



# **Sigur E2 Series Controller. Specifications and User Guide**

**Revision dated 06/05/2026**

# Table of Contents

- 1. Introduction ..... 5
- 2. Document version control ..... 6
- 3. Overview and box contents ..... 7
  - 3.1. Circuit board components diagram ..... 7
  - 3.2. Contents of the box ..... 9
- 4. Controller specifications ..... 10
  - 4.1. Physical properties ..... 10
  - 4.2. Electrical properties ..... 10
  - 4.3. Operating conditions ..... 11
  - 4.4. Interfaces ..... 11
- 5. Functionality of controllers in the SIGUR access control system ..... 13
- 6. Installation of the controller ..... 15
  - 6.1. General power supply connection considerations ..... 15
  - 6.2. Power supply of the controller ..... 17
  - 6.3. Connecting and configuring the communication line ..... 18
    - 6.3.1. Ethernet ..... 18
    - 6.3.2. Configuring the IP parameters ..... 18
    - 6.3.3. Resetting the IP parameters ..... 19
  - 6.4. Tamper sensor ..... 19
  - 6.5. Fire alarm and emergency door release ..... 20
    - 6.5.1. Connection options for a 2-wire fire emergency release line ..... 21
  - 6.6. Connection of a security alarm cable ..... 23
- 7. Programming and configuration of the controller ..... 24
  - 7.1. Programming and configuration of the controller, general considerations ..... 24
  - 7.2. Hardware reset ..... 27
  - 7.3. Standard controller configurations ..... 27
    - 7.3.1. Overview of standard configurations ..... 27
    - 7.3.2. Configuration for the Time and Attendance Terminal ..... 28
    - 7.3.3. One Door, Potential Control Mode configuration ..... 31
    - 7.3.4. One Door, Pulse Control Mode configuration ..... 33
    - 7.3.5. Two Doors, Potential Control Mode configuration ..... 35
    - 7.3.6. Two Doors, Pulse Control Mode configuration ..... 37
    - 7.3.7. Turnstile, Potential Control Mode configuration ..... 39
    - 7.3.8. Turnstile, Pulse Control Mode configuration ..... 42
  - 7.4. Configurable controller ports ..... 44
- 8. Connection of readers ..... 45
  - 8.1. Connection of readers, general considerations ..... 45
  - 8.2. General considerations for connecting your readers ..... 45
  - 8.3. Wiegand readers ..... 46
  - 8.4. OSDP readers ..... 48
    - 8.4.1. Indication of readers connected via OSDP ..... 52
    - 8.4.2. Encryption of data transmitted over OSDP ..... 58
  - 8.5. Connection of indication controlled by 5V input ..... 61
  - 8.6. Blacklisted readers ..... 62
- 9. Connection of doors ..... 63

- 9.1. Locks, general considerations ..... 63
  - 9.1.1. Locks, general consideration ..... 63
  - 9.1.2. Electromagnetic locks and electromechanical latches ..... 63
  - 9.1.3. Electromechanical locks ..... 65
  - 9.1.4. Long distances between the controller and the lock ..... 66
  - 9.1.5. Critical considerations on locks and latches ..... 67
- 9.2. Door Open sensors (magnetic contacts) ..... 68
- 9.3. Hall effect sensor ..... 70
- 9.4. RTE buttons ..... 70
- 9.5. Connection options for doors ..... 71
- 10. Connection of intercoms ..... 73
- 11. Connection of card collectors ..... 75
- 12. Connection of breathalyzers ..... 76
  - 12.1. Connection of breathalyzers, general considerations ..... 76
    - 12.1.1. Standard mode ..... 76
    - 12.1.2. Extended mode ..... 76
  - 12.2. Alcobarrier (by Alcotector) ..... 77
  - 12.3. Alcoframe (by Laser Systems) ..... 78
- 13. Turnstiles and swing gates ..... 80
  - 13.1. Connection of turnstiles, general considerations ..... 80
  - 13.2. Turnstile control options ..... 80
  - 13.3. Available access control sensor configurations ..... 80
  - 13.4. Turnstile remote control, general considerations ..... 81
  - 13.5. Connection option for a turnstile ..... 81
  - 13.6. 3V turnstiles ..... 82
  - 13.7. PERCo turnstiles and swing gates ..... 83
    - 13.7.1. PERCo TTR-04.1, TTD-03, T-5, TTR-07, TTR-08A, TTD-08A ..... 83
    - 13.7.2. PERCo-RTD-15 ..... 84
    - 13.7.3. PERCo ST-01, ST-02 ..... 84
    - 13.7.4. PERCo remote control unit ..... 86
  - 13.8. Praktika turnstiles (Oxgard) ..... 87
    - 13.8.1. Praktika T-01...06 ..... 87
    - 13.8.2. Cube C-04 ..... 88
  - 13.9. CARDDEX turnstiles ..... 89
    - 13.9.1. CARDDEX CBU-250 (CBU-150/250) control unit ..... 89
    - 13.9.2. CARDDEX CBU-240 control unit ..... 91
- 14. Controller operating logic ..... 93
  - 14.1. Startup of the controller ..... 93
  - 14.2. Indication lines of the reader ..... 93
  - 14.3. Processing of fire alarm signals ..... 94
  - 14.4. Processing of security and fire alarm signals ..... 94
  - 14.5. General-purpose outputs ..... 94
  - 14.6. Input and output protection circuits of the controller ..... 95
    - 14.6.1. Power supply of the controller ..... 95
    - 14.6.2. Power supply of the readers ..... 95
    - 14.6.3. Outputs of the controller ..... 95
    - 14.6.4. Inputs of the controller ..... 96
  - 14.7. Access points controlled by doors ..... 96
    - 14.7.1. Operating modes ..... 96

- 14.7.2. RTE buttons ..... 97
    - 14.7.3. Lock buttons ..... 97
  - 14.8. Access points controlled by turnstiles ..... 97
    - 14.8.1. Operating modes ..... 97
    - 14.8.2. Operating the turnstile remote control unit ..... 98
- 15. Troubleshooting ..... 100
  - 15.1. Troubleshooting power supply and controller startup issues ..... 100
  - 15.2. Troubleshooting Ethernet connection ..... 101
  - 15.3. Troubleshooting server connection issues ..... 101
  - 15.4. Troubleshooting lock connection issues ..... 102
  - 15.5. Troubleshooting reader connection issues ..... 102
  - 15.6. Troubleshooting turnstile connection issues ..... 103
- 16. Appendix. Sound indication of the controller ..... 105
- 17. Appendix. LED indication of the controller ..... 106
- 18. Appendix. Controller configuration parameters and values ..... 109
- 19. Appendix. Recommended cable choices ..... 112
- 20. Appendix. Character encoding for readers with a keypad ..... 114
- 21. Contacts ..... 115

# 1. Introduction

This document provides an overview of Sigur controllers and their functionality. Sigur controllers are designed to operate as part of the Sigur Access Control System (ACS).

Depending on the setup and availability of terminals, a controller can control two access points of different types, including doors, turnstiles, arm barriers or gates in the basic operating mode.

Sigur controllers instantaneously process all access requests (a card presented, a button pressed, etc.).

The response time is not affected by the number of controllers in the system, the quality of your connection, the number of cardholders or the length of your communication lines.

Even if the server is not available at the moment, the controller will decide on whether to grant access independently based on the cardholders and access rules database stored in the non-volatile memory of the controller.

All detected events are stored in the non-volatile memory of the controller. The date and time of an event are registered based on the integrated real-time clock. When the server connection is restored, the events are automatically synchronized with the server of your access control system.

This ensures maximum reliability of the system, independent operation of the controllers regardless of the availability of the server and quick responses of the controllers to events in real time.

The manufacturer is responsible for the accuracy of the documentation provided and, if the system components are significantly modified, it will provide an updated version of this documentation.

This document applies to Sigur software ver.1.6.8.101 and compatible controller firmware version 1.24.0.

## 2. Document version control

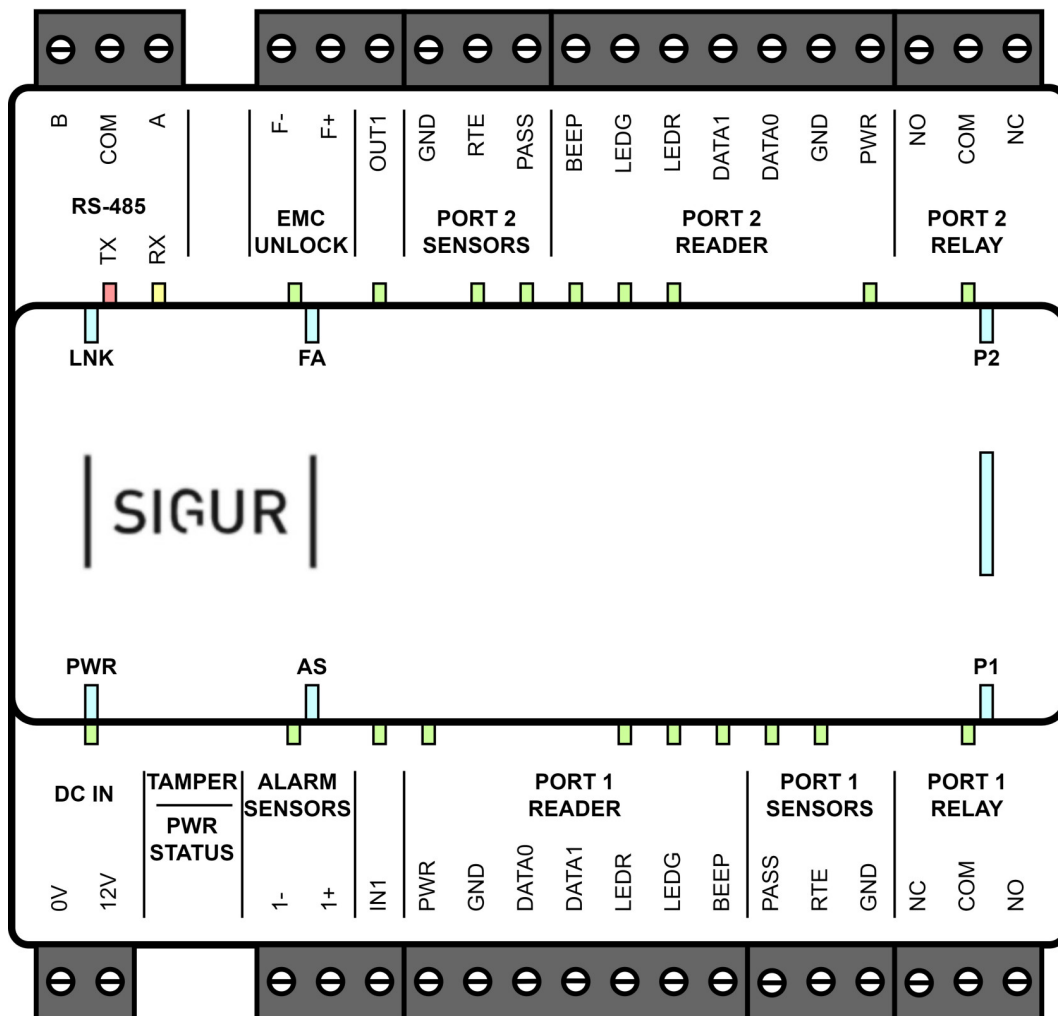
Below is the document revision history.

Revision	Issue date	Changes
0001	May 6, 2026	First issued.

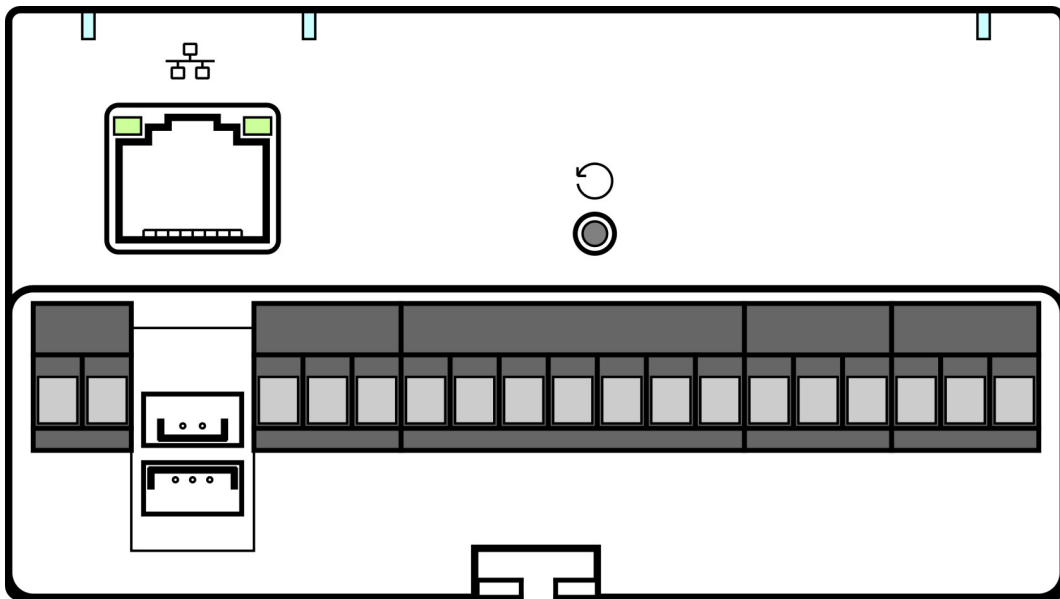
### 3. Overview and box contents

#### 3.1. Circuit board components diagram

The controller is a microprocessor circuit board in a plastic case mounted on a DIN rail.



Layout of the main components on the E2 controller board, top view.



E2 controller, side view.

**List of elements located on the controller board.**

Element	Description
	Controller IP settings reset button.
	Ethernet port.
MAIN	Status of the controller.
PWR	Status of the power supply of the controller.
LNK	Status of connection between the controller and the server.
FA	Status of the fire alarm line.
AS	Status of the security alarm line.
P1	Status of the PORT1 terminal group.
P2	Status of the PORT2 terminal group.
RX	(yellow) Indicates that data is being received via RS485 (OSDP).
TX	(red) Indicates that data is being sent via RS485 (OSDP).

## 3.2. Contents of the box

### Sigur E2 box contents.

Item No.	Description	Quantity
1	Sigur controller	1 pc
2	Technical datasheet	1 pc
3	IP reset key	1 pc
4	Cable to connect to the TAMPER port <sup>1</sup>	1 pc
5	Cable to connect to the PWR STATUS port <sup>1</sup>	1 pc

<sup>1</sup> May vary in different batches. Supplied upon request.

## 4. Controller specifications

### 4.1. Physical properties

Dimensions	108 * 90 * 60 mm
Case	ABS plastic
Installation	TH35 DIN rail
Net weight, max.	0.3 kg
Gross weight, max.	0.5 kg

### 4.2. Electrical properties

Supply voltage	10V...15V
Current	max. 250mA
Wattage	max. 3.75W
Power supply line tripping voltage	18V
Max. switching voltage of the power relay outputs	30V
Max. switching current of the power relay outputs	10A Normally open mode: 5A Normally closed mode: 3A
Max. switching voltage of the open collector outputs	30V
Max. switching current of the open collector outputs	0.1A

<p>Integrated controller safety circuits</p>	<p><b>Power supply:</b></p> <ul style="list-style-type: none"> <li>• Overvoltage and reverse polarity protection.</li> <li>• All power supply circuits of all readers are independently protected against overloads.</li> </ul> <p><b>Communication line (Ethernet):</b></p> <ul style="list-style-type: none"> <li>• Complete galvanic isolation.</li> </ul> <p><b>Input interfaces:</b></p> <ul style="list-style-type: none"> <li>• All lines are protected against overloads and overvoltages.</li> </ul> <p><b>Output interfaces:</b></p> <ul style="list-style-type: none"> <li>• All lines are protected against overloads and overvoltages.</li> </ul>
--	--

### 4.3. Operating conditions

IP rating	IP20
Ambient temperature	-40...+50°C
Relative humidity	max. 85% at t°=30 °C
Atmospheric pressure	84...106.7kPa

### 4.4. Interfaces

Communication line	<p>One standard Ethernet port.                  Data rate: Ethernet 10/100BASE-TX, full duplex.                  Connection to the IP network: via active network equipment.                  Supported protocols include DHCP, DTLS, SNMP v3, SNMP Trap v2.</p>
Connection of sensors	Up to 5 sensors with open collector or dry contact outputs.
Open collector control outputs	7 outputs, including reader induction control lines.
Power relay outputs	2 relays, each relay's terminal block is set for switching.

Supported readers	<ul style="list-style-type: none"> <li>• Wiegand or OSDP readers.</li> <li>• Clock &amp; Data readers (Ompron 5 bit, Magstripe Track II).</li> <li>• OSDP v2.2 readers.</li> </ul> <p>Supported Wiegand formats: Wiegand-26, Wiegand-34, Wiegand-36, Wiegand-37, Wiegand-42, Wiegand-58. Additionally Wiegand 4, Wiegand HID (6 bits) or Wiegand-Motorola (8 bits) support keypad connection.<sup>1</sup></p>
Max. number of connected readers (regardless of interface)	4
Max. number of Wiegand and Clock & Data readers	2
Max. number of OSDP readers	4
Connection to a fire alarm system	2-wire galvanically isolated line to connect several controllers to a single fire alarm cable. When the alarm sets off, the cable connected to the controllers will be tripped.
Connection of a security alarm cable	Two-wire line. When the alarm sets off, the cable connected to the controller will be tripped.

<sup>1</sup> Note: Prior to using the reader with a keypad, please check if the output interface and the character encoding comply with the [Character Encoding for Readers with a Keypad](#) section of this document. Some readers may operate in the package accumulation mode, i.e. they will not generate Wiegand packages for every keypress, instead they will generate a standard Wiegand package (such as Wiegand 26) when the entire code is entered. If this is the case, then you will not need to check if the character encoding complies with the [Character Encoding for Readers with a Keypad](#) section of this document.

## 5. Functionality of controllers in the SIGUR access control system

Sigur controllers are designed to operate as part of the Sigur access control system and control various devices connected to them over a network.

### Controller parameters in the Sigur access control system.

Max. number of autonomously stored credentials <sup>1</sup>	90.000 <sup>1</sup>
Number of autonomously stored events <sup>2</sup>	400.000 <sup>2</sup>
Number of autonomously stored access rules (time zones) <sup>2</sup>	30.000 <sup>2</sup>
Supported types of access points	<ol style="list-style-type: none"> <li>1. <b>Doors</b> with electromagnetic and electromechanical locks or latches.</li> <li>2. <b>Turnstiles</b>. Both pulse and potential control modes are supported as well as three sensor signal processing modes.</li> <li>3. <b>Swing gates</b>. Electromechanical gates of any type.</li> </ol>
Alternatively	If not connected to any types of doors or gates, the controller can operate as a time and attendance tracker.
Antipassback and zonal control	<p>When connected to the server, provides global antipassback functionality with configurable controlled periods.</p> <p>Zonal control and monitoring of personnel movements.</p>
Autonomous controller status indication	<ol style="list-style-type: none"> <li>1. LED and sound indication of the controller status and configuration errors.</li> <li>2. Power supply indication (mains or battery, supply voltage outside the operating range, battery performance).</li> <li>3. Ethernet status indication (reception, transmission).</li> <li>4. Controller inputs and outputs status indication.</li> </ol>

Firmware updates	The firmware can be updated via a communication line from any client or server PC connected to the Sigur system.
------------------	--

<sup>1</sup> The number of credentials that can be stored in the controller memory will also depend on the Sigur software license used.

<sup>2</sup> The autonomous memory will be distributed automatically between access rules and events. The numbers provided in this table reflect one of the memory distribution options. In real life, the values can vary depending on the nature of the event and the complexity of the access rules.

## 6. Installation of the controller

Please read these instructions and specifications of the system carefully prior to installation.

Before installing the controller, please read the section of this manual on the relevant configuration. First, you should find optimal locations for your controllers, readers, other access control equipment and sensors. Mark the desired mounting location. Perform all the cablework. Check every line and cable for breaks and faults. Install all turnstiles, arm barriers, locks, sensors, etc. according to the instructions in the manuals for the relevant equipment.

Consider the following when choosing the location for controllers and cabling:

1. Do not position your controllers within 1 m from power generators, magnetic starters, electric motors, AC relays, thyristor light controllers and other powerful sources of electromagnetic interference.
2. All signal and LV cables should be positioned at least 50 cm apart from AC power cables, control cables for powerful motors, pumps, drives, etc.
3. All signal cables can cross power cables only at the right angle (90°).
4. Signal cables can be extended only by soldering. Power cables can be extended by using terminal blocks.

All cables connected to the controller must be securely attached.

The location of the controller should be chosen taking into account convenience of future maintenance.

The cable types depend on the installation and operating conditions, whether they are laid inside, outside or are hanged, etc. You can find some cabling considerations in the [Recommended Cable Choices](#) section of this document.



You must power off the controller before connecting or disconnecting any equipment.

### 6.1. General power supply connection considerations

Any suitable cables (at least 0.75mm<sup>2</sup>) can be used, including flat vinyl-vinyl cords, general purpose flat flexible cords, general-purpose flat cords, vinyl connection cords or vinyl-vinyl bare cords (for external cables).

- If the controller is the only device powered by a power supply unit, install it at any convenient location between the closest distribution board and the controller. Make sure it provides 12VDC output and the min. current of 300mA.

- If in addition to the controller, you will use the same power supply unit to power up readers, locks and other peripherals, make sure that the capacity of the power supply unit used is enough to power up all connected devices plus that it has reserve capacity of the supply current of 10–15%. Reserve power capacity of the power supply unit is needed to ensure correct operation of the controller in emergencies, such as short circuiting of communications lines, power supply circuits of readers, etc.

In case of emergency, the internal safety circuits of the controller will power off the overloaded or short-circuited line; however, when tripped, the power demand on the power source can surge for a short period of time.

The following uninterruptible power supply units are recommended: Adelsystem CBI, Comatec USV2, MEAN WELL DRS-240.



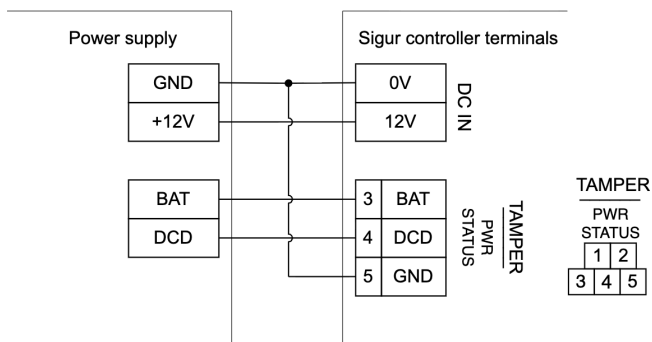
When using an uninterruptible power supply unit without integrated battery protection, it is recommended to equip it with a third-party battery protection device.



When using a power supply unit in a metal case, make sure to use a protective ground line connected to it.

## 6.2. Power supply of the controller

The controller uses the voltage of 10...15VDC and the max. current of 250mA.



Connection of the power source to the controller.

After the installation, the power supply unit is connected to a ~220V single-phase power outlet.

### Connection of an additional status control line for power supply

The DCD line is an additional input used by the controller to monitor the supply voltage of the power supply unit. The DCD input is controlled by connecting it to the negative voltage (via the open collector or dry contact output) or supplying the logical low voltage (0...0.5V). If logic level control is used to control this input, the max. voltage must not exceed 3.3V.

