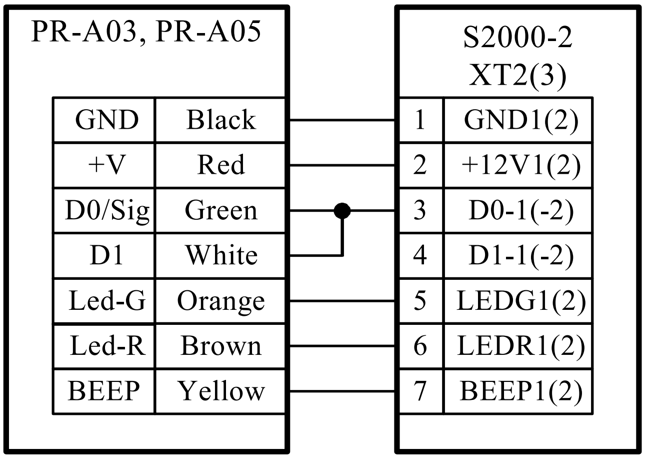
S2000-2 Configuration Settings

Reader Output Interface	**1 Touch Memory**
LED Control Polarity	Forward (1 active)
Sounder Control Polarity	Forward (1 active)

Reader Output Interface	**2 Wiegand**
LED Control Polarity	Reverse (0 active)
Sounder Control Polarity	Reverse (0 active)

PR-A03 / PR-A05 / PR-P09 READER CONNECTION

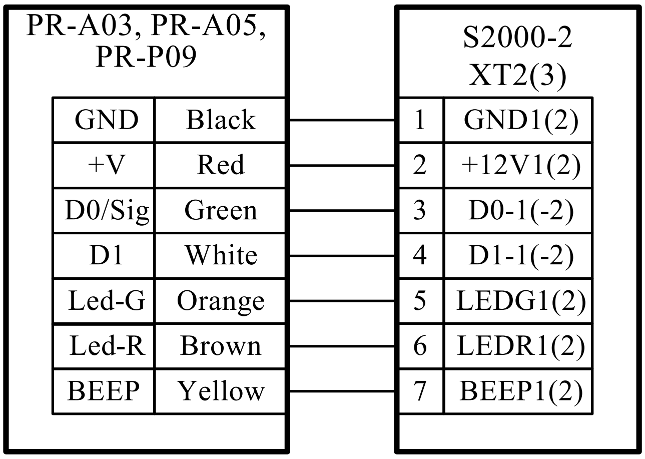
Variant 1 –Touch Memory Interface



PR-A03, PR-A05

			S2000-2 XT2(3)
GND	Black	1	GND1(2)
+V	Red	2	+12V1(2)
D0/Sig	Green	3	D0-1(-2)
D1	White	4	D1-1(-2)
Led-G	Orange	5	LEDG1(2)
Led-R	Brown	6	LEDR1(2)
BEEP	Yellow	7	BEEP1(2)

Variant 2 –Wiegand Interface



PR-A03, PR-A05, PR-P09

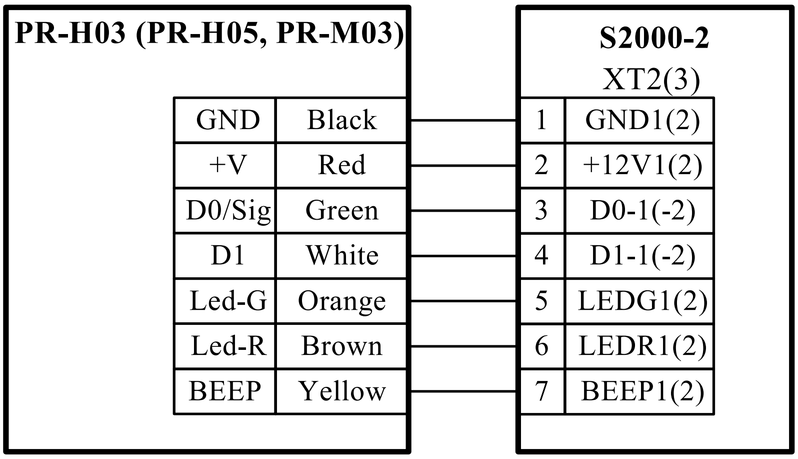
			S2000-2 XT2(3)
GND	Black	1	GND1(2)
+V	Red	2	+12V1(2)
D0/Sig	Green	3	D0-1(-2)
D1	White	4	D1-1(-2)
Led-G	Orange	5	LEDG1(2)
Led-R	Brown	6	LEDR1(2)
BEEP	Yellow	7	BEEP1(2)

S2000-2 Configuration Settings

Reader Output Interface	**1–Touch Memory**
LED Control Polarity	Forward (1 active)
Sounder Control Polarity	Forward (1 active)

Reader Output Interface	**2 – Wiegand**
LED Control Polarity	Reverse (0 active)
Sounder Control Polarity	Reverse (0 active)

PR-H03 / PR-H05 / PR-M03 READER CONNECTION



PR-H03 (PR-H05, PR-M03)

			S2000-2 XT2(3)
GND	Black	1	GND1(2)
+V	Red	2	+12V1(2)
D0/Sig	Green	3	D0-1(-2)
D1	White	4	D1-1(-2)
Led-G	Orange	5	LEDG1(2)
Led-R	Brown	6	LEDR1(2)
BEEP	Yellow	7	BEEP1(2)