Logical low voltage on this input corresponds to the power supply unit powered up from the mains.

Some of uninterruptible power supply unit models have outputs complying with the above requirements.



By default, the DCD input is not active. If connected, this input must be enabled in the controller settings. To do this, go to the Client software and select your controller from the list on the Access Points tab and press the Settings button. Uncheck the Show only basic settings box on the General tab and enable the Use power source control sensor parameter.

The BAT line is an additional input used by the controller to monitor the battery status of the power supply unit. The BAT input is controlled by connecting it to the negative voltage (via the open collector or dry contact output) or supplying the logical low voltage (0...0.5 V). If logic level control is used to control this input, the max. voltage must not exceed 3.3V.

Logical low voltage on this input corresponds to a non-working battery.



By default, the BAT input is active.

## 6.3. Connecting and configuring the communication line

### 6.3.1. Ethernet

The controllers are connected to the Ethernet network via a standard (straight-through) patch cable with one end connected to the RJ45 port on the controller and the other end connected to a respective port on the active Ethernet equipment (hub, switch, etc.).

However, for initial configuration purposes the controller can be connected directly to the network card of the ACS server machine.

### 6.3.2. Configuring the IP parameters

To ensure stable operation of the controller, it must be configured to obtain the IP address through DHCP or you will have to manually configure the following parameters:

- IP address;
- subnet mask;
- default gateway.

By default, obtaining the IP parameters and server address through DHCP is enabled on the controller. If the network has no available DHCP server when the controller is launched, the controller will automatically assign the IP address in the format of 169.254.xxx.xxx, where "xxx" is a number between 1 and 254.

The default password to access the settings is "**sigur**" (without quotation marks). You can change the password during the configuration process.

To configure your controller:

- Connect it to a vacant port of your local network.
- Power it on.

- Install the Sigur server software on one of the computers in your local network (you do not need to launch the server service or have a license).
- Configure all the required parameters in the Server Administration tool.

For a detailed configuration process, please see the [Sigur ACS Quick Guide](#).

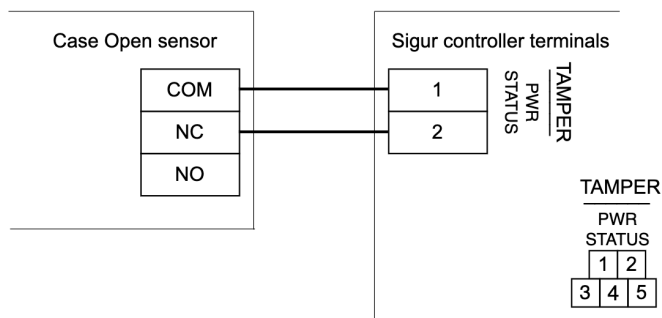
If a firewall is used in your IP network, for the controller to operate normally, enable free exchange of UDP datagrams between the system server and controllers on ports 3303 and 3305 (including ports 3306 and 3307 if the controller and the server communicate over DTLS).

### 6.3.3. Resetting the IP parameters

In some cases, the controller might need to be reset to default. For instance, if the password is lost or the incorrect settings make the controller inaccessible via the IP network. To reset the controller, press and hold the IP reset button (which can be found on the side of the controller case next to the Ethernet port) using a special key included in the box with your controller. Two short beeps mean that the device is reset to default.

## 6.4. Tamper sensor

When connected, the Tamper sensor enables monitoring of the opening and closing of the external case or rack. By default, a normally-closed sensor is supposed to be connected as a Tamper sensor.



Connection of a Tamper sensor to the controller.



By default, the TAMPER input is not active. If connected, this input must be enabled in the controller settings. To do this, go to the **Client** software and select your controller from the list on the **Access Points** tab and press the **Settings** button. Uncheck the **Show only basic settings** box on the General tab and enable the **Use Case Open sensor** parameter.

## 6.5. Fire alarm and emergency door release

Connection of fire alarm or an emergency door release button will ensure emergency unlocking of access points (doors, turnstiles, arm barriers, etc.) in case of fire.

They are connected to the galvanically isolated controller inputs to ensure that the system works properly even if there is a significant potential difference between the power supply circuits of different controllers.

Please see the detailed description of the fire alarm inputs in the [Processing of Fire Alarm Signals](#) section of this document.



By default, the input is not active. If connected, this input must be enabled in the controller settings.

To do this, go to the **Client** software and select your controller from the list on the **Access Points** tab and press the **Settings** button. Uncheck the **Show only basic settings** box on the **General** tab and enable the **Use fire alarm sensor** parameter.

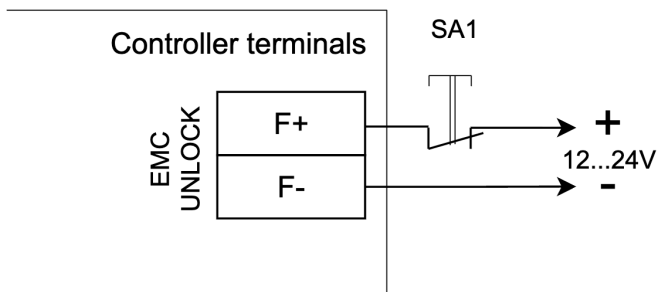
### Symbols used in the diagrams below.

SA1	Normally-closed emergency release button, active only for Controller 1.
SA2	Normally-closed emergency release button, active for all controllers connected to the same line.
K1	Normally-closed fire alarm relay that opens if the alarm is activated.

Examples of alarm devices (SA1, SA2) that can be used: manual fire and security alarm device TANTOS TS-ERButton.

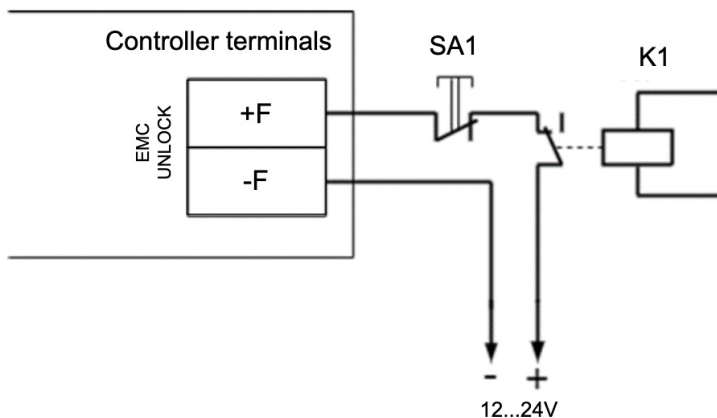
### 6.5.1. Connection options for a 2-wire fire emergency release line

- The button unlocks one controller:



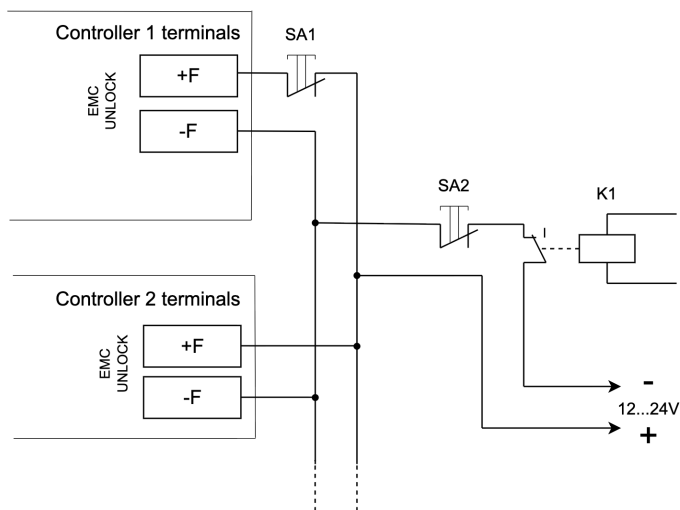
Connection of an emergency release button to one controller.

- The SA1 button and K1 relay unlock one controller:



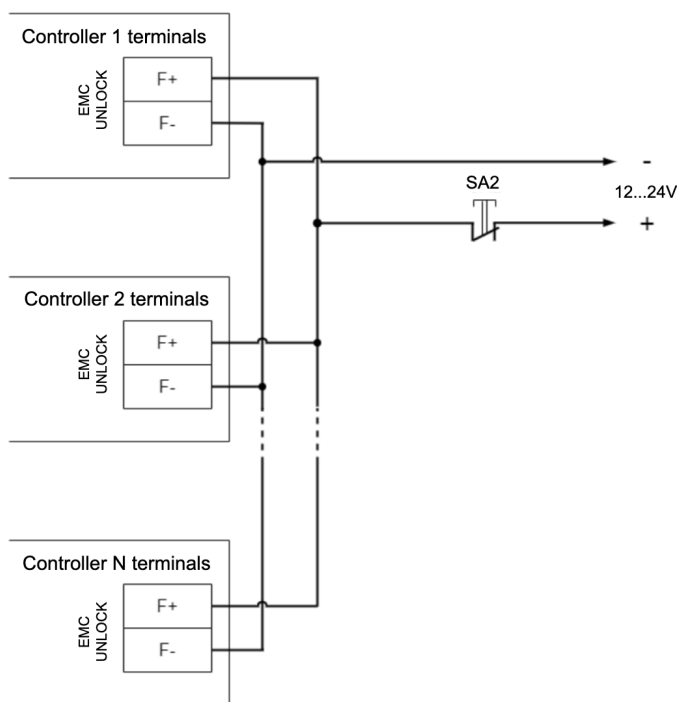
Connection of a fire alarm line and emergency release button to the controller.

- The SA1 button unlocks only its own controller, while the SA2 button and the K1 relay unlock all controllers on the line. An external power supply unit is used to power up the fire alarm line:



Connection of a fire alarm line and emergency release buttons to multiple controllers.

- One button unlocks multiple controllers:



Connection of an emergency release button to multiple controllers.

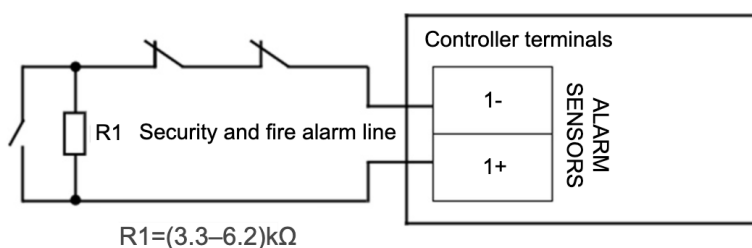
## 6.6. Connection of a security alarm cable

The controller can operate one security and fire alarm line to instantly notify about fire or unauthorized access to the territory controlled by sensors.

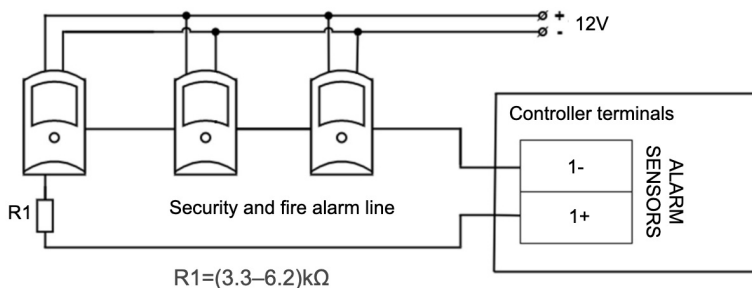
Please see the detailed description of the security and fire alarm input in the Processing of Security and Fire Alarm Signals section of this document.

The security and fire alarm line is connected to the ALARM SENSORS terminals of the controller: 1+ and 1-. The voltage of 12V is supplied to these terminals of the controller to power up the sensors.

Below are connection options for the security and fire alarm line.



Connection of security and fire alarm sensors without an external power source.



Connection of security and fire alarm sensors requiring an external power source.

## 7. Programming and configuration of the controller

Our controllers are flexible and versatile and support a wide range of access point types of various manufacturers.

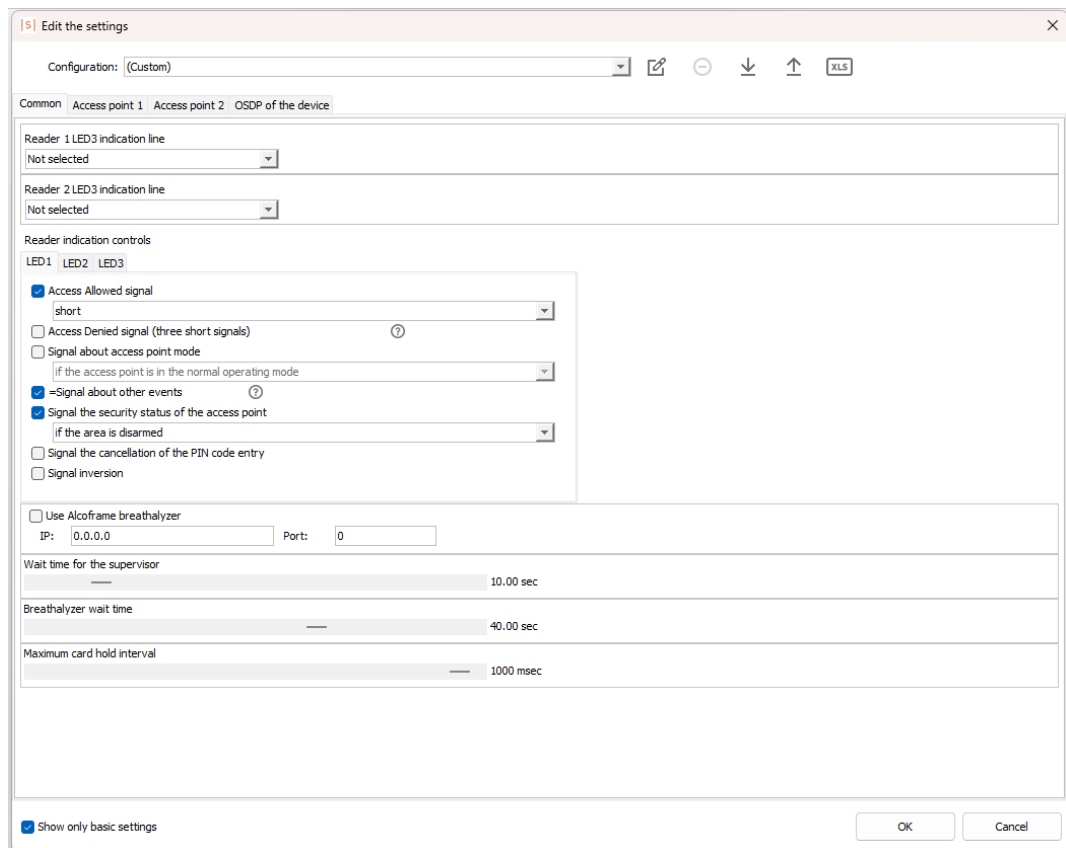
To fine-tune the controller to work with a specific access point type, please read the section of the manual on the respective equipment and the examples of connection carefully. If you cannot find your equipment in this document, please contact us via our [website](#) or [email](#).

### 7.1. Programming and configuration of the controller, general considerations

You can configure the basic parameters and select a configuration of the controller in the Client software (**Access Points** tab > **Settings** button).

For most applications, we recommend using the standard terminal configurations for logical functions (as set in the default settings). Where necessary, you can assign your own values.

The user can edit the configuration of any controller in the controller settings accessed from the **Access Points** tab by selecting the respective access point and clicking the **Settings** button on the right of the **Access Points** tab. When the button is pressed, the selected access points will be analyzed and the **Edit Settings** window will open.



Controller settings editor.

In the settings window, you can change the default configuration and save it as a custom configuration.

The configuration control buttons are found at the top of the window:

- **Rename configuration.** Renames a newly created configuration. The configuration will become available for any controller and can be exported to a file.
- **Delete configuration.** Deletes a configuration from the list.
- **Export configurations to file.** Saves the custom configuration with all assigned functions and parameters to a file. To save the configuration, please rename it.
- **Import configurations from file.** Uploads a configuration from a file with all assigned functions and parameters.
- **Export configuration to MS Excel (.xls).** Saves the configuration description (assigned functions and parameters) to an .xls file.

The configuration settings include:

1. Configuration of access points controlled by the controller. The controller can support up to two access points of different types. Parameters for each of them (ports of the readers, active control lines, sensors, buttons, etc.) are set on the **Access Point 1/2** tabs. The selected access point type (doors, turnstiles, gates / arm barriers or terminals) affects which controller options are available

and the general control logic of the selected access point.

i

If you manually change the access point type, all functions assigned to real inputs and outputs of the controller will also have to be configured manually.

2. Configuration of common parameters for all access points connected to the controller. These parameters can be configured on the General tab, including such parameters as reader indications, timing, etc.

To assign a function, please find it in the function list of a particular access point and first select the physical input / output to which the equipment is connected from the dropdown menu and then the default normal state (closed or open for inputs and active or not active for outputs).

Common
Access point 1
Access point 2
OSDP of the device

Access point type: Door

---

Entrance reader port  
PORT 2 READER

Exit reader port  
PORT 1 READER

Lock control line  
PORT 1 RELAY normally not active

Open sensor  
PASS (PORT 1 SENSORS) normally closed

Request permit to enter button  
Not selected

Request permit to exit button  
RTE (PORT 2 SENSORS) normally closed

Wait time till the door opens  
5.00 sec

Controls:  
Potential

Alarm line: Not selected

Access point settings view.

## 7.2. Hardware reset

If needed, you can perform a hard reset of the controller. The following data will be reset (erased):

- controller network parameters (DHCP-based assignment of IP parameters for the controller and server is enabled);
- password for access to settings (reset to the default value "sigur ");
- SNMP parameters;
- DTLS encryption profile;
- installed configuration for management of connected access points;
- all uploaded identifier data and access time intervals.

Access events stored in the controller's non-volatile memory are preserved.

To perform a hardware reset, press and hold the IP parameter reset button for 3 seconds using the special tool (supplied with the controller). The button is located on the side panel of the enclosure near the Ethernet connector.

The short audible signals confirm successful completion of the operation.

If the procedure cannot be completed successfully, please contact Sigur technical support.

## 7.3. Standard controller configurations

### 7.3.1. Overview of standard configurations

You can select one of the standard configurations in the Client software.

To do this, select an access point on the Access Points tab, press the Settings button and select the configuration from the Configuration dropdown menu. We recommend using standard configurations (listed in the table below). However, you can always modify standard configurations or create custom configurations.

**Standard controller configurations.**

No.	Name	Description
1	Time and attendance terminal.	The controller operates as a terminal and collects employees' check-ins and check-outs. Access point control functionality is not available.
2	One door, potential control mode; One door, pulse control mode.	The controller operates one access point of the Door type. There are two readers (one for the entrance and one for the exit). Locks are operated in either the potential or pulse control mode.
3	Two doors, potential control mode; Two doors, pulse control mode.	The controller operates two access points of the Door type. There is one reader for each door (for the entrance) and one button for each door for the exit. Locks are operated in either the potential or pulse control mode.
4	Turnstile, potential control mode; Turnstile, pulse control mode.	The controller operates one access point of the Turnstile type. There are two readers (one for the entrance and one for the exit). It operates in either the potential or pulse control mode.

**7.3.2. Configuration for the Time and Attendance Terminal**

This configuration can be used if the controller is not connected to any access points (doors, turnstiles, arm barriers, etc.).

In this configuration, the controller will register all employees' workplace check-ins and check-outs (using their electronic IDs) and generally access events for any cardholders (when two consecutive sensors are passed, depending on the direction).

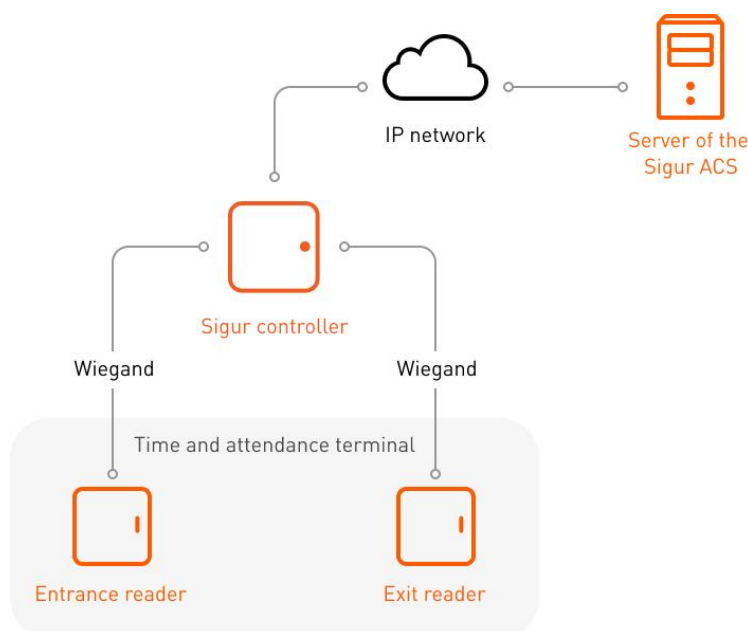
When a card is tapped on the reader, the controller will automatically register a check-in or a check-out for this cardholder.

If consecutive access control sensors are installed, the controller will be able to additionally register the direction of access (entry or exit).



Please keep in mind that the controller in this configuration does not send any signals other than reader indication, which is always the same. Relays and general-purpose outputs are disabled. To enable control of other equipment, such as information displays, please use the **One Door** mode of the controller.  
 If the controller is used in any other setting (including **One Door**), it will also be able to track time and attendance.

Two readers are connected to the controller and optionally two access control sensors.



Connection option for the Time and Attendance Terminal configuration.

The readers are connected to the controller terminals according to the Connection of Readers section of this document.

**Standard Time and Attendance Terminal configuration.**

Порт	Role	Description
PORT1 READER	Port of the entrance reader.	The check-in reader of the first terminal.
PORT2 READER	Port of the exit reader.	The check-out reader of the first terminal.

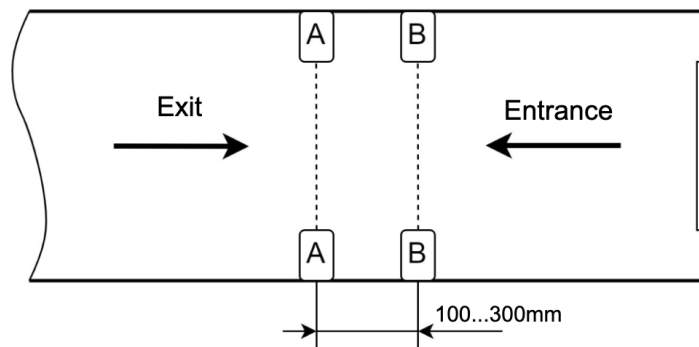
Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

If you want to register access events without electronic IDs, you can modify the standard configuration by connecting access control sensors to the controller and adding the respective settings.

The distance between the beams of photoelectric sensors must be between 100...300mm.

To avoid the sensors affecting each other, we recommend installing them as follows: the emitter of the first sensor and the receiver of the second sensor on one side and the receiver of the first sensor and the emitter of the second sensor on the other side.

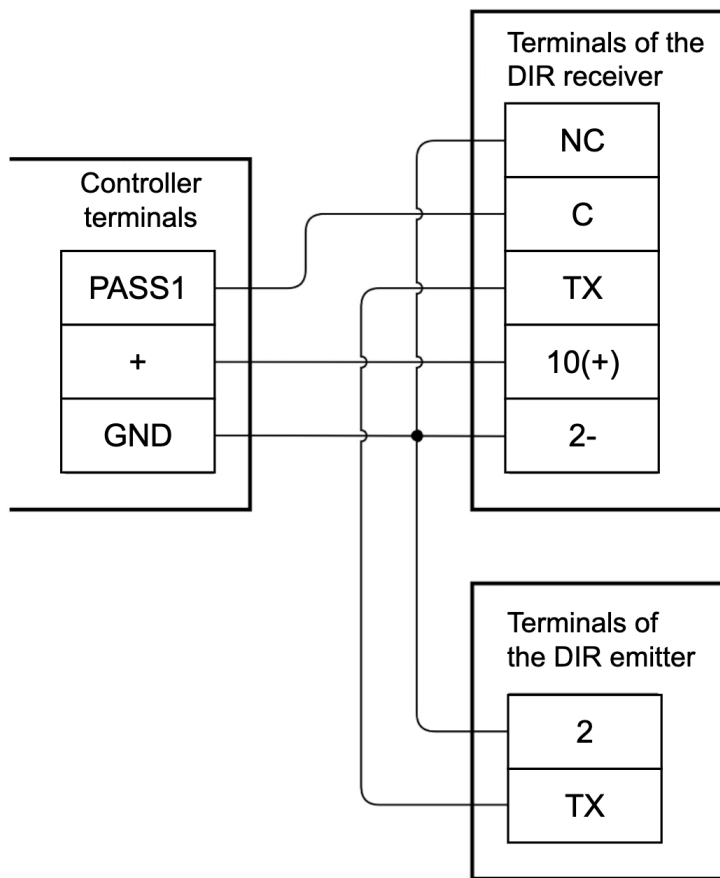
Sensor A is activated first for exit. Sensor B is activated first for entry.



Example locations of access control sensors in the hallway.

**Example of additional port mapping in the Time and Attendance Terminal configuration.**

Port	Role
PASS (PORT 1 SENSORS)	Entrance access control sensor line (normally closed).
PASS (PORT 2 SENSORS)	Exit access control sensor line (normally closed).



Example connection of a CAME DIR photoelectric sensor for Time and Attendance Terminal configuration.

**Designations on the figure:**

- Terminal "+" means +12V power supply of the controller.
- A DIR photoelectric sensor shall be set to 12V power supply.
- The other photoelectric sensors are connected in the same way to PASS 1 and PASS 2 terminals.

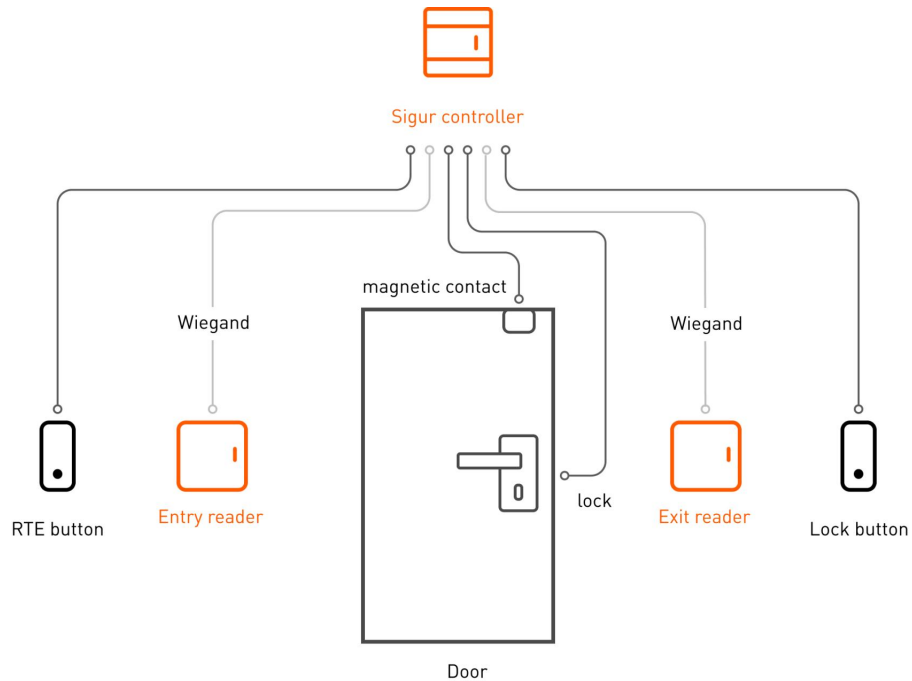
**7.3.3. One Door, Potential Control Mode configuration**

In this configuration, the controller can operate one door fitted with a lock in the potential control mode (the lock is locked when powered on). These usually include electromagnetic locks or electromechanical latches.

The controller can operate one door. Below is the list of access control equipment that can also be connected to the controller:

- lock;
- door open sensor (magnetic contact);
- entrance reader;
- exit reader;
- request to enter (RTE) button;
- request to exit (RTE) button;

- door lock button;
- security desk door release button.



Equipment connection for the One Door configuration.

Either readers or RTE buttons can be located at the entrance and exit. Different readers and buttons for exit and entrance allow the system to identify the direction of access through the door.

A security desk door release button allows the security guard to open the door manually and the event will be recorded in the system as an unknown direction access granted from the security control panel.

The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

**Port mapping in the standard One Door, Potential Control Mode configuration.**

Port	Role	Description
PORT 1 READER	Port of the entrance reader.	
PORT 2 READER	Port of the exit reader.	

Port	Role	Description
PORT 1 RELAY	Lock control line.	The relay is activated when the locking signal is received.
PORT 2 RELAY	Unlock control line.	The relay is activated when the unlocking signal is received.
PORT 1 SENSORS - PASS	Open sensor (normally closed).	
PORT 1 SENSORS - RTE	Request to Enter button (normally open).	
PORT 2 SENSORS - RTE	Request to Exit button (normally open).	
IN1	Unknown direction RTE button (normally open).	Operating as an Unlock button with an unknown access direction or in the Access Granted by Security mode.

**Settings for the standard One Door, Potential Control Mode configuration.**

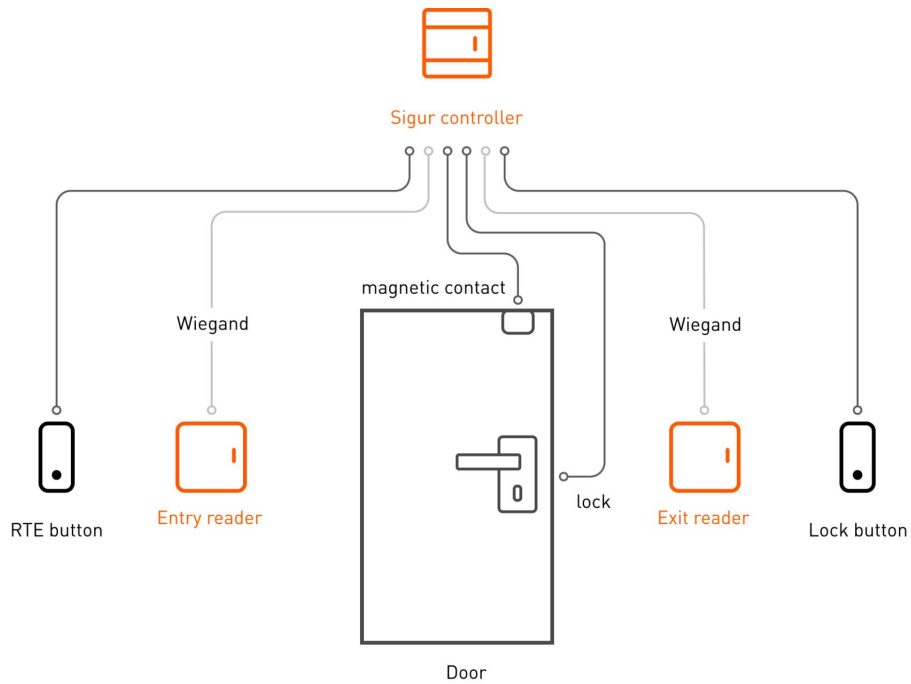
Parameter	Value	Description
Control:	Potential.	The relays stay switched while waiting for an access event.

**7.3.4. One Door, Pulse Control Mode configuration**

In this configuration, the controller can operate one door fitted with a lock in the pulse control mode. These usually include electromechanical locks, but not latches.

The controller can operate one door. Below is the list of access control equipment that can also be connected to the controller:

- lock;
- door open sensor (magnetic contact);
- entrance reader;
- exit reader;
- request to enter (RTE) button;
- request to exit (RTE) button;
- door lock button;
- security desk door release button.



Equipment connection option for the One Door configuration.

Either readers or RTE buttons can be located at the entrance and exit. Different readers and buttons for exit and entrance allow the system to identify the direction of access through the door.

A security desk door release button allows the security guard to open the door manually and the event will be recorded in the system as an unknown direction access granted from the security control panel.

The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

**Port mapping in the standard One Door, Pulse Control Mode configuration.**

Port	Role	Description
PORT 1 READER	Port of the entrance reader.	
PORT 2 READER	Port of the exit reader.	
PORT 1 RELAY	Lock control line.	The relay is activated when the locking signal is received.

Port	Role	Description
PORT 2 RELAY	Unlock control line.	The relay is activated when the unlocking signal is received.
PORT 1 SENSORS - PASS	Open sensor (normally closed).	
PORT 1 SENSORS - RTE	Request to Enter button (normally open).	
PORT 2 SENSORS - RTE	Request to Exit button (normally open).	
IN1	Unknown direction RTE button (normally open).	Operating as an Unlock button with an unknown access direction or in the Access Granted by Security mode.

**Settings for the standard One Door, Pulse Control Mode configuration.**

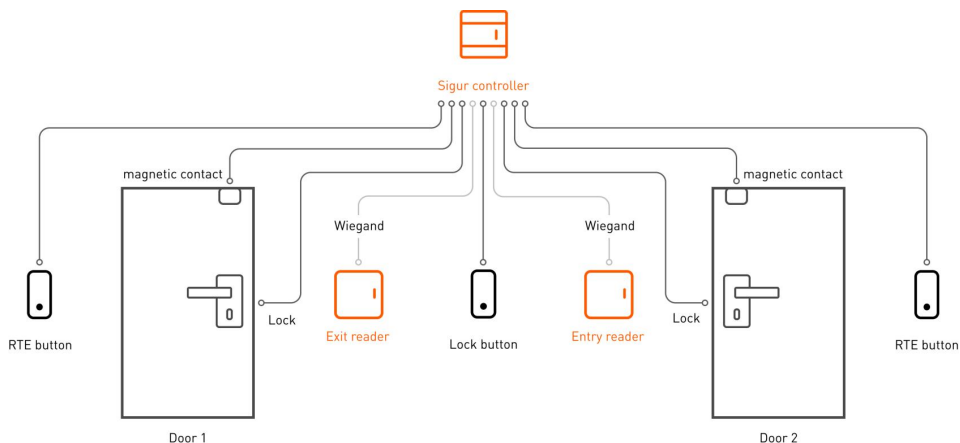
Parameter	Value	Description
Control:	Pulse.	The relays are switched when the pulse is received, but only for the time specified in the settings.

**7.3.5. Two Doors, Potential Control Mode configuration**

In this configuration, the controller can operate one or two doors fitted with locks in the potential control mode (the lock is locked when powered on). These usually include electromagnetic locks or electromechanical latches.

Below is the list of access control equipment for one door that can also be connected to the controller:

- lock;
- door open sensor (magnetic contact);
- entrance reader;
- exit reader;
- request to enter (RTE) button;
- request to exit (RTE) button;
- door lock button;
- security desk door release button.



Equipment connection option for the Two Doors configuration.

Either readers or RTE buttons can be located at the entrance and exit. Different readers and buttons for exit and entrance allow the system to identify the direction of access through the door.

A security desk door release button allows the security guard to open the door manually and the event will be recorded in the system as an unknown direction access granted from the security control panel.

The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

**Port mapping in the standard Two Doors, Potential Control Mode configuration.**

Port	Role	Description
<b>For Door 1:</b>		
PORT 1 READER	Port of the entrance reader.	
PORT 1 RELAY	Lock control line.	The relay is activated when the locking signal is received.
PORT 1 SENSORS - PASS	Open sensor (normally closed).	
PORT 1 SENSORS - RTE	Request to Exit button (normally open).	

Port	Role	Description
<b>For Door 2:</b>		
PORT 2 READER	Port of the entrance reader.	
PORT 2 RELAY	Lock control line.	The relay is activated when the locking signal is received.
PORT 2 SENSORS - PASS	Open sensor (normally closed).	
PORT 2 SENSORS - RTE	Request to Exit button (normally open).	
<b>Common</b>		
IN1	Lock button (normally open).	One Lock button for both access points.

**Settings for the standard Two Doors, Potential Control Mode configuration.**

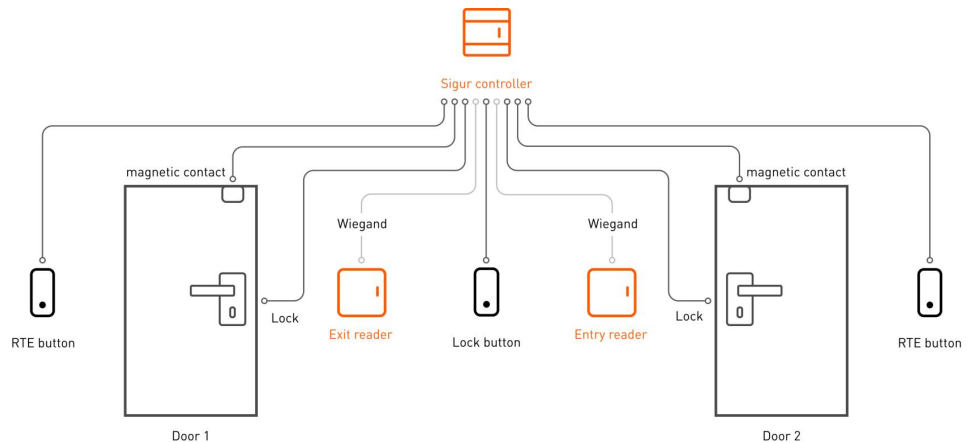
Parameter	Value	Description
Control:	Potential.	The relays stay switched while waiting for an access event.

**7.3.6. Two Doors, Pulse Control Mode configuration**

In this configuration, the controller can operate one or two doors fitted with locks in the pulse control mode. These usually include electromechanical locks, but not latches.

Below is the list of access control equipment for one door that can also be connected to the controller:

- lock;
- door open sensor (magnetic contact);
- entrance reader;
- exit reader;
- request to enter (RTE) button;
- request to exit (RTE) button;
- door lock button;
- security desk door release button.



Equipment connection option for the Two Doors configuration.

Either readers or RTE buttons can be located at the entrance and exit. Different readers and buttons for exit and entrance allow the system to identify the direction of access through the door.

A security desk door release button allows the security guard to open the door manually and the event will be recorded in the system as an unknown direction access granted from the security control panel.

The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

**Port mapping in the standard Two Doors, Pulse Control Mode configuration.**

Port	Role	Description
<b>For Door 1:</b>		
PORT 1 READER	Port of the entrance reader.	
PORT 1 RELAY	Unlock control line.	The relay is activated when the unlocking signal is received.
PORT 1 SENSORS - PASS	Open sensor (normally closed).	

Port	Role	Description
PORT 1 SENSORS - RTE	Request to Exit button (normally open).	
<b>For Door 2:</b>		
PORT 2 READER	Port of the entrance reader.	
PORT 2 RELAY	Unlock control line.	The relay is activated when the unlocking signal is received.
PORT 2 SENSORS - PASS	Open sensor (normally closed).	
PORT 2 SENSORS - RTE	Request to Exit button (normally open).	
<b>Common:</b>		
IN1	Lock button (normally open).	One Lock button for both access points.

**Settings for the standard Two Doors, Pulse Control Mode configuration.**

Parameter	Value	Description
Control:	Pulse.	The relays are switched when the pulse is received, but only for the time specified in the settings.

**7.3.7. Turnstile, Potential Control Mode configuration**

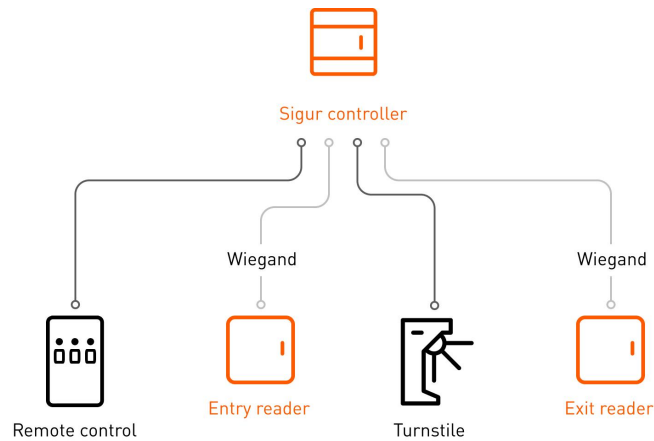
The controller can operate one turnstile in the potential control mode.

When the controller authorizes access, the entrance relay or the exit relay is activated. The default relay activation time pending an access event is 5 seconds and can be changed, where necessary. When the waiting time expires or the access event is completed, the relay returns to its inactive state and locks the turnstile.

The standard configuration uses a simplified sensor processing logic: the turnstile controller uses two lines to send pulses to notify about exits or entries (most turnstile models operate in the similar manner).

The following equipment can be connected to the controller:

- turnstile;
- remote control;
- entrance reader;
- exit reader.



Connection option for the Turnstile, Potential Control Mode configuration.

The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

**Port mapping in the standard Turnstile, Potential Control Mode configuration.**

Port	Role	Description
PORT 1 READER	Port of the entrance reader.	
PORT 2 READER	Port of the exit reader.	
PORT 1 RELAY	Unlock for Entry control line.	Unlock for Entry line.
PORT 2 RELAY	Unlock for Exit control line.	Unlock for Exit line.

Port	Role	Description
OUT1	Unlocked Mode indication line.	Unlocked (Free Access) line. It is activated in case of fire alarm or if the turnstile is unlocked in the software. It is used for turnstile models with a dedicated input used to send a signal to fold the bars.
PORT 1 SENSORS - PASS	Entrance control sensor line (normally closed).	Entrance control sensor line.
PORT 2 SENSORS - PASS	Exit control sensor line (normally closed).	Exit control sensor line.
PORT 1 SENSORS - RTE	Entry button on the remote control (normally open).	
PORT 2 SENSORS - RTE	Exit button on the remote control (normally open).	
IN1	Stop button on the remote control (normally open).	

**Settings for the standard Turnstile, Potential Control Mode configuration.**

Parameter	Value	Description
Control:	Potential.	The relays stay switched while waiting for an access event.
Turnstile sensor type:	Simplified interface.	The turnstile uses two lines to send pulses to notify about exits or entries.

### 7.3.8. Turnstile, Pulse Control Mode configuration

The controller can operate one turnstile in the pulse control mode.

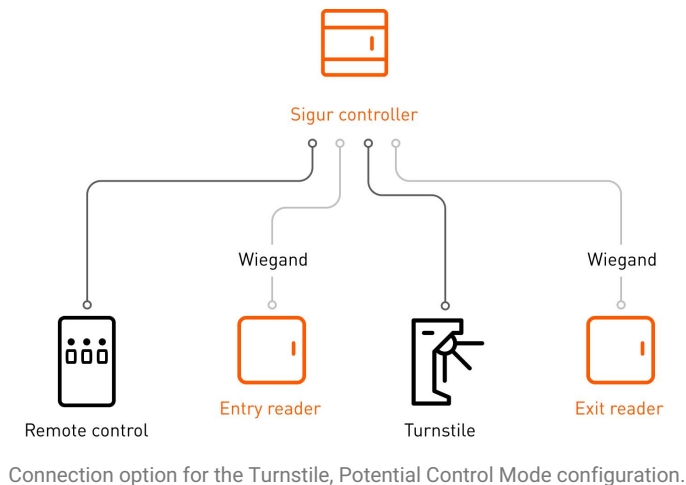
When the controller authorizes access, the entry or exit line is shortly activated. When the waiting time expires or the access event is completed, the lock line is activated to lock the turnstile.

By default, the relay activation pulse duration in the pulse control mode is 200msec and can be configured as necessary.

The standard configuration uses a simplified sensor processing logic: the turnstile controller uses two lines to send pulses to notify about exits or entries (most turnstile models operate in the similar manner).

The following equipment can be connected to the controller:

- turnstile;
- remote control;
- entrance reader;
- exit reader.



The detailed connection considerations are described in the respective sections of this document.

Where necessary, standard configurations can be modified on the **Access Points** tab in the **Client** software.

#### Port mapping in the standard Turnstile, Pulse Control Mode configuration.

Port	Role	Description
PORT 1 READER	Port of the entrance reader.	

Port	Role	Description
PORT 2 READER	Port of the exit reader.	
PORT 1 RELAY	Unlock for Entry control line.	Unlock for Entry line.
PORT 2 RELAY	Unlock for Exit control line.	Unlock for Exit line.
OUT1	Lock control line.	Lock line (Stop).
PORT 1 SENSORS - PASS	Entrance control sensor line (normally closed).	Entrance control sensor line.
PORT 2 SENSORS - PASS	Exit control sensor line (normally closed).	Exit control sensor line.
PORT 1 SENSORS - RTE	Entry button on the remote control (normally open).	
PORT 2 SENSORS - RTE	Exit button on the remote control (normally open).	
IN1	Stop button on the remote control (normally open).	

**Settings for the standard Turnstile, Pulse Control Mode configuration.**

Parameter	Value	Description
Control:	Pulse.	The relays are switched when the pulse is received, but only for the time specified in the settings.
Turnstile sensor type:	Simplified interface.	The turnstile uses two lines to send pulses to notify about exits or entries.

## 7.4. Configurable controller ports

Most ports on Sigur controllers (PASS, RTE, IN1, TAMPER, PWR STATUS) can be controlled by dry contacts or open collector outputs. Since these ports have integrated 3.3V pull-up resistors, it is not recommended to use 5V logic levels to control the ports.

The EMC UNLOCK port has a different arrangement, is galvanically isolated from the controller circuit and is controlled by applying voltage in the range of 5...24V to the F- and F+ terminals.

The controller has the following outputs:

- PORT1 RELAY and PORT2 RELAY (dry contact);
- general output OUT1 (open collector);
- reader indication control outputs LEDR, LEDG and BEEP (PORT1 READER and PORT2 READER) (open collector);
- loudspeaker on the controller board.

Ports can be mapped and inputs and outputs enabled in the controller settings window accessible from the **Access Points** tab. To do this, select the access point you want to configure and press the **Settings** button.

When you have completed the setup or configuration of ports, press **OK** to save and apply the changes or **Cancel / Discard** to discard the changes.

If the OK button is pressed, you will shortly see the **Writing the configurations to the controller memory** message. If successful, the window will automatically close.

## 8. Connection of readers

### 8.1. Connection of readers, general considerations

The controller supports up to two readers via the standard output interface such as Wiegand and Clock & Data (Omron 5bit, Magstripe Track II) or up to 4 readers via OSDP.

Wiegand readers are connected to the matching ports designated on the circuit board as PORT1 READER and PORT2 READER.

OSDP readers are connected to the RS485 port (A, B and COM).

The purpose and the number of connected readers are described in the relevant sections on specific configurations of the equipment connected to the controller.