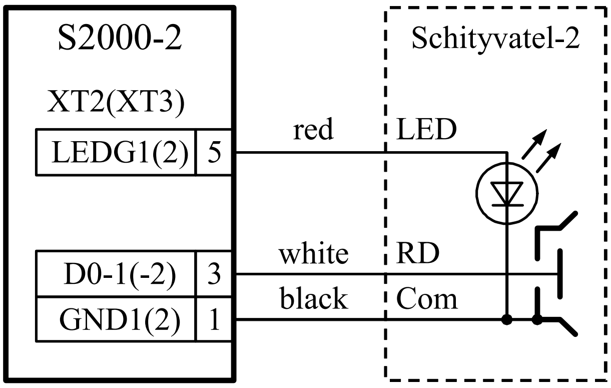
Variant 1 – Touch Memory Interface

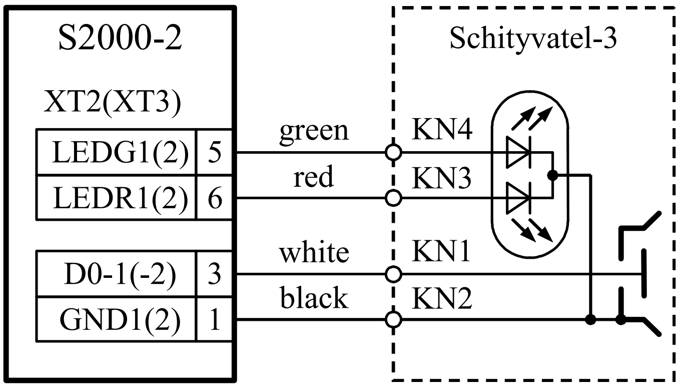
S2000-2 Settings		**Reader's Jumpers**	
Reader Output Interface	1 Touch Memory	red	**remove**
		yellow	**remove**
LED Control Polarity	Forward (1 active)	orange	**remove**
Sounder Control Polarity	Forward (1 active)	green	**remove**

Variant 2 – Wiegand Interface

S2000-2 Settings		**Reader's Jumpers**	
Reader Output Interface	2 Wiegand	red	put on
		yellow	**remove**
LED Control Polarity	Reverse (0 active)	orange	put on
Sounder Control Polarity	Reverse (0 active)	green	put on

BOLID SCHITYVATEL-2 / SCHITYVATEL-3 READER CONNECTION





S2000-2 Configuration Settings

Reader Output Interface	1 – Touch Memory
LED Control Polarity	Forward (1 active)

BOLID ONE YEAR LIMITED WARRANTY

Bolid Company and its divisions and subsidiaries («Seller»), 4 Pionerskaya Str., Korolev 141070, Moscow Region, Russia warrants its security equipment (the «product») to be free from defects in materials and workmanship for one year from date of original purchase, under normal use and service. Seller's obligation is limited to repairing or replacing, at its option, free of charge for parts or labor, any product proven to be defective in materials or workmanship under normal use and service. Seller is not responsible for results where the product is used improperly, where it is used for any application it is not intended for, used under unacceptable environmental conditions and mishandled or stored under improperly. Seller shall have no obligation under this warranty or otherwise if the product is altered or improperly repaired or serviced by anyone other than the Seller. In case of defect, contact the security professional who installed and maintains your security equipment or the Seller for product repair.

This one year Limited Warranty is in lieu of all other express warranties, obligations or liabilities. THERE ARE NO EXPRESS WARRANTIES, WHICH EXTEND BEYOND THE FACE HEREOF. ANY IMPLIED WARRANTIES, OBLIGATIONS OR LIABILITIES MADE BY SELLER IN CONNECTION WITH THIS PRODUCT, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, ARE LIMITED IN DURATION TO A PERIOD OF ONE YEAR FROM THE DATE OF ORIGINAL PURCHASE. ANY ACTION FOR BREACH OF ANY WARRANTY, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, MUST BE BROUGHT WITHIN 12 MONTHS FROM DATE OF ORIGINAL PURCHASE. IN NO CASE SHALL SELLER BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, OR UPON ANY OTHER BASIS OF LIABILITY WHATSOEVER, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT. Some countries do not allow limitation on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Seller does not represent that the product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. Buyer understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery, fire or other events occurring without providing an alarm, but it is not insurance or guarantee that such will not occur or that there will be no personal injury or property loss as a result. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. HOWEVER, IF SELLER IS HELD LIABLE, WHETHER DIRECTLY OR INDIRECTLY, FOR ANY LOSS OR DAMAGE ARISING UNDER THIS LIMITED WARRANTY OR OTHERWISE, REGARDLESS OF CAUSE OR ORIGIN, SELLER'S MAXIMUM LIABILITY SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT, WHICH SHALL BE THE COMPLETE AND EXCLUSIVE REMEDY AGAINST SELLER. This warranty gives you specific legal rights, and you may also have other rights which vary from country to country. No increase or alteration, written or verbal, to this warranty is authorized.

4 Pionerskaya Str., Korolev 141070,
Moscow Region, Russia
Phone/fax: +7 495 513-32-35
Email: info@bolid.ru

www.bolid.com