When readers are powered on from the controller ports, the max. current consumption on each of the ports must not exceed 200mA. Otherwise, the integrated protection mechanisms of the controller will be activated and power off the readers. If readers with higher current consumption requirements are used, the positive terminals of the readers must be connected directly to the power supply unit terminals. The common wires of the reader and the controller must be connected together.



**DO NOT** use the GND terminals on the controller to connect any equipment with an external power supply source. This may result in the controller failure.

The GND terminals are connected to the negative terminal of the controller via a common-mode choke. The choke current is calculated based on the max. current achievable on the ports of the controller.

Any extra load between the positive terminal of the controller and any of the GND terminals can result in the controller failure. The GND terminals can be used only together with other ports of the controller (PWR, PASS, RTE, etc.).

### 8.2. General considerations for connecting your readers

- We recommend to locate your readers taking into consideration convenience of the authentication process. The optimal recommended height is between 1.1m and 1.4m from the ground level.

- Wiegand readers are connected to the controller using a non-twisted pair cable (such as 8x0.5 indoor signal cable). If a twisted pair cable is used, wires from different pairs must be used to connect the DATA lines. The second wire from each pair can be used as a power supply line (i.e., one pair = DATA0 and GND, the second pair = DATA1 and "+" terminal).
- Do not place readers close to sources of broad-range electromagnetic interference. These might include motors, generators, DC-to-AC converters, uninterruptible power supply units, AC relays, light dimmers, monitors, etc.
- Make sure to place the cable of the reader at least 0.5m away from other cables, including AC power cables, computer cables, telephone cables or power cables of electromechanical locks.
- To avoid interference, two readers with the standard reading distance (up to 15cm) must be placed at least 0.5m apart. For long-range readers, the distance shall increase proportionately and for shorter-range readers it can be decreased.

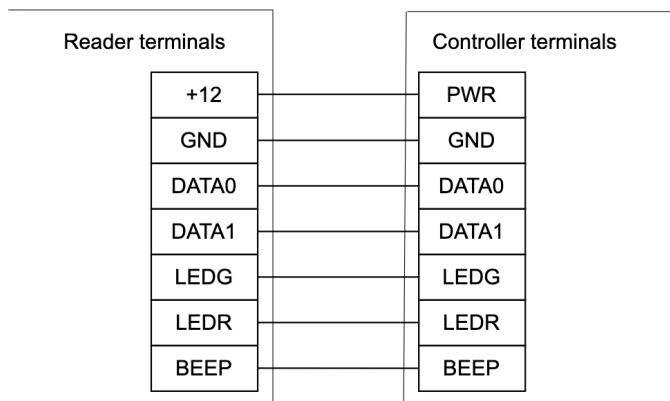
**Critical considerations on reader usage:**

- Many readers support multiple output interface standards. To switch between the output interfaces, please see the manual for your reader. Generally, the interfaces are switched by connecting the reader lines onto each other, cutting the connecting loops or using the DIP switch on the board of the reader.
- If readers with the standard Wiegand interface are used, you can connect several readers in parallel to a single input of the controller. This method can be used if you do not have a hybrid reader that provides all the required functionality, such as a fingerprint scanner and a keypad. However, the interoperability of this method heavily relies on the circuit design of the readers and not always can be achieved.

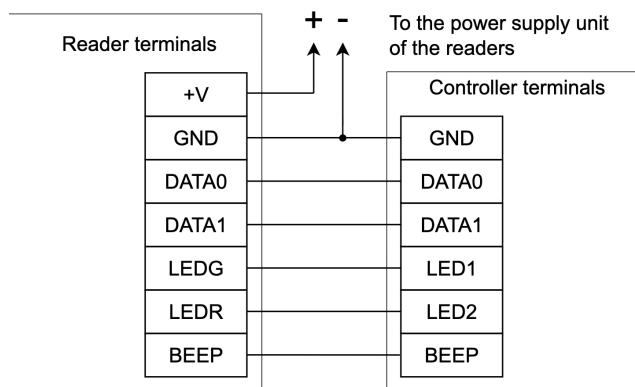
### 8.3. Wiegand readers

Electrical properties of the standard Wiegand interface ensure guaranteed reader connection distance of up to 100m, which will be enough for most applications. If the proper cables are used and the wiring considerations are observed, the connection distance can be extended to up to 150m (see the [Recommended Cable Choices Appendix](#)).

To connect a reader via Wiegand, the PWR (powers up the reader from the controller), GND, DATA0, DATA1 and, where necessary, LEDR, LEDG and BEEP ports are used.



Connection option for the reader with the supply voltage equal to the supply voltage of the controller.

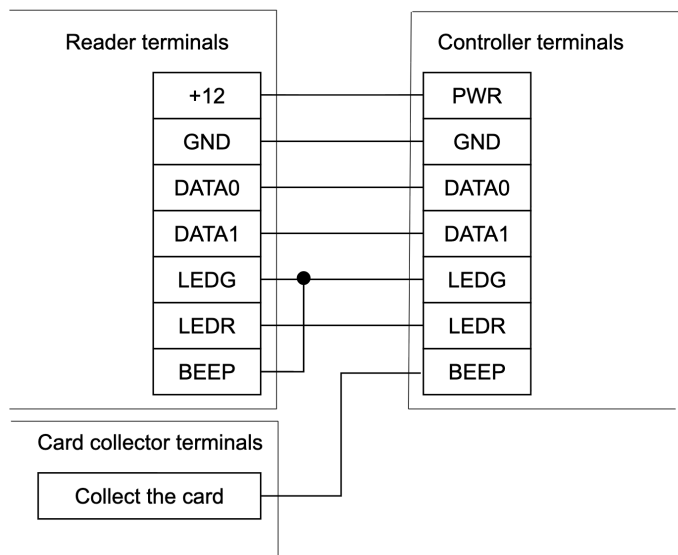


Connection option for readers with the supply voltage NOT equal to the supply voltage of the controller or for readers with the current consumption exceeding 200mA.

**Description of the terminals used in the diagrams above.**

PWR	Positive power supply terminal.
GND	Common wire.
DATA0	Wiegand data lines.
DATA1	
LEDG	Reader green LED control port.
LEDR	Reader red LED control port.
BEEP	Reader loudspeaker control port.

- The LEDG, LEDR and BEEP indication lines can be left not connected if the reader is configured for internal indication control.
- Any of the LEDG, LEDR and BEEP indication lines can be mapped to perform other controller roles. For instance, the BEEP line on the controller can be used to control the connected card collector. The BEEP line and the LEDG line of the reader can be connected together for synchronous indication.



Connection option for a reader with one indication control line mapped to perform a different role.

## 8.4. OSDP readers

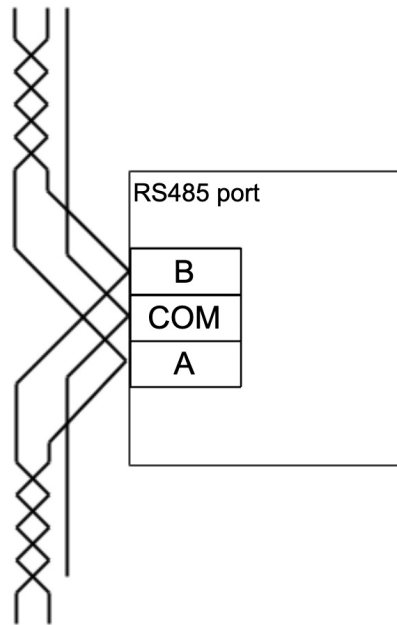
The controllers are compatible with any readers that support OSDP v.2.2 and above.

OSDP readers are connected to the controller via the RS485 interface. If more than one reader is connected to the line, you should use the bus topology, i.e. all the devices connected to this cable should be connected in line, one after the other.

If all the installation considerations are followed, the electrical properties of the RS485 interface make it possible to build sections of communication lines up to 1,200m long. For the detailed cable considerations for communication lines, please go to the [Recommended Cable Choices](#) section of this document.

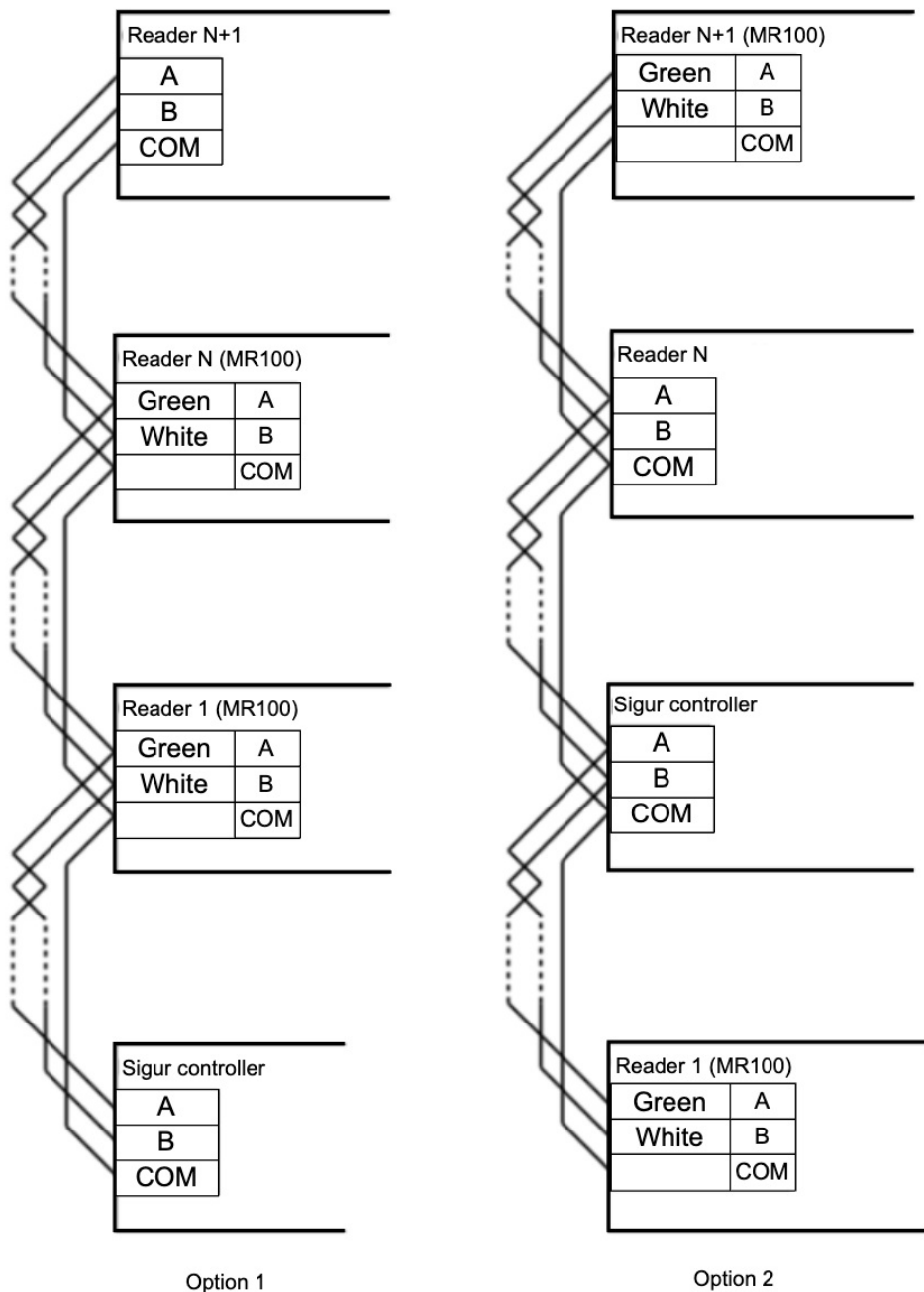
Where necessary (if longer communication lines or higher communication speeds are required), you can enable line termination at your endpoints. By default, line termination is disabled in our controllers and can be enabled in the software. To enable line termination, go to the **General** tab in the controller settings and uncheck the **Show basic settings only** box and check the **Enable RS485 termination** box. To find out more about enabling line termination on connected readers, please read the manual provided by the manufacturer of your reader.

The communication line is connected to the A port (the first wire of the twisted pair), B port (the second wire of the twisted pair) and COM port (common). Any free wire of the cable, except for the screen, can be used as the COM wire.




Wiring configuration for non-endpoint readers via OSDP.

When connecting your devices, you must match A and B wires of the communication line on the controller and on all the readers connected to the same line. All A ports must be connected by the same wire in the twisted pair and all B ports must be connected by the second wire in the same twisted pair.



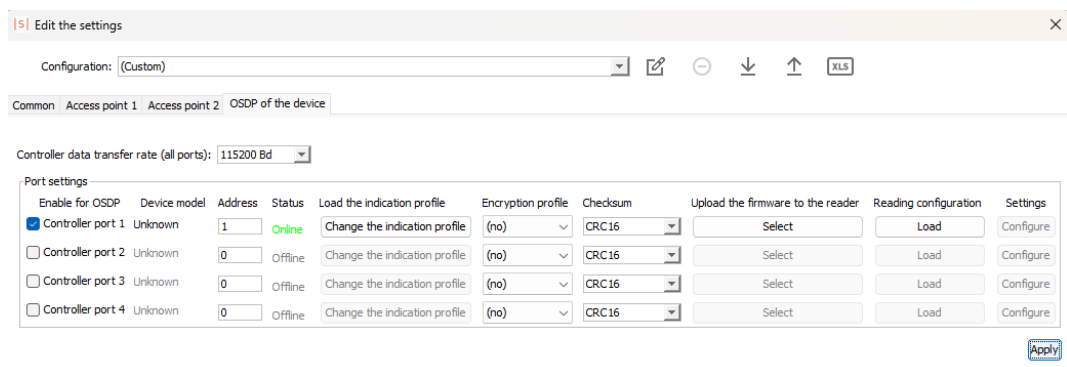
Connection options for several readers via OSDP.

 The A and B wires must be a twisted pair. You must never use wires from different pairs of the cable!



If these communication line requirements are not followed, the manufacturer does not guarantee stable operation of the device.

If your readers are connected via OSDP, you must manually specify the network parameters for each of the readers in the controller settings. To do this, select an access point on the **Access Points** tab and press the **Settings** button. In the popup window, select the **OSDP Devices** tab. There you can set the communication speed between the controller and the connected readers and configure the connection parameters for your readers and logical ports of the controller.



Configuration window for OSDP devices.

In the **Port settings** table, you can configure your controller’s logical ports. In the **Enable for OSDP** column, you can select which logical ports of your controller will be OSDP-enabled.



When a port is enabled on the **OSDP Devices** tab, the Wiegand port of the controller with the same number is automatically disabled.

The following parameters can be configured for every logical port of the controller on the **OSDP Devices** tab:

- Device model: model of the Sigur reader connected to the controller.
- Address: The address of the device in the line in the range of 1...127. The address is set in the reader settings (see the reader manual provided by the manufacturer).
- Status: The connection status of the reader.

- **Encryption profile:** Allows users to select an encryption profile for the traffic between the controller and the reader. The profiles can be created, configured and deleted in the Client software. To do this, go to **File > Settings > OSDP encryption profiles**. Every profile must have a name and an AES encryption key (can be entered manually or auto-generated). If multiple readers are connected to one controller, we recommend selecting a different encryption profile for each connected reader. To find out more about this functionality, please read the [Encryption of data sent via OSDP](#) section of this document.
- **Checksum:** The way the checksum is calculated depends on the reader settings. If Sigur readers are used, select the default value, which is "CRC16".



If Parsec OSDP readers are used, select "SINGLEBYTE" instead of "CRC16" for the Checksum parameter from the dropdown menu.

- **Load the indication profile:** Here you can select an indication profile to be used by the controller to control the indication of your OSDP readers. For a detailed description of the indication control functionality via OSDP, please see [this section](#).
- **Upload the firmware to the reader:** Here you can update the firmware of your Sigur readers via SSDP.
- **Reading configuration:** Here you can update the reading configuration of your Sigur readers via SSDP. For a detailed description of this functionality, please see the [Sigur ACS Quick Guide](#).

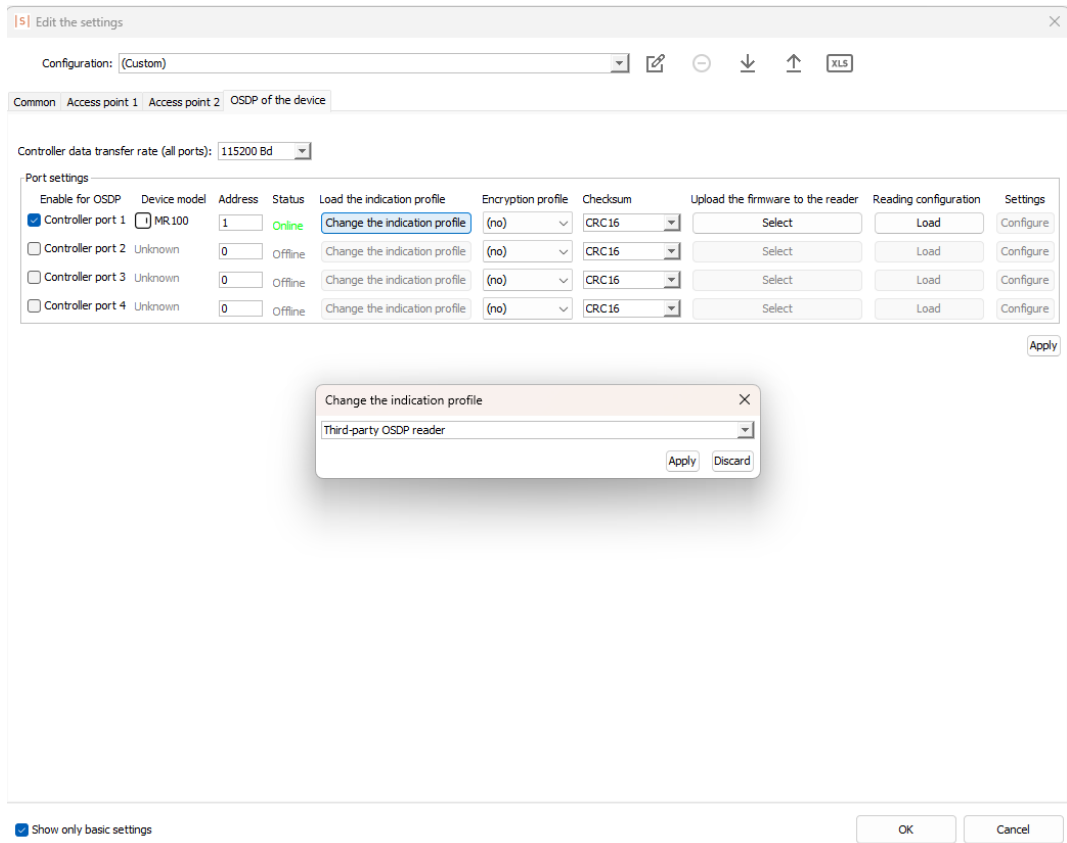
### 8.4.1. Indication of readers connected via OSDP

Indication of readers connected via OSDP is controlled via the A and B lines as follows: when a specific event is detected, the controller sends a control signal to the reader to activate its LED and sound indication. Upon receiving the signal, the reader activates the respective indication.

Sound and LED indication for different events that trigger the controller to send a control signal can be configured in the Client software by selecting a respective indication profile. To do this, follow the steps below:

- Go to the **Access Points** tab and in the settings menu of the respective access point go to the **OSDP Devices** tab;

- Select the respective reader port and press the **Change the indication profile** button, select the standard indication profile **Third-party OSDP reader** or a custom indication profile and press **Apply**. Read on to find out how to create a custom profile.

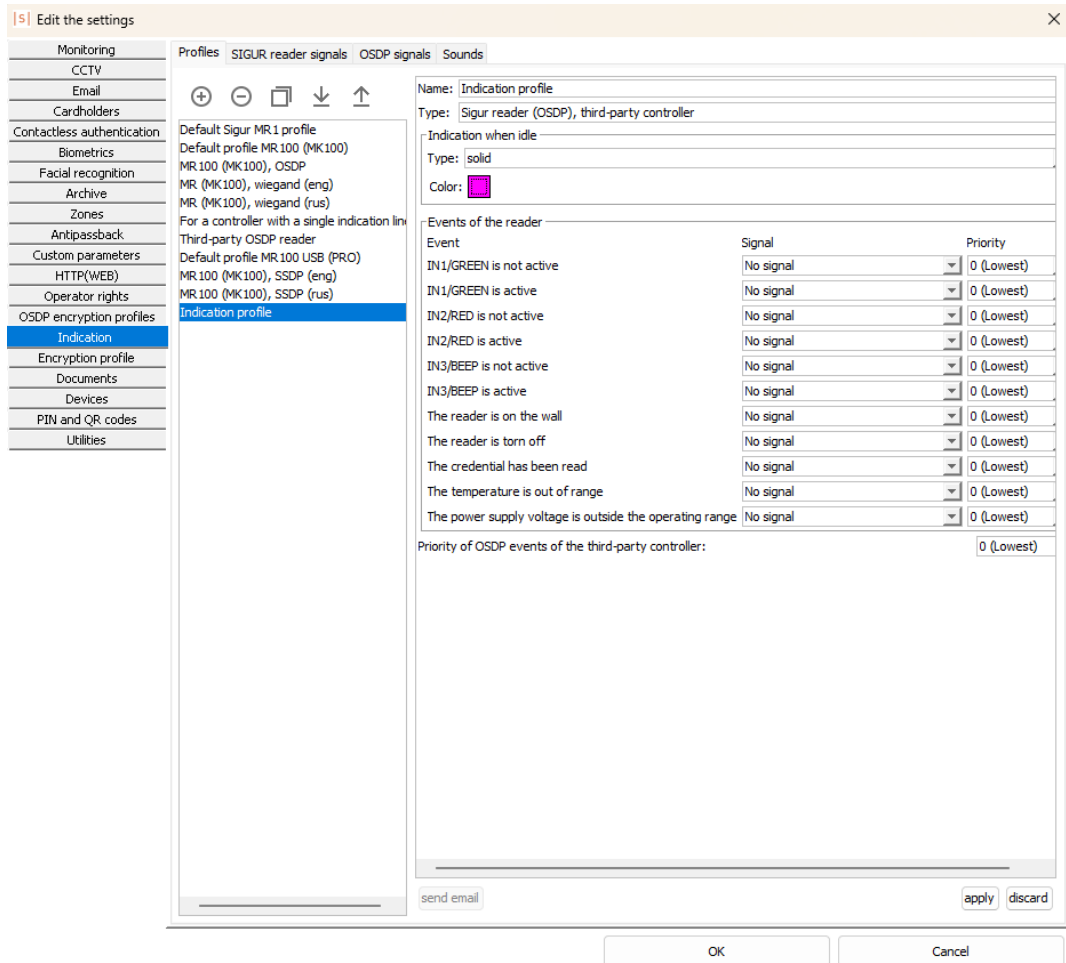


Reader indication profile selection menu.

### How to create a custom indication profile.

You can create custom indication profiles in the **Client** software by going to **File > Settings > Indication > Profiles**.

To create a new indication profile, click the "+" button or copy another profile by clicking the respective button. The user can change the profile name in the **Name** field. To apply the changes, click **Apply**.



Creating a new indication profile for a third-party reader.

To create an indication profile for a third-party reader, select the Third-Party Reader, Sigur Controller option.

Settings available in indication profiles:


1. LED indication of the reader in standby mode in the absence of any events. The **Indication type** parameter can have the values as follows:
  - **Solid.** The LED color does not change unless an event occurs.
  - **Blinking.** The reader switches between its LED colors: first, Color 1 lights up for the set period of time, then Color 2 lights up for the period indicated in the settings.
2. ▪ **Failed to arm the zone.** the attempt to arm the zone has failed for any reason. Signals of the reader in response to various events generated by the controller.

Signals to the following events generated by the controller can be configured in an indication profile:

- **Pending access completion.** When access has been granted to a cardholder, the controller is waiting for the cardholder to complete the access event.
- **Break-in.** Unauthorized access through the access point has been detected.
- **Door held open.** The Door Open sensor has not returned to its normal state and timed out (the waiting time is set in the access point settings in the **Delay before the Door Held Open signal** parameter).
- **Security alarm.** The security line of the Sigur controller has reported the Alarm event. The reader will respond to the incoming Alarm signal only from the alarm line connected to the access point belonging to this reader.
- **Pending operator permission.** The authenticated cardholder is subject to the **Request operator permission to access** rule and the system is waiting for the operator's intervention.
- **Pending the PIN code.** The authenticated cardholder is subject to the **Additionally request the PIN code** rule and the controller is waiting for the PIN code from the connected keypad.
- **Pending second card.** The authenticated cardholder is subject to the **Only if accompanied** or **Two persons** rule and the system is waiting for the supervisor or the other cardholder (for the **Two persons** rule) to authenticate.
- **Access granted.** The authenticated cardholder was granted access.
- **Access denied.** The authenticated cardholder was denied access.
- **Pending alcohol testing.** The authenticated cardholder is subject to the **Alcohol testing** rule and the system is waiting for the alcohol test results .
- **Zone armed.** The controller's alarm loop has generated an **Armed** event.
- **Zone is armed.** The indication remains active for as long as the zone status is **Armed**. It is triggered after the **Zone armed** event and remains active until the **Zone disarmed** event occurs.
- **Zone is arming.** Activated after the arming process starts and remains active during the time when the system ignores short-term sensor

triggers in the zone.

- **Waiting for card confirmation.** The indication is activated when an additional credential must be presented to confirm actions such as arming the zone or changing the access point mode. Applicable when the action requires **PIN + card**.



Reader responses to access point mode changes will be available in future versions of Sigur controller firmware and the main software.

3. **Priority.** This parameter controls whether the current indication is overridden by another indication if a new event occurs. Two types of responses are available:

1 – The duration of the signal depends on the duration of the event (changing the color, continuous blinking);

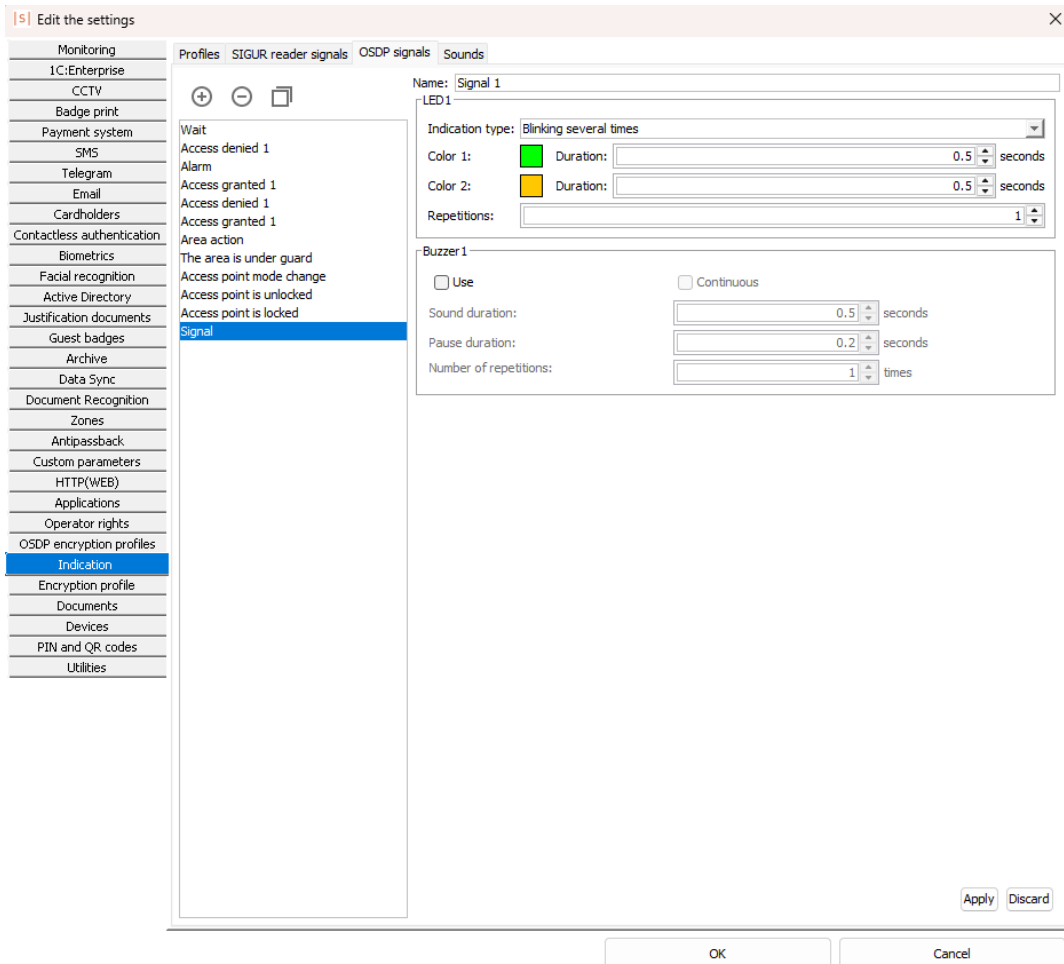
2 – The signal has a fixed duration (blinking once, blinking several times).

**Activation of signaling depending on the priority and type.**

Signal type		Priority of the current signal	Result. The second signal:
Current	Second		
1	1	Lower or equal	Overrides the current signal
		Higher	Does not override the current signal
1	2	Any	Overrides the current signal
2	1	Lower or equal	Overrides the current signal
		Higher	Does not override the current signal
2	2	Any	Overrides the current signal

### Creating reader reactions on the OSDP Signals tab.

To add a new reader signal reaction to an event, go to **File > Settings > Indications > OSDP signals** tab. To create a new signal reaction, click the "+" button or copy another signal reaction by clicking the respective button. You can rename the reaction in the **Name** field. To apply the changes, click **Apply**.



Creating an OSDP reader signal reaction.

A signal reaction consists of the following elements:

- **Indication type.** The type of LED indication for an event. LED indication types include:
  - **No reaction.** No LED indication for events. The LED light remains unchanged.
  - **Blink once.** The reader’s LED changes to Color 1 for a set period of time.
  - **Blink several times.** The reader changes its LED colors: first, Color 1 lights up for the set period of time, then Color 2 lights up for the period indicated in the settings. The pattern repeats a set number of times.

- **Change color.** The reader's LED changes to Color 1.
- **Continuous blinking.** The reader continuously changes its LED colors: first, Color 1 lights up for the set period of time, then Color 2 lights up for the period indicated in the settings.
- **Buzzer.** Enables the integrated buzzer. When the integrated buzzer is used, the following buzzer parameters can be configured: the number of times it will buzz (the fixed duration of the signal) or continuous signal (the duration of the signal depends on the duration of the event). In both cases, the user can choose the interval between the beeps.

#### 8.4.2. Encryption of data transmitted over OSDP

When the reader is operated via the OSDP interface, to ensure the maximum security, you have an option to enable encryption of data transmitted between the reader and the controller.

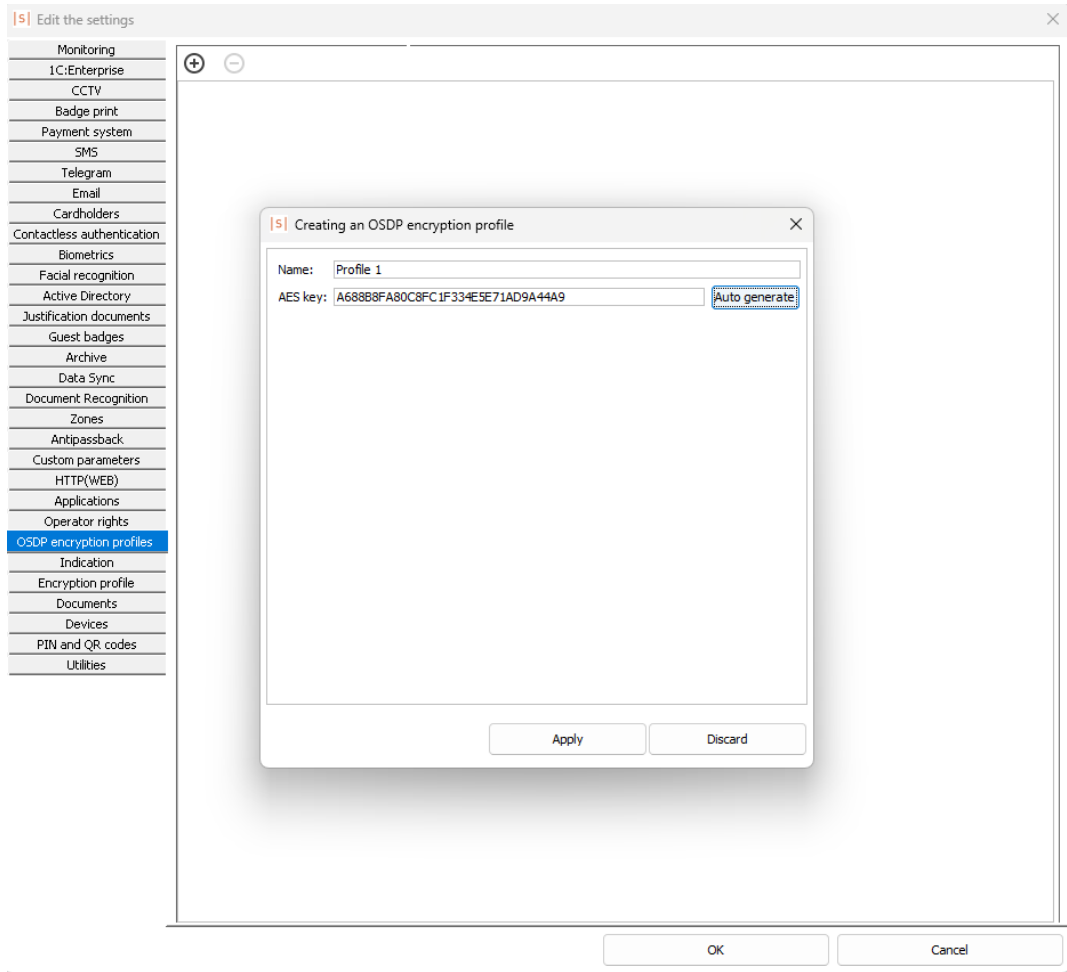
This can be done by following the steps below:

1. Create an OSDP encryption profile.
2. Apply the OSDP encryption profile.

##### Creating an encryption profile.

Encryption profiles can be created and managed in the **Client** software.

To create a new OSDP encryption profile, go to **File > Settings > OSDP encryption profiles**. There press the "+" button, choose a name for your encryption profile and type in or auto-generate the AES key by pressing **Auto generate**.



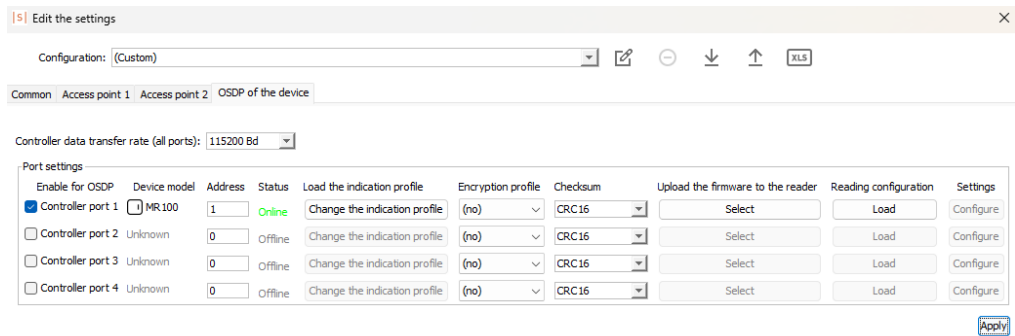
OSDP encryption profile editor.

When done, press **Apply** and the encryption profile will appear in the list.

**Applying the OSDP encryption profile.**

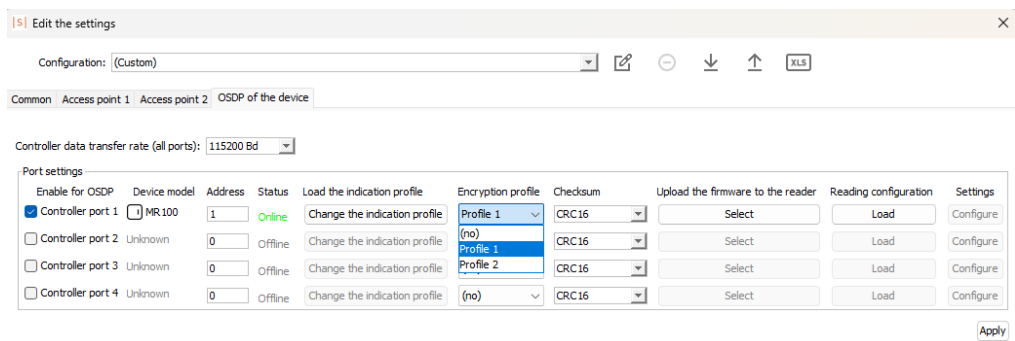
To upload an OSDP encryption profile to a reader, follow the steps below:

- Make sure the reader and the controller are online and connected. To do this, go to the **Access Points** tab in the **Client** software and select the respective access point belonging to the controller to which the reader is connected and press the **Settings** button. On the **OSDP Devices** tab, make sure that the reader is assigned to a port of the controller with the **Online** status.



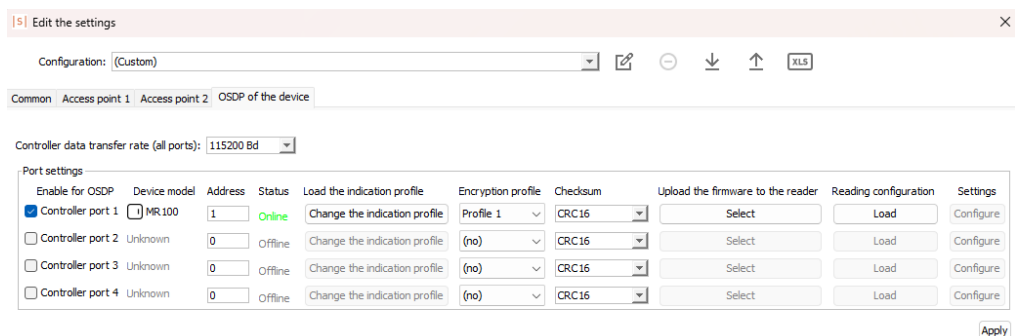
Checking the status of OSDP connection between the reader and the controller.

- Make sure that the reader is ready to connect securely. To do this, in **Sigur Config** Android app open section **Connection settings** and choose Security install mode option.
- In the access point settings menu on the **OSDP Devices** tab of the Client software, select the previously created encryption profile for the respective port of the controller and press **Apply** .



Applying the OSDP encryption profile.

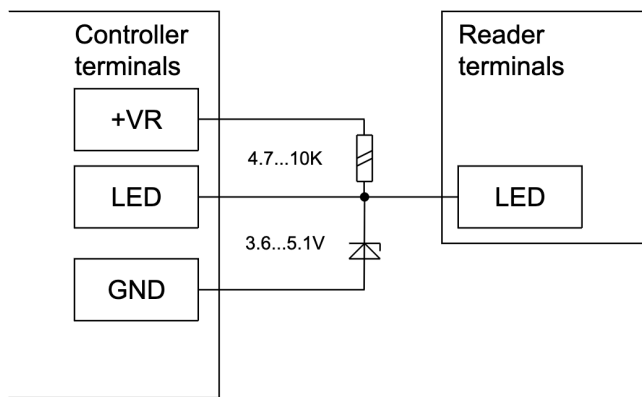
- Next, make sure that the connection status after applying the OSDP encryption profile is shown as **Online** .



Checking the status of OSDP connection between the reader and the controller after applying the OSDP encryption profile.

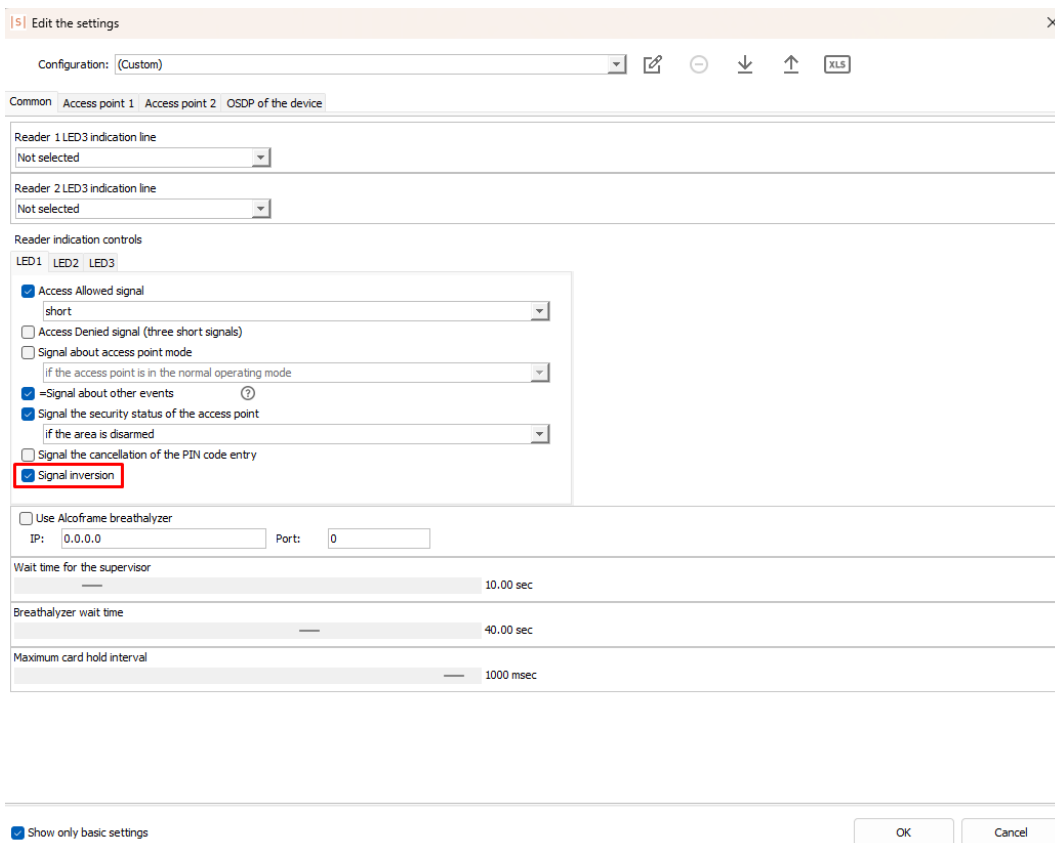
## 8.5. Connection of indication controlled by 5V input

Indication on some models of readers is controlled by applying 5V to their LED terminals. If this is the case, you can rely on the diagram below:



Connection of a reader indication control line operated by 5V input.

Additionally, in the controller settings (in the **Client** software, go to the **Access Points** tab, select the respective access point and press **Settings**) on the **General** tab, find the **Reader indication controls** section and enable the **Signal inversion** option for the respective output.



LED1 controller output settings view.

## 8.6. Blacklisted readers

Some reader models available on the market do not comply with the specifications and standards and therefore do not work at all or work inconsistently and require extra efforts to set up.

Currently, incompatible readers include earlier-generation KODOS readers (high-value resistors in the output stage of these readers make it impossible to ensure normal logical levels on the controller terminals). We have also received a number of complaints about U-prox mini readers.

The readers that require extra efforts to set them up include Farpointe Data P-640 and RE-15 receivers because they provide incorrect checksums for Wiegand packages. To make these devices compatible, go to the controller settings and tick the **Do not check Wiegand checksum** box.

## 9. Connection of doors

Sigur controllers can operate access points of the Door type (the number of doors that can be connected to one controller depends on the model of your controller). Follow the steps below to connect your door to the controller:

- Connect the lock (electromagnetic, electromechanical, latch, etc.).
- Connect readers (the number and roles depend on the selected configuration).
- Connect door open sensors (magnetic contacts).
- Connect Hall effect sensors for electromagnetic locks.
- Connect a door unlock button (the number and roles depend on the selected configuration).
- Connect a door lock button.

### 9.1. Locks, general considerations

#### 9.1.1. Locks, general consideration

Locks are controlled by relays located on the controller board.

Each relay has a switching terminal block: COM (common), NC (normally closed) and NO (normally open).

The relays are assigned to particular locks of particular doors in the controller settings.

To ensure that Sigur controllers can operate a variety of lock models, two lock control modes are supported: potential and pulse control modes.

In the potential control mode, the relay is normally activated (the lock is locked) and, when the lock is unlocked, the relay is deactivated during this time. Electromagnetic locks and latches are operated in this mode.

In the pulse control mode, the relay is normally inactive and will shortly become activated to unlock or lock the lock. Electromechanical locks are operated in this mode.

#### 9.1.2. Electromagnetic locks and electromechanical latches

Sigur controllers can operate any types of electromagnetic locks and electromechanical latches.

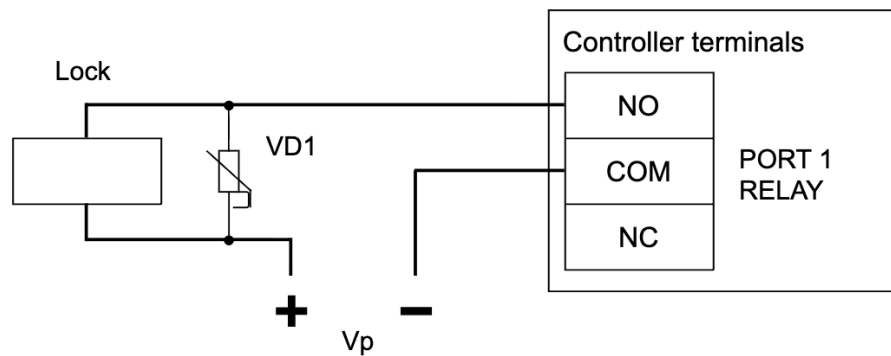
Generally, electromagnetic locks are locked when powered up.

Electromechanical latches can be both unlocked and locked when powered up.



It is expressly prohibited to use electromagnetic latches that unlock when powered up if they are not designed to withstand continuous power supply. When a door is unlocked from the software or due to fire alarm, the latch can stay powered up for quite a long period of time. Using latches that can withstand only short voltage pulses (such as FERMAX) will burn the coil of the latch leading to uncontrollable locking that may result in injuries and death!

To connect electromagnetic locks or electromechanical latches, select either the **One door, potential control mode** configuration or the **Two doors, potential control mode** configuration.



Connection option for an electromagnetic lock.

**Designations on the figures:**

VD1	Varistor.
Vp	Lock power supply (a single power supply unit can be used both for the lock and the controller).



It is expressly prohibited to use locks without connected varistors! When powered off, self-induced EMF in the coil of the lock can reach hundreds of volts. With no varistor connected, sparking will burn the relay terminals and damage the relay and if a single power supply unit is used for the locks and the controller, high-voltage interference on the power supply line can cause malfunctioning of the controller.

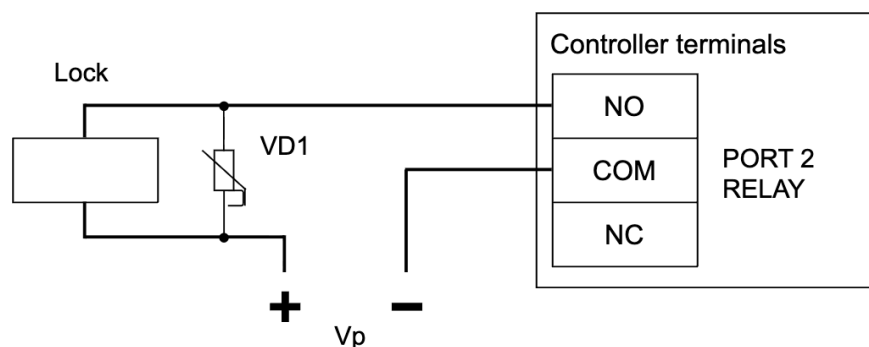
**Default relay port mapping for electromagnetic locks and latches.**

Port	Description
<b>One Door, Potential Control Mode standard configuration:</b>	
PORT1	COM: The negative power source terminal of the lock locked when powered up. NO: The negative terminal of the lock locked when powered up.
PORT2	COM: The negative power source terminal of the lock unlocked when powered up. NO: The negative terminal of the lock unlocked when powered up.
<b>Two Doors, Potential Control Mode standard configuration:</b>	
PORT1 PORT2	COM: The negative power source terminal of the lock locked when powered up. NO: The negative terminal of the lock locked when powered up.
PORT1 PORT2	COM: The negative power source terminal of the lock unlocked when powered up. NC: The negative terminal of the lock unlocked when powered up.

**9.1.3. Electromechanical locks**

The controller can operate any types of electromechanical locks.

To connect electromechanical locks, select either the One door, pulse control mode configuration or the Two doors, pulse control mode configuration.



Connection option for an electromechanical lock for the first door.

**Designations on the figures:**

VD1	Varistor
Vp	Lock power supply (a single power supply unit can be used both for the lock and the controller).



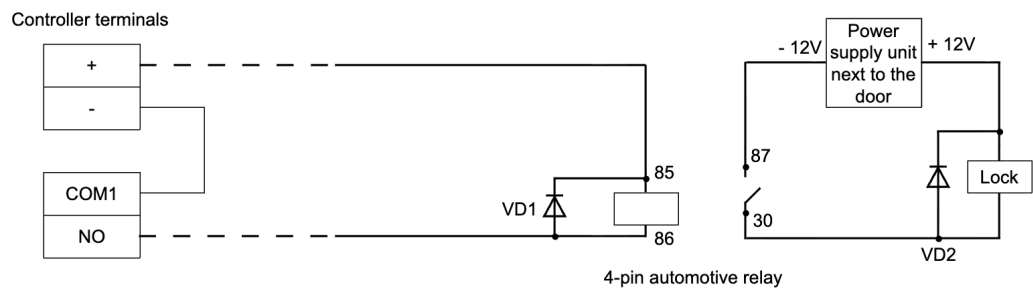
It is expressly prohibited to use locks without connected varistors! When powered off, self-induced EMF in the coil of the lock can reach hundreds of volts. With no varistor connected, sparking will burn the relay terminals and damage the relay and if a single power supply unit is used for the locks and the controller, high-voltage interference on the power supply line can cause malfunctioning of the controller.

Port	Description	
<b>One Door, Pulse Control Mode standard configuration:</b>		
PORT2 RELAY	COM: The negative power source terminal of the lock. NO: The negative terminal of the lock.	
<b>Two Doors, Pulse Control Mode standard configuration:</b>		
PORT1 RELAY	Door 1.	COM: The negative power source terminal of the lock. NO: The negative terminal of the lock.
PORT2 RELAY	Door 2.	COM: The negative power source terminal of the lock. NO: The negative terminal of the lock.

**9.1.4. Long distances between the controller and the lock**

If the controller is installed further away from the door (50–150 meters), you should factor in the voltage drop on the supply lines of the lock.

To ensure stable operation, please consider this connection option:



Connection of an electromagnetic lock for the first door far away from the controller.

An additional power supply unit and relay are installed next to the door. The controller is operated under low voltage (relay coil). In this configuration, the voltage drop along long connecting lines is minimal and does not affect relay operation that provides additional power supply directly to the lock.

### 9.1.5. Critical considerations on locks and latches



It is expressly prohibited to use locks without connected varistors! When powered off, self-induced EMF in the coil of the lock can reach hundreds of volts. With no varistor connected, sparking will burn the relay terminals and damage the relay and if a single power supply unit is used for the locks and the controller, high-voltage interference on the power supply line can cause malfunctioning of the controller.



When a lock is powered on from the power supply unit of the controller, it is not recommended to connect the power supply lines of the lock directly to the "+" and "-" terminals of the controller. The power supply lines of the controller and the locks must start directly on the terminals of the power supply unit. If you fail to comply with this requirement, it can result in voltage surges on the terminals of the controller when the lock is activated, because it has a high current demand, which can result in malfunctioning of the controller.



In combination with an electromagnetic lock, it is prohibited to use NC, COM terminals instead of NO, COM terminals.

When the controller is powered off, the locks must unlock. If you fail to comply with this requirement, it can result in uncontrollable locking of the locks in cases like when the power supply circuit of the controller is malfunctioning.



It is expressly prohibited to use electromagnetic latches that unlock when powered up if they are not designed to withstand continuous power supply! When a door is unlocked from the software or due to fire alarm, the latch can stay powered up for quite a long period of time.

Using latches that can withstand only short voltage pulses (such as FERMAX) will burn the coil of the latch leading to uncontrollable locking that may result in injuries and death!



DO NOT use the GND terminals on the controller to connect any equipment with an external power supply source. This may result in the controller failure.

The GND terminals are connected to the negative terminal of the controller via a common-mode choke. The choke current is calculated based on the max. current achievable on the ports of the controller.

Any extra load between the positive terminal of the controller and any of the GND terminals can result in the controller failure. The GND terminals can be used only together with other ports of the controller (PWR, PASS, RTE, etc.).

## 9.2. Door Open sensors (magnetic contacts)

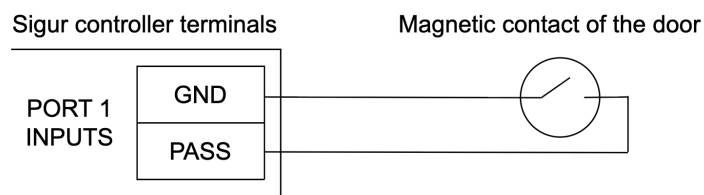
Door Open sensors are used to monitor authorized or unauthorized access through the door.

If the Door Open sensor is disabled:

- The controller will not be able to register break-ins and break-outs.
- The controller will not be able to register door propping (when the door was opened and is held open for a longer period of time than specified in the controller settings).

- The controller will not be able to unlock the door with an electromechanical lock after each access event when unlocked manually or for fire emergency reasons.
- In some cases, the zonal control functionality will not work properly (if a cardholder presented the card but did not complete the access event).
- The lock opened by the controller will be locked only by the timer and not immediately after the door is closed.

Generally, a normally closed (when the door is closed) magnetic contact (sealed magnetically operated reed switch) is used as the Door Open sensor.



Connection of a Door Open sensor.



If you do not have a Door Open sensor, do not use jumpers on the PASS and GND terminals, because in this case the controller will not register access events (as it will always see the door as closed).



Some electromagnetic locks have a Hall effect sensor. We expressly do not recommend to use this sensor as the Door Open sensor since it is intended for other purposes and cannot replace a magnetic contact. The Hall effect sensor is intended to monitor the lock state and identify any failures.

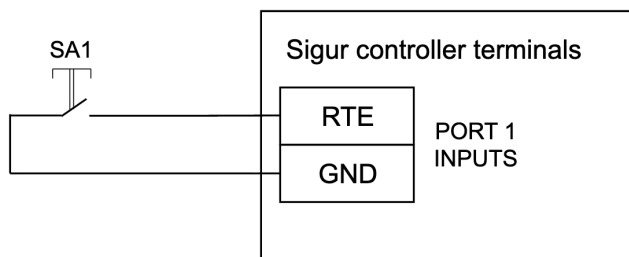
### 9.3. Hall effect sensor

The Hall effect sensor is integrated in some electromagnetic lock models and is intended to monitor the lock state and identify any failures.

If necessary, you can connect the Hall effect sensor to free inputs of your Sigur controller. In this case, you will need to select the Door: Hall effect sensor role for this port in the controller settings.

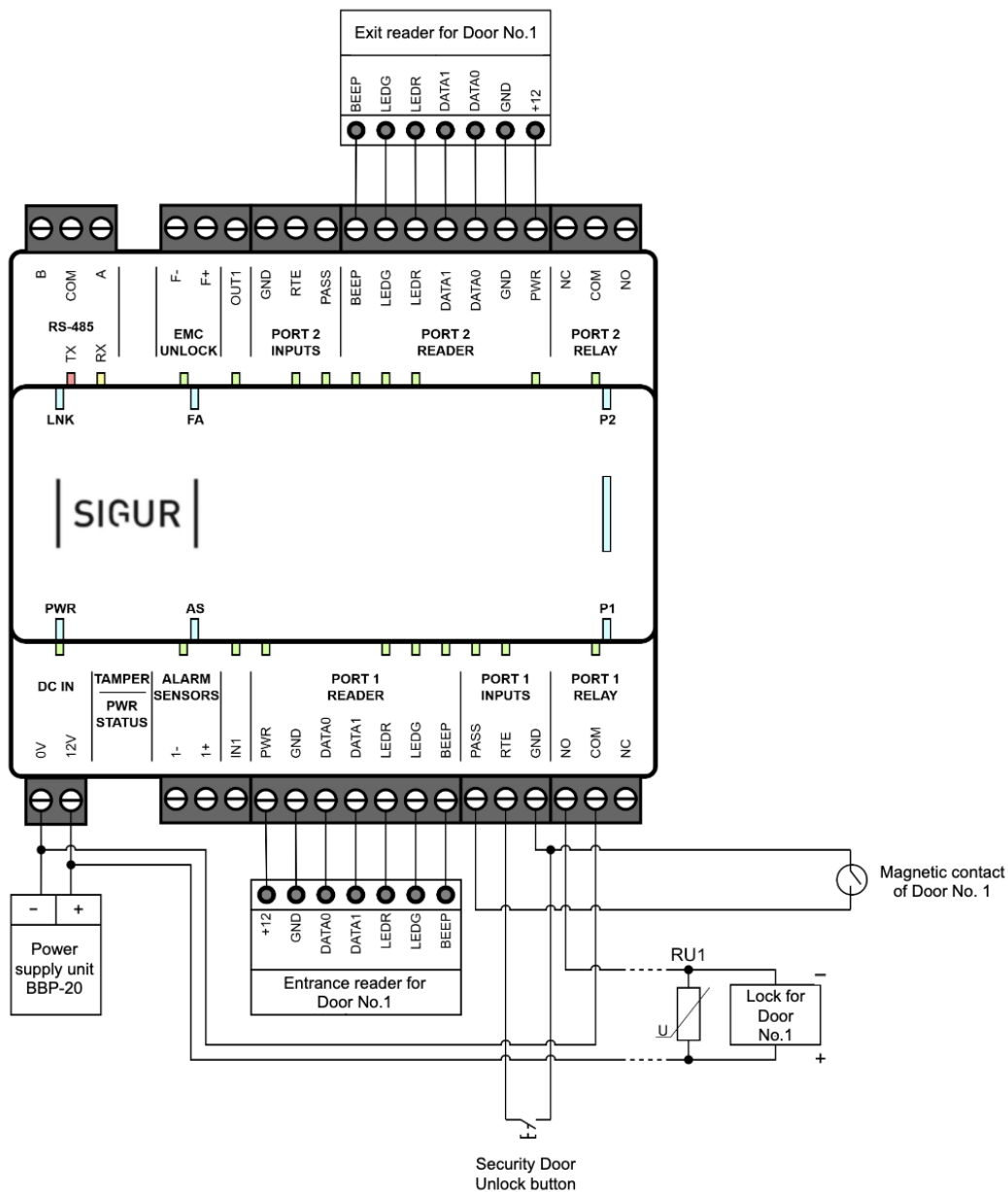
### 9.4. RTE buttons

RTE buttons are intended for unlocking the respective door unless the Door Lock button is pressed. General practice is to use normally open buttons.

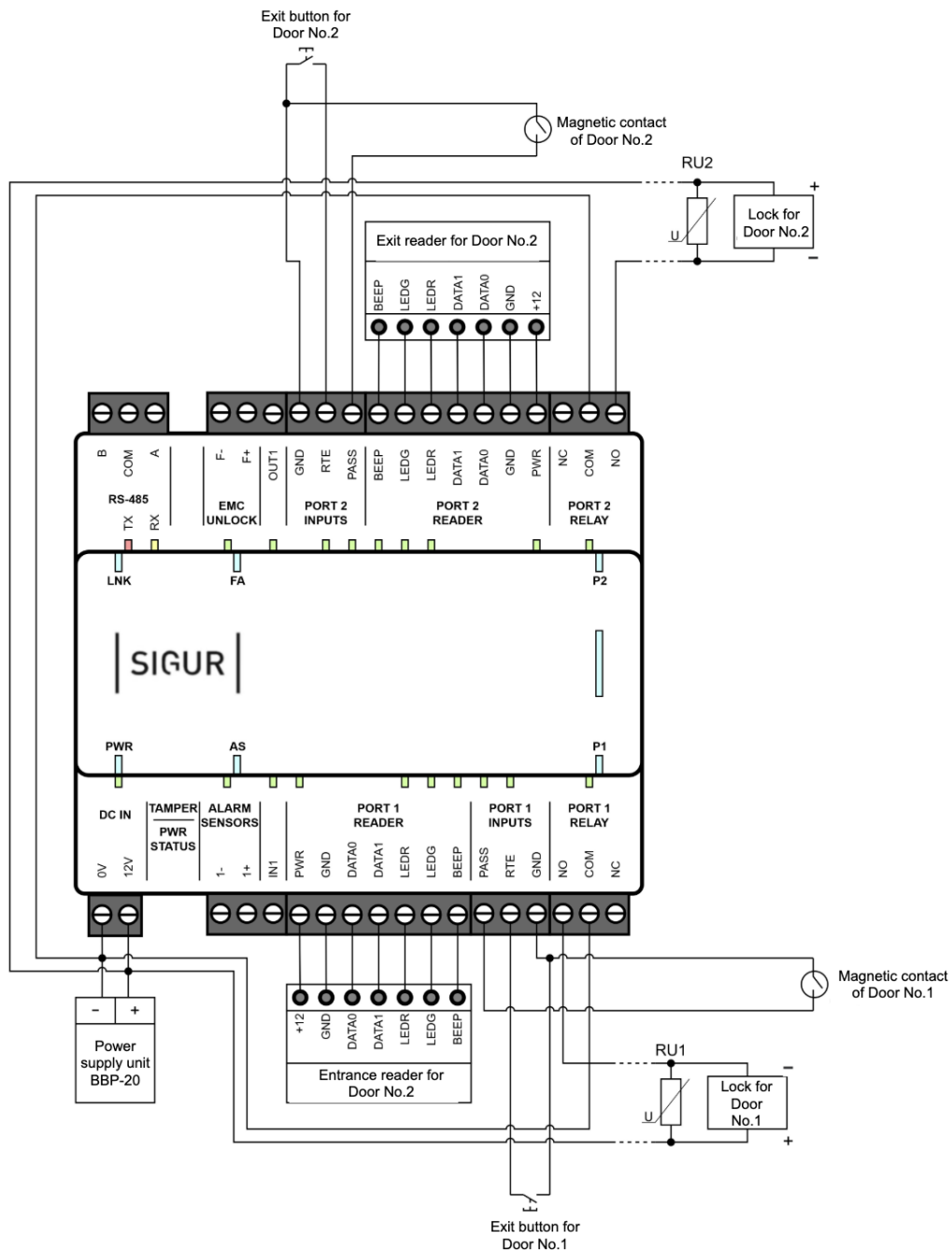


Connection option for an RTE button.

## 9.5. Connection options for doors



Connection option for one door.



Connection option for two doors.

## 10. Connection of intercoms

Sigur controllers support any types of intercoms regardless of the manufacturer or design.



Some IP intercoms are integrated with Sigur. The integrated models do not require use of or connection to the Sigur controller to operate access points. In this section, non-integrated models are discussed.

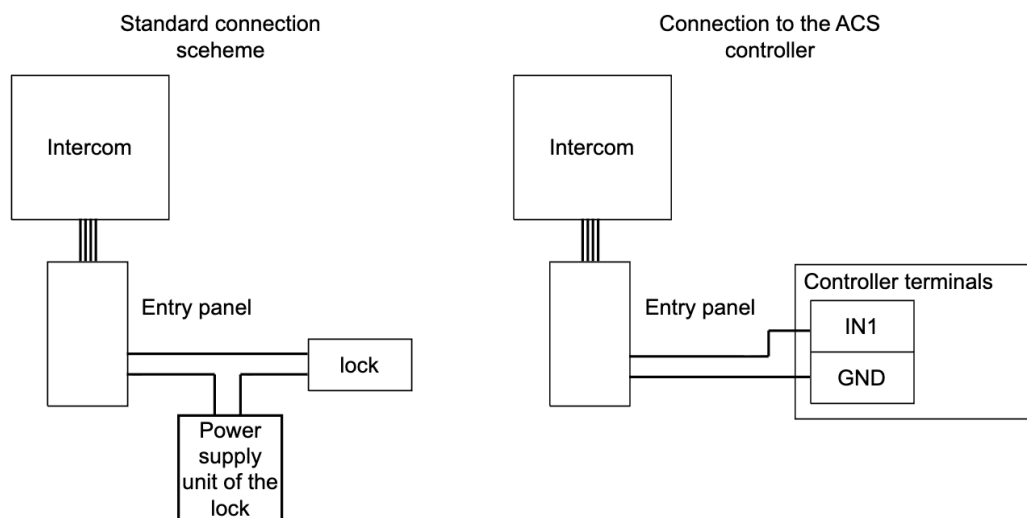
To connect an intercom, first you need to know the power switch type of the lock. Below are two common types.

The first type, when the entry panel controls the lock using an integrated relay, is the most common type. It includes such intercoms as Activision AVP-506, AVC-302, 304, 305, 308; Commax DRC-4xx, DVC-201C; Falcon eye FE-311; ERCON SV4L, SV4R, SV4T; Slinex ML-15; Kocom KC-MB30, KVM-301, etc.

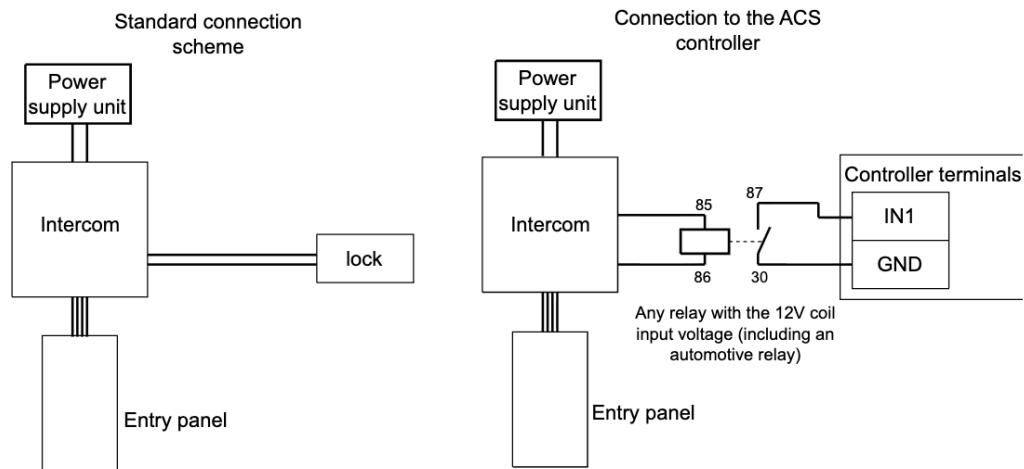
Sometimes, the other type is used. In this case, the circuit connecting the lock is not just closed or open, it is directly connected to the voltage source. It includes such intercoms as JSB-V05M.

These two types are easily distinguished based on the lock connection scheme recommended in the intercom or entry panel manual.

Please take into account that when an intercom is connected to the ACS controller, it will no longer control the lock directly, but it will send a command to the controller to open the door.



Connection option for a dry-contact (relay) intercom.



Connection option for an intercom with the direct power supply to the lock.

If the intercom is configured to operate an electromechanical lock, the terminals of the intercom relay are normally open and no additional settings are required.

If the intercom is configured to operate an electromagnetic lock (this is usually the case for intercoms in residential blocks such as Vizit, Metakom, Cyfral, etc.), the terminals of the intercom relay are normally closed and will require some basic configuration. In the **Client** software, go to the **Access Points** tab and select the respective controller, press **Settings** and add the following options for the respective access points. For example:

- Select **Unknown Direction RTE button** for the role and **INPUTS - IN1, normally closed for the terminal**.

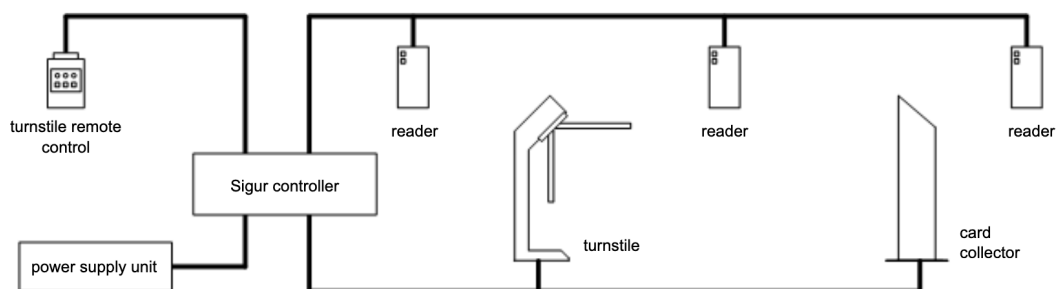
Some intercom models have an integrated card reader with a Wiegand output. If this is the case, it can be connected to the same ports of the controller as any regular Wiegand readers.

## 11. Connection of card collectors

Card collectors are designed to collect cards when a visitor leaves the building or site.



A card collector is connected to the same controller as the access point (turnstile, door or arm barrier). No additional controllers are required!



Connection option for a turnstile with a card collector.

The following lines can be used depending on the card collector model:

- Card collection control line;
- Card return control line;
- Card collection confirmation line.

A reader for guest badges is installed inside a card collector. This reader can be used to authenticate employees as well, but only if this feature is designed into the card collector (the cardholder should be able to take their card back after authentication). In this case, it can replace the primary exit reader connected to the access point.



Please review the recommended connection diagrams for the model of your card collector and the turnstile / arm barrier in question before connecting your card collector to your controller and check whether there are enough free inputs and outputs on the controller to connect the necessary control lines.

## 12. Connection of breathalyzers

A breathalyzer ensures that the selected group of cardholders will be able to access the premises only after two-factor authentication: the presence of the primary credential (e.g., a contactless card) and the absence of alcohol in their breath.

### 12.1. Connection of breathalyzers, general considerations

Sigur controllers support almost any discrete breathalyzer models that identify the presence or absence of alcohol in the breath and some models that can identify the exact alcohol content, which can be used in the system for more flexible configuration of access rights for various categories of users.

#### 12.1.1. Standard mode

This option will enable or disable testing for selected groups of employees with the per mille threshold set in the breathalyzer settings. The following connections and settings are needed on the controller side:

- **Pending alcohol testing to enter / Pending alcohol testing to exit** sends a test request to the breathalyzer.
- **Alcohol Testing Disabled input** sends the OK command from the breathalyzer to the controller (as per the threshold set on the breathalyzer).
- **Breathalyzer wait time.**

For employees who are subject to alcohol testing, a special rule is created (e.g., a Level 2 rule) with the following parameters:

- **Cardholders affected by the rule.** Select all applicable credentials.
- **Affected access points.** Select all access points with breathalyzers.
- Make sure that the start date of the new exception is within the appropriate date range and the end date is set far in the future.
- Make sure to set the end date for the rule many years ahead.
- In the **Days** tab, add at least one day when the rule applies and add access intervals for entrance and exit.
- In the **Special rules** tab, enable the **Alcohol testing** option in the respective direction and change the **Alcohol testing probability**, where necessary.

#### 12.1.2. Extended mode

In this mode, alcohol testing can be set to be requested only after authentication. It provides options to record and store alcohol test results, configure thresholds and organize random testing. In this mode, you can use a breathalyzer in both directions and in combination with a card collector or other auxiliary access control devices.

As of the date of this document, the following breathalyzer models are compatible:

- Dingo B-02 with special Sigur firmware;
- Alcobarrier (manufactured by Alcotector);
- Alcoframe (manufactured by Laser Systems).

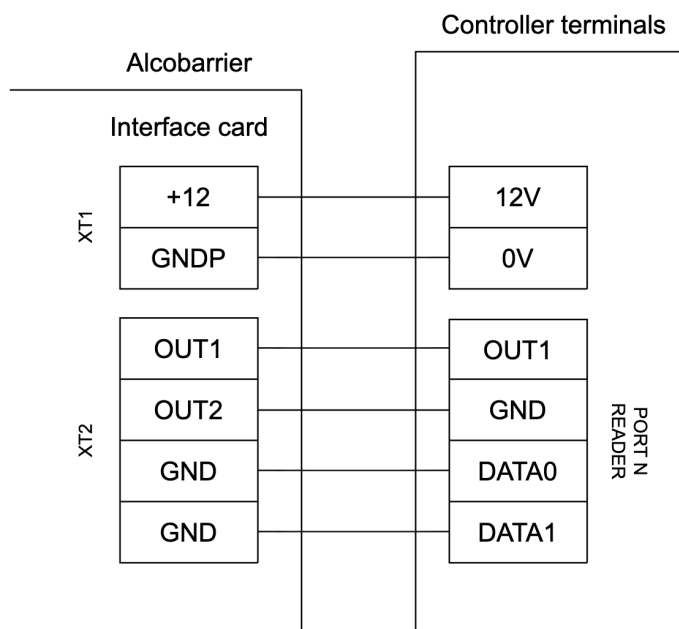
For connection and configuration options for the controller, please see the respective sections of this document.

## 12.2. Alcobarrier (by Alcotector)

It can record and store alcohol test results, breathalyzer errors, configure thresholds and organize random testing. These breathalyzers can be connected for both directions and in combination with a card collector and other access control devices.



To enable interoperability, this breathalyzer must have a special interface card installed by the manufacturer. The **Alcobarrier Setup** utility helps configure the device. You can download an archived configuration file by following this [link](#). Before installation, please extract the file from the archive.



Alcobarrier connection diagram.

### Access point configuration:

Go to the **Client** software, select the respective controller from the list on the **Access Points** tab and press **Settings**.

On the **General** tab, uncheck the **Show basic settings only** and enter the value "1.0" for the **Alcohol testing factor** parameter.

Configure the following options for access points connected to breathalyzers:

- **Pending alcohol testing to enter** (or **Pending alcohol testing to exit**), the **OUT1, normally not active** terminal.
- **Port of the entrance reader > Breathalyzer** (or **Port of the exit reader > Breathalyzer**, depending on the direction), the port number "N".

Where N is the number of the port to which the breathalyzer is connected. Press **OK**.

**Configuration of access rules:**

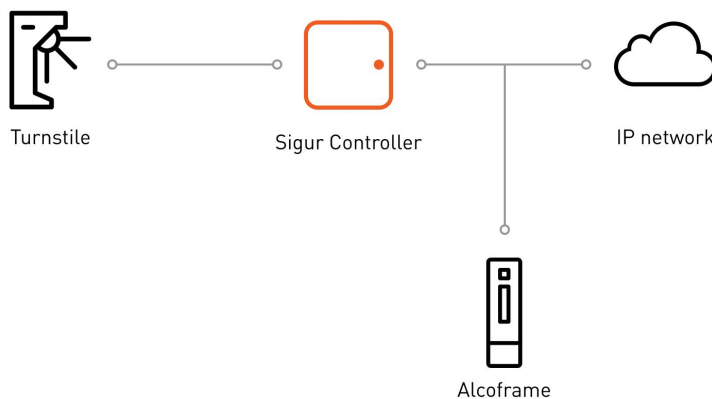
For employees who are subject to an additional check at entrance or exit, create an exception with the following parameters:

- **Cardholders affected by the rule.** Select all applicable credentials.
- **Affected access points.** Select all access points with breathalyzers.
- Make sure that the start date of the new exception is within the appropriate date range and the end date is set far in the future.
- Make sure to set the end date for the rule many years ahead.
- In the **Days** tab, add at least one day when the rule applies and add access intervals for entrance and exit.
- On the **Special rules** tab, change all applicable options in the **Alcohol testing** section as necessary.

### 12.3. Alcoframe (by Laser Systems)

It can record and store alcohol test results in per mille, configure thresholds and organize random testing.

Alcoframe is connected to the local network of your site and does not require to be directly connected to the controller.



Connection option for Alcoframe in the Sigur ACS.



One Sigur controller supports only one Alcoframe. This must be taken into consideration when designing the system and assessing the number of controllers needed.

Go to the Alcoframe web interface and configure the network parameters of the device and the UDP port for commands. To do this, type `http://10.0.0.103/` (where 10.0.0.103 is the default IP address of the device) in the address bar of your browser, go to the menu **Network > UDP Connection Settings** and change the "**Command UDP port**" and "**Result Transmission UDP port**" parameters.

#### Access point configuration:

Go to the **Client** software, select the respective controller from the list on the **Access Points** tab and press **Settings**. There go to the **General** tab and enable the **Use Alcoframe breathalyzer** option. Enter the IP address and port (the **UDP port for commands** parameter in the Alcoframe settings) assigned to the device.

Use Alcoframe breathalyzer

IP:  Port:

Example settings for the controller parameters.

#### Configuration of access rules:

For employees who are subject to an additional check at entrance or exit, create an exemption with the following parameters:

- **Cardholders affected by the rule.** Select all applicable credentials.
- **Affected access points.** Select all access points with breathalyzers.
- Make sure that the start date of the new exception is within the appropriate date range and the end date is set far in the future.
- Make sure to set the end date for the rule many years ahead.
- In the **Days** tab, add at least one day when the rule applies and add access intervals for entrance and exit.
- On the **Special rules** tab, change all applicable options in the **Alcohol testing** section as necessary.

## 13. Turnstiles and swing gates

### 13.1. Connection of turnstiles, general considerations

The controller supports various turnstile control modes and sensor processing modes. Turnstiles are controlled by relay contacts located on the controller board.

The turnstile control logic is described in more detail below.



DO NOT use the GND terminals on the controller to connect any equipment with an external power supply source. This may result in the controller failure.

The GND terminals are connected to the negative terminal of the controller via a common-mode choke. The choke current is calculated based on the max. current achievable on the ports of the controller.

Any extra load between the positive terminal of the controller and any of the GND terminals can result in the controller failure. The GND terminals can be used only together with other ports of the controller (PWR, PASS, RTE, etc.).

### 13.2. Turnstile control options

#### Potential control mode:

When the controller authorizes access, the entrance relay or the exit relay is activated. The default relay activation time pending an access event is 5 seconds and can be changed, where necessary. When the waiting time expires or the access event is completed, the relay returns to its inactive state and locks the turnstile.

#### Pulse control mode:

When the controller authorizes access, the entrance relay or the exit relay is shortly activated. When the waiting time expires (5sec by default) or the access event is completed, Relay 3 will shortly be activated to close the turnstile. The relay activation pulse duration in the pulse control mode can be configured as necessary.

### 13.3. Available access control sensor configurations

1. **Direct connection.** It uses two access control sensors that are activated at different stile rotation angles of the turnstile (some models of PERCo turnstiles).
2. **Simplified connection.** It uses two lines that the turnstile controller uses to send pulses to notify of entry or exit (most turnstile models).

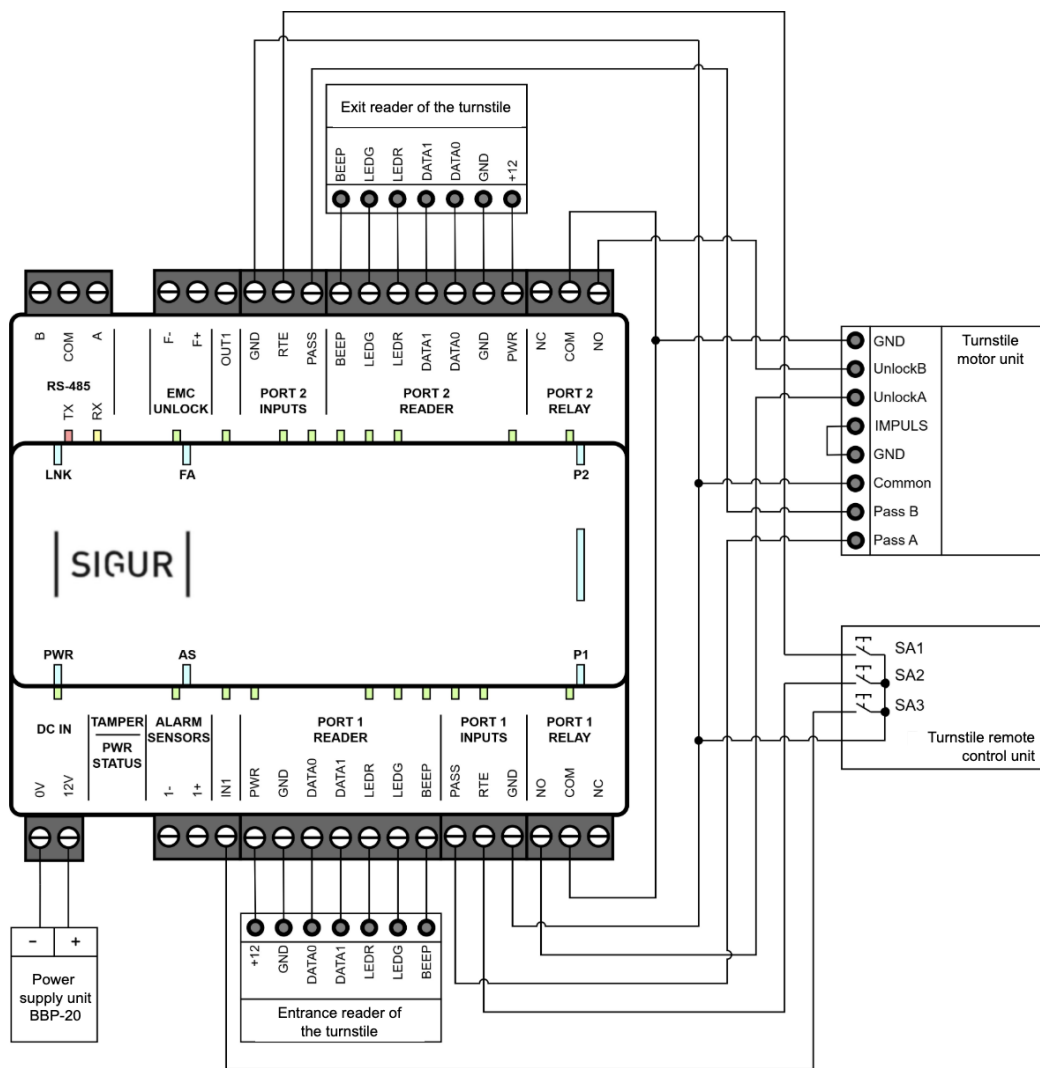
3. **Single-wire connection.** In this case, the turnstile uses one sensor that is activated in both directions of access (e.g., older Rostov-Don turnstile models).

### 13.4. Turnstile remote control, general considerations

Connecting the remote control to the controller instead of directly to the turnstile will ensure error-free registration of access events permitted from the remote control and flexible management of single-time access events or recurring access permissions granted in various directions.

The controller can process commands from three normally open remote control buttons. The remote control indication is controlled by the turnstile control unit.

### 13.5. Connection option for a turnstile



Connection option for a turnstile.

## 13.6. 3V turnstiles

To operate a 3V turnstile, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

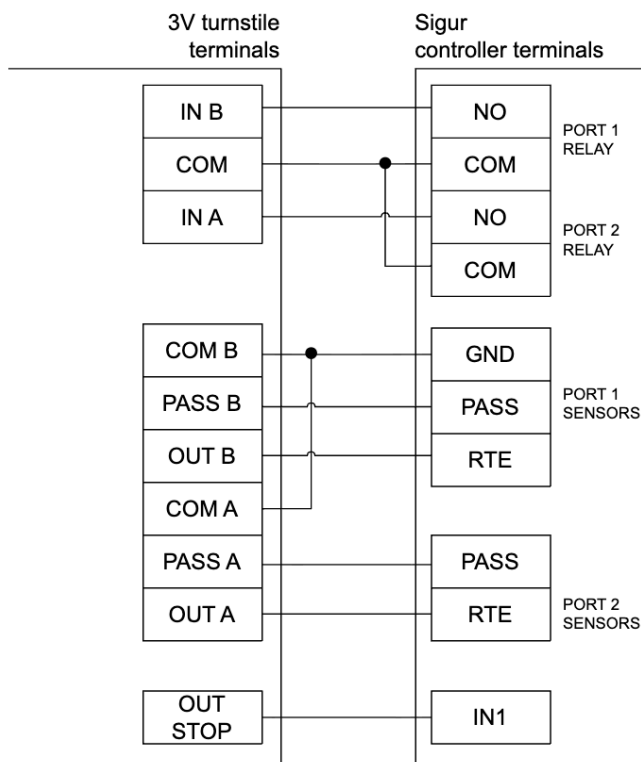
Select the standard Turnstile, potential control mode configuration on controller.

If the PASS A and PASS B jumpers on the turnstile circuit board are in the NC position, no additional settings are required.

If the PASS A and PASS B jumpers on the turnstile circuit board are in the NO position, change the sensor state to **normally open**. To do this, make the following controller settings:

- Option: **Entrance access control sensor line**; Access point 1;  
Terminal: **PASS(PORT 1 SENSORS)** set to **normally open**.
- Option: **Exit access control sensor line**; Access point 1;  
Terminal: **PASS(PORT 2 SENSORS)** set to **normally open**.

To connect 3V turnstiles, either terminals on the front side of the turnstile circuit board or ports on the back side of the turnstile circuit board can be used.



Connection of a 3V turnstile to the controller via the ports on the front side of the turnstile circuit board.

The remote control is connected directly to the turnstile according to the respective turnstile user guide.

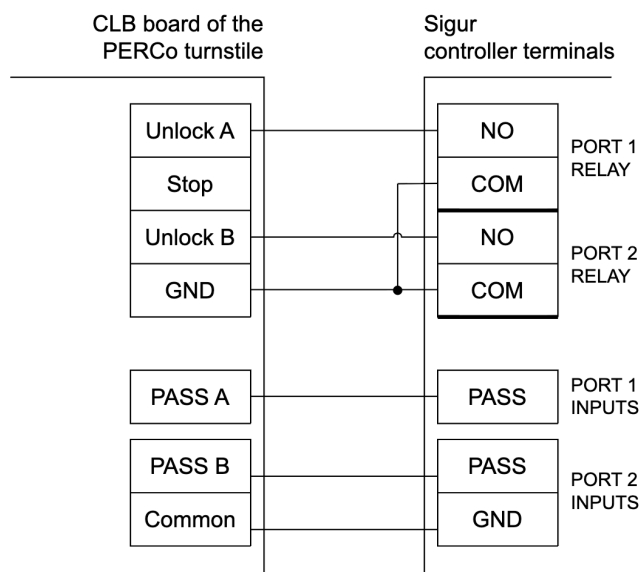
## 13.7. PERCo turnstiles and swing gates

### 13.7.1. PERCo TTR-04.1, TTD-03, T-5, TTR-07, TTR-08A, TTD-08A

To operate PERCo turnstiles, such as TTR-04.1, TTD-03, T-5, TTR-07, TTR-08A, TTD-08A, the controller should be switched to the potential control mode and set to operate normally closed access control sensors in the simplified mode.

Select the standard Turnstile, potential control mode configuration on controller.

In the **Client** software, go to the controller settings and enable the **Perco turnstile compatibility** option. To do this, select the access point on the **Access Points** tab, press **Settings**, uncheck the **Show basic settings only** box and check the **Perco turnstile compatibility** box and then press **OK**.



PERCo TTR-04.1, TTD-03, T-5, TTR-07, TTR-08A, TTD-08A.



When connecting PERCo turnstiles series TTR-04.1, TTD-03, T-5, TTR-07, TTR-08A, TTD-08A, make sure you remove the J1 jumper on the CLB board of the turnstile to switch to the potential control mode. In the pulse control mode, it will automatically lock in a set period of time that cannot be changed by the Sigur controller.

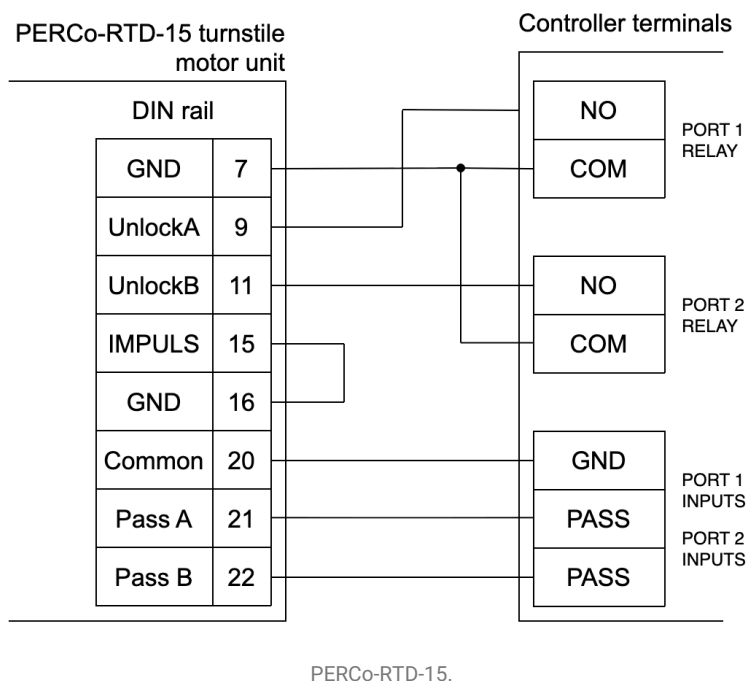
For detailed instructions on how to connect the remote control, please see the PERCo remote control unit section of this document.

### 13.7.2. PERCo-RTD-15

To operate a PERCo-RTD-15 turnstile, the controller should be switched to the potential control mode and set to operate normally closed access control sensors in the simplified mode.

Select the standard Turnstile, potential control mode configuration on controller.

In the **Client** software, go to the controller settings and enable the **Perco turnstile compatibility** option. To do this, select the access point on the **Access Points** tab, press **Settings**, uncheck the **Show basic settings only** box and check the **Perco turnstile compatibility** box and then press **OK**.



For detailed instructions on how to connect the remote control, please see the PERCo remote control unit section of this document.

### 13.7.3. PERCo ST-01, ST-02

To operate PERCo ST-01 and ST-02 turnstiles, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

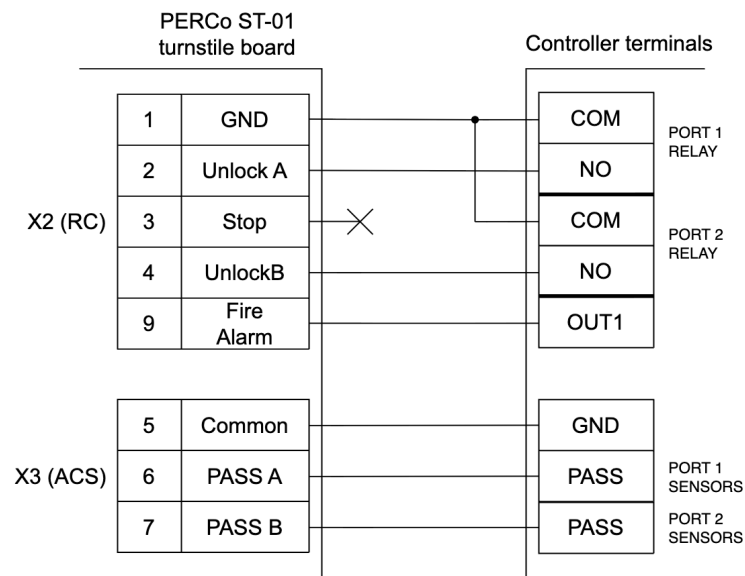
Select the standard Turnstile, potential control mode configuration on controller.

In the Client software, go to the controller settings and enable the Perco turnstile compatibility option. To do this, select the access point on the Access Points tab, press Settings, uncheck the Show basic settings only box and check the Perco turnstile compatibility box and then press OK.

The sensor state should be also changed to normally open.

To do this, make the following controller settings:

- Option: **Entrance access control sensor line**;  
Terminal: **PORT 1 SENSORS** set to **normally open**.
- Option: **Exit access control sensor line**;  
Terminal: **PORT 2 SENSORS** set to **normally open**.



PERCo ST-01 and ST-02.

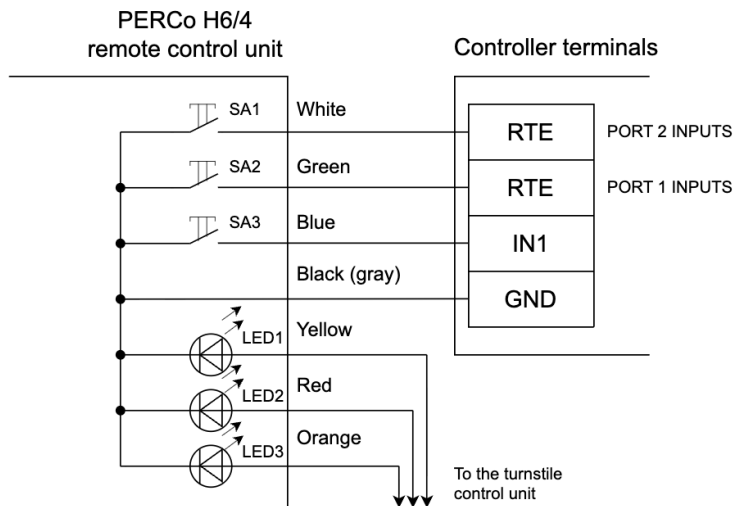


Make sure you **DISABLED** the Pulse switch on the PERCo ST-01 turnstile board to switch to the potential control mode. In the pulse control mode, it will automatically lock in a set period of time that cannot be changed by the Sigur controller.

For detailed instructions on how to connect the remote control, please see the [PERCo remote control unit](#) section of this document.

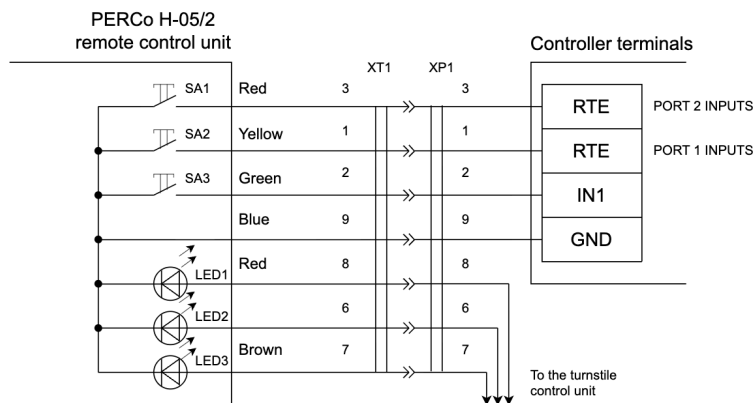
### 13.7.4. PERCo remote control unit

PERCo remote control buttons (H6/4, H-05/2) are connected to the Sigur controller and the indication is connected to the PERCo turnstile controller.



PERCo H6/4 remote control unit.

**i** The wire colors of the remote control can vary in different batches. To ensure correct connection, please see the documents for your turnstile.



PERCo H-05/2 remote control unit.

Where necessary, the remote control wires can be directly connected to the terminals of the controller. However, please keep in mind that the colors of the wires on the diagram might not match the actual colors. To ensure correct connection, please remember which wires match which plugs.

**Designations on the figures:**

SA1	Normally open A button of the remote control.
SA2	Normally open B button of the remote control.
SA3	Normally open Stop button of the remote control.
LED1	LED indicator A of the remote control.
LED2	LED indicator B of the remote control.
LED3	LED indicator Stop of the remote control.
XT1	DB-9M plug of the remote control.
XP1	A DB-9F connector to connect the remote control to the Sigur controller is not supplied with the controller.

Two connection options are available for remote control buttons.

1. Directly to the turnstile control unit. In this case, either all access events allowed from the remote control will be registered as break-in events by the access control system or all unauthorized access events will be registered as access events allowed from the remote control (depending on the controller settings). The operator will be able to manually enable the free access mode in one or both directions.
2. To the controller. Access events allowed by button will be registered in the access control system as **Access granted by button** events. However, the free access mode becomes unavailable.

## 13.8. Praktika turnstiles (Oxgard)

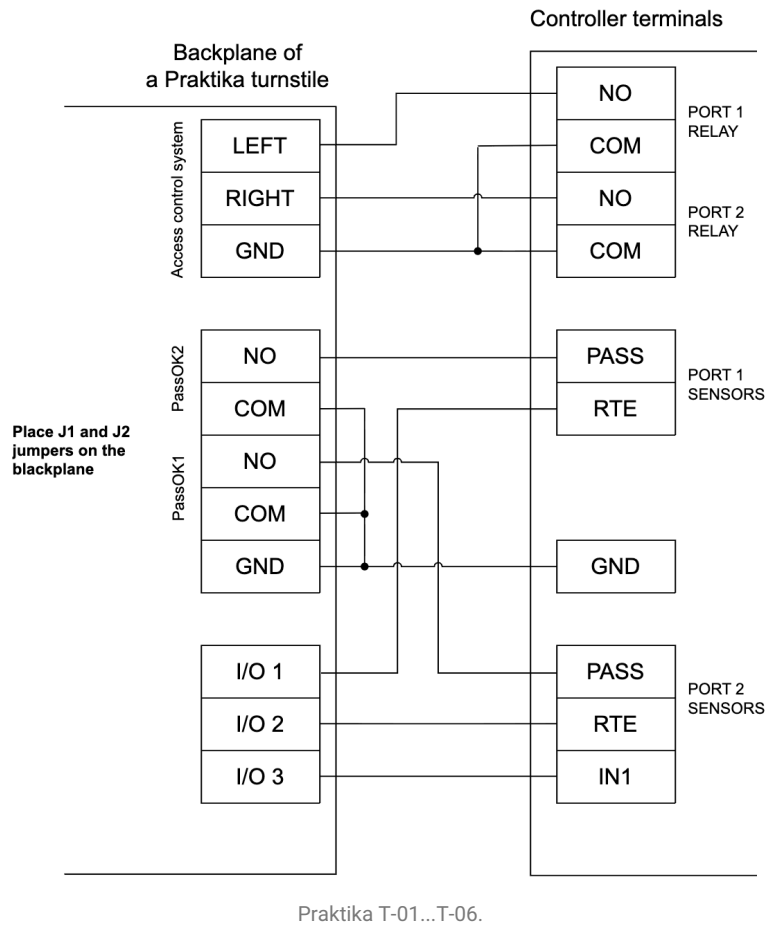
### 13.8.1. Praktika T-01...06

To operate Praktika T-0X turnstiles, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

Select the standard Turnstile, potential control mode configuration on controller.

The sensor state should be also changed to **normally open**. To do this, make the following controller settings:

- Option: **Entrance access control sensor line**; Access point 1; Terminal: **PASS(PORT 1 SENSORS)** set to **normally open**.
- Option: **Exit access control sensor line**; Access point 1; Terminal: **PASS(PORT 2 SENSORS)** set to **normally open**.



The remote control is connected to the controller of the turnstile.

### 13.8.2. Cube C-04



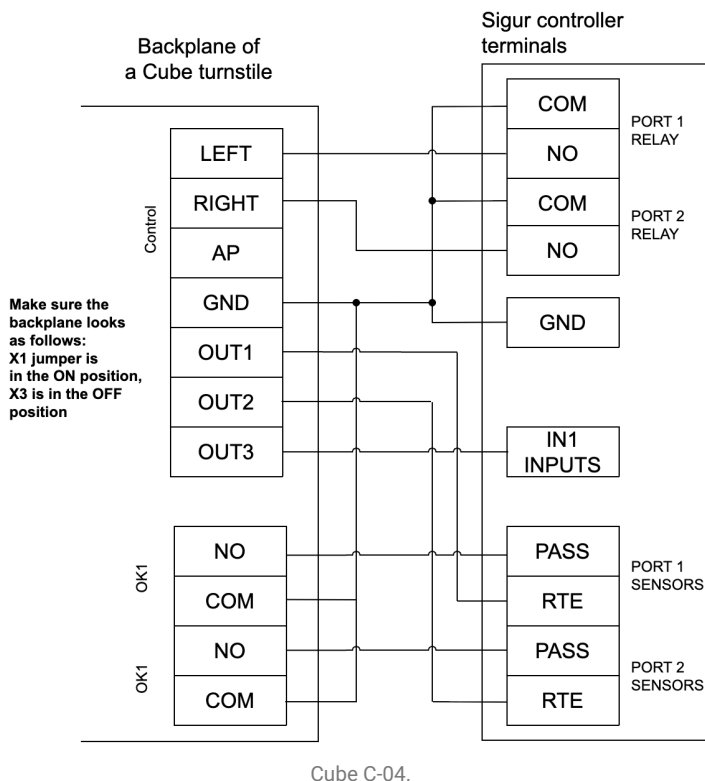
A connection diagram is provided for a standard turnstile model without an integrated card collector. If you need to connect a card collector, we recommend using other Sigur controller models, including E4, E510, etc.

To operate Cube C-04 turnstiles, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

Select the standard Turnstile, potential control mode configuration on controller.

Next, configure Access Point 1 as follows:

- Option: **Entrance access control sensor line** ;  
Terminal: **PASS(PORT 1 SENSORS)** set to **normally open**.
- Option: **Exit access control sensor line** ;  
Terminal: **PASS(PORT 2 SENSORS)** set to **normally open**.
- Uncheck the **Show basic settings only** and check the **Lock the turnstile when the signal from the access control sensor is at the falling edge** option.



## 13.9. CARDDEX turnstiles

### 13.9.1. CARDDEX CBU-250 (CBU-150/250) control unit



Due to some non-standard features of this turnstile model (non-standard manual remote control), it has some limitations when connected to the access control system:

1. All access events not authorized by the ACS controller (including potential break-ins) are registered as access granted from the remote control.
2. There can be conflicts when a card is used at the same time as the remote control button is pressed.

This unit is installed in turnstiles and electronic checkpoints CARDDEX series STR-01/02/03/04 and STX-01/02/03/04.

If a turnstile has integrated readers, terminals W 1.0, W 1.1, W 2.0, W 2.1 of CBU-250 (CBU-150/250) control unit must be connected to the controller according to the diagram. Otherwise, you can connect it directly to the Sigur controller according to the standard connection scheme.

The turnstile control unit is equipped with a potential port ALRM for instant unlocking in both directions in emergency situations. In some turnstile models, the "Anti-panic" stiles will also fold automatically. It is recommended to connect this control line to a relay on the Sigur controller. If no free relays are available, unused controller outputs for other purposes may be used.

To operate CARDDEX CBU-250 (CBU-150/250) control unit, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

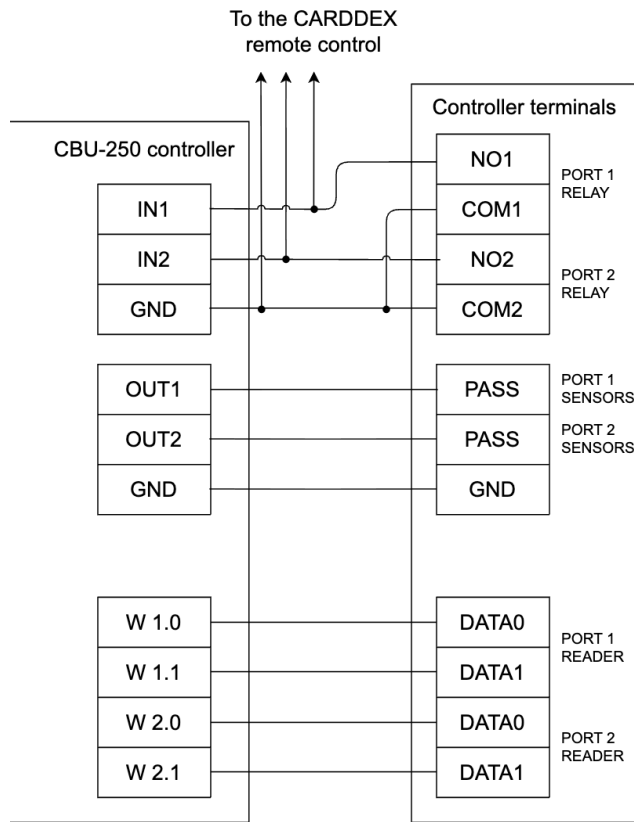
Select the standard Turnstile, potential control mode configuration on controller.

The sensor state should be also changed to **normally open**. To do this, in the **Client** software, select the respective access point on the **Access Points** tab and press **Settings** to add the following options:

- Option: **Exit access control sensor line**; Terminal: **PASS(PORT 1 SENSORS)** set to **normally open**.
- Option: **Entrance access control sensor line**; Terminal: **PASS(PORT 2 SENSORS)** set to **normally open**.


Before you start using your access point, please also make sure you configured your controller (select it in the list on the Access Points tab, press **Settings**, disable the **Show basic settings only** parameter):

- **Turnstile No.1 break-out response**. Set to **Register entry permitted by button**.
- **Turnstile No.1 break-in response**. Set to **Register exit permitted by button**.



CARDDEX electronic checkpoints, CBU-250 (CBU-150/250) turnstile controller.

### 13.9.2. CARDDEX CBU-240 control unit



Due to some non-standard features of this turnstile model (non-standard manual remote control), it has some limitations when connected to the access control system:

1. All access events not authorized by the ACS controller (including potential break-ins) are registered as access granted from the remote control.
2. There can be conflicts when a card is used at the same time as the remote control button is pressed.

The Sigur controller supports connection of CARDDEX turnstiles of the STR and STL series equipped with the CBU-240 control unit. Control is carried out in potential mode, in which the turnstile remains unlocked for the entire duration of the signal from the Sigur controller.

The turnstile control unit is equipped with a potential port ALRM for instant unlocking in both directions in emergency situations. In some turnstile models, the “Anti-panic” stiles will also fold automatically. It is recommended to connect this control line to a relay on the Sigur controller. If no free relays are available, unused controller outputs for other purposes may be used.

To operate CARDDEX CBU-240 control unit, the controller should be switched to the potential control mode and set to operate normally open access control sensors in the simplified mode.

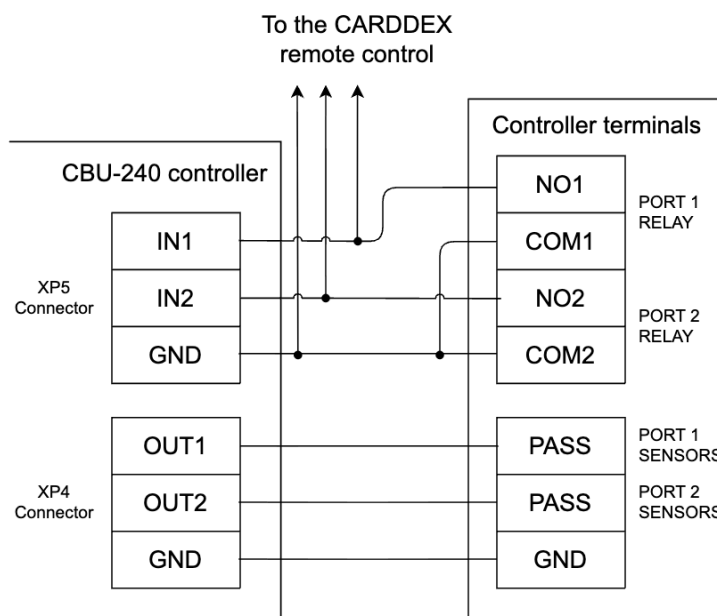
Select the standard Turnstile, potential control mode configuration on controller.

The sensor state should be also changed to **normally open**. To do this, in the **Client** software, select the respective access point on the **Access Points** tab and press **Settings** to add the following options:

- Option: **Exit access control sensor line**; Terminal: **PASS(PORT 1 SENSORS)** set to **normally open**.
- Option: **Entrance access control sensor line**; Terminal: **PASS(PORT 2 SENSORS)** set to **normally open**.

Before you start using your access point, please also make sure you configured your controller (select it in the list on the Access Points tab, press **Settings**, disable the **Show basic settings only** parameter):

- **Turnstile No.1 break-out response**. Set to **Register entry permitted by button**.
- **Turnstile No.1 break-in response**. Set to **Register exit permitted by button**.



CARDDEX electronic checkpoints, CBU-240 turnstile controller.

## 14. Controller operating logic

### 14.1. Startup of the controller

When powered up, the controller will:

1. Check the RESET button status. If the button is pressed and:
  - Held for less than 5 seconds, the controller will reset the IP settings and continue launching.
  - Held for at least 5 seconds, hardware reset will be initiated. (Note: Hardware reset is available only for devices with the firmware version 15 and newer).
2. Initiate sensor lines and access point control lines according to the current configuration.
3. Check the status of the fire alarm line:
  - If the fire alarm line is not in its normal state, please see the [Processing of Fire Alarm Signals](#) section of this document for further controller actions.
  - If the fire alarm line is in its normal state, the controller will check the access point operating mode from its non-volatile memory stored when the controller was powered off and lock all the respective connected access points.
4. Check if the security system is activated. If it is activated and does not operate normally, when the controller is launched, the controller will send an alarm signal to the server. For a detailed description of the normal operation of the lines and possible issues, please see the [Processing of Security and Fire Alarm Signals](#) section of this document.
5. Start controlling the RESET button. If pressed, the IP configuration will be reset and you will hear a specific sound.

### 14.2. Indication lines of the reader

If the readers are connected according to the [Connection of readers](#) section, the controller will also control their indication.

By default, when no cards are present within the reading distance of the reader, the LEDG line of the controller is active and the LEDR and BEEP lines of the controller are not active. In this configuration, LEDR (the red LED of the reader) is on, LEDG (the green LED of the reader) is off and BEEP (the loudspeaker of the reader) is inactive.

By default, when a card code is read, the controller can respond in two different ways:

- Access granted. The red LED will turn off once shortly and the green LED will light up on the reader (if the integrated loudspeaker is enabled, you will hear a simultaneous short beep).
- Access denied. The green LED will blink three times (the red LED will turn off as the green LED lights up and you will hear short beeps, if the loudspeaker is enabled).

In addition to reading credentials, the controller can also activate indication control lines of the reader if any alarms are detected such as break-in or door propping.

Where necessary, the indication control logic can be modified in the controller settings window in the **Client** software.

### 14.3. Processing of fire alarm signals

The fire alarm line operates as follows:

1. In the normal state, the fire alarm line should be closed.
2. If the line breaks and stays open for a set amount of time, the controller will:
  - Unlock (open) all connected access points;
  - Switch to the Fire Alarm state;
  - Activate the Fire Alarm sound indication (see the [Sound indication of the controllers appendix](#));
  - Wait for the fire alarm line to restore (close).
3. When the fire alarm line is restored, the controller will return to normal operation.

### 14.4. Processing of security and fire alarm signals

Under the normal operating conditions, the connected security and fire alarm line has a constant resistance value between 3.3...6.2k $\Omega$ . If at least one of the security and fire alarm sensors is activated, the resistance value will change and the controller will send an alarm signal to the ACS server. The controller will keep sending the alarm signal unless the system operator deactivates the alarm in the Sigur software.

### 14.5. General-purpose outputs

The controller has general-purpose outputs which can be configured through the port mapping feature.

## 14.6. Input and output protection circuits of the controller

### 14.6.1. Power supply of the controller

If polarity is not observed when connected to the power source or the supply voltage exceeds the threshold, the controller will be switched to a hardware protection mode and normal operation will be disrupted.

When the supply voltage parameters return to normal, the controller will automatically switch to the normal operating mode.

If the supply voltage exceeds the tolerated range, the controller will inform the server and this information will be seen in the power supply status field.

The operating supply voltage range required for the stable operation of the controller is provided in the [Controller Specifications](#) section of this document.

### 14.6.2. Power supply of the readers

The power supply circuits of the readers are protected against overloads and reverse polarity by self-resetting fuses with the trip current of 200mA and protection diodes.

If the input current exceeds 200mA, the power supply circuit of the reader will automatically switch off. If the voltage supplied to the power terminals of the reader is higher than the specified supply voltage of the controller, the protection diodes will trip and protect the power supply unit and the controller from damage.

After the emergency has been fixed, the reader will be automatically powered on.

### 14.6.3. Outputs of the controller

The common collector and common drain outputs of the controller are protected against overloads, overvoltage and reverse polarity by self-resetting fuses with the trip current of 200mA and protective diodes.

If the output current exceeds 200mA or the negative voltage or the voltage exceeding 30V is supplied to the output, the output circuit will automatically switch off.

After the emergency has been fixed, the functionality of the output will be automatically restored.

#### 14.6.4. Inputs of the controller

The inputs of the controller are protected against overvoltage and reverse polarity by self-resetting fuses and protection diodes.

If the negative voltage or the voltage exceeding 5V is supplied to the input of the controller, the input circuit will automatically switch off.

After the emergency has been fixed, the functionality of the input will be automatically restored.



The controller protection systems are designed to withstand the maximum voltage up to 60V. The manufacturer does not guarantee automatic restoration of the inputs / outputs if the supplied voltage exceeds 60V.

### 14.7. Access points controlled by doors

#### 14.7.1. Operating modes

Doors connected to the controller can operate in one of the three modes below:

- **Normal operating mode.**

The door is normally locked. When the RTE button is pressed, the door will unlock for a set period of time. After the access event has successfully completed, the lock will be automatically locked. If the door is held open for too long, the controller will signal about this event via the indicators on both connected readers.

- **Locked operating mode.**

The door is locked and cannot be unlocked neither by the RTE button nor by presenting a credential. The door can be switched to this mode:

- by a system operator from the client workstation;
- by double-tapping a credential (if this feature is enabled in the system);
- according to the schedule;
- while the Door Lock button is pressed;
- when the button that was assigned to switch it to the blocked mode is pressed.

- **Unlocked operating mode.**

The door is normally open. The door can be switched to this mode:

- by a system operator from the client workstation;
- by double-tapping a credential (if this feature is enabled in the system);
- according to the schedule;
- when the button that was assigned to switch it to the unlocked mode is pressed.



Some types of locks (e.g., electromechanical locks) cannot be force-locked by the controller and thus in some cases can remain open (e.g., if no access event is registered after the lock was opened, the door will remain open).

### 14.7.2. RTE buttons

RTE (Request to Enter / Exit) buttons can be connected to the controller. One button can open the door for an unknown direction of access, other buttons can be recognized by the controller as entry or exit.

This flexibility helps avoid errors in registering the direction of access and, where necessary, you can add a button that will grant access in an unknown direction at the security desk and the security guard can both let the visitors in and out.

### 14.7.3. Lock buttons

- When the Door Lock button is pressed and held, the door will not open until the button is released.
- The Door Lock button also overrides the **Access Granted by Security** feature.

## 14.8. Access points controlled by turnstiles

### 14.8.1. Operating modes

Turnstiles connected to the controller can operate in one of the three modes below:

- **Normal operating mode.**

The turnstile is normally locked in both directions. After reading an authorized credential, the turnstile will unlock for a set period of time in the respective direction. If the access event was successful or if the time expired, the turnstile will be automatically locked. The same logic applies to access granted from the remote control.

- **Locked operating mode.**

The turnstile will be locked in both directions and will not be unlocked even when a credential is presented. This mode can be activated:

- by a system operator from the client workstation;
- by double-tapping a credential (if this feature is enabled in the system);
- according to the schedule;
- by pressing a certain combination of buttons on the turnstile remote control;
- when the button that was assigned to switch it to the blocked mode is pressed.

- **Unlocked operating mode (free access).**

The turnstile is always unlocked in both directions. This mode can be activated:

- by a system operator from the client workstation;
- by double-tapping a credential (if this feature is enabled in the system);
- according to the schedule;
- when the button that was assigned to switch it to the unlocked mode is pressed.

- **Partially unlocked operating mode.**

The turnstile is always unlocked in one or both directions. This mode can be activated by pressing a certain combination of buttons on the turnstile remote control.

## 14.8.2. Operating the turnstile remote control unit

A turnstile remote control has two or three buttons with the designations as described in the table below.

### Turnstile remote control buttons.

Name	Description
Button A	Unlocks the turnstile to exit or allows exit.
Button B	Unlocks the turnstile to enter or allows entry.
Stop button	Locks the turnstile or denies access. This button is not required, but not using it will significantly reduce the functionality of the remote control.

**Commands sent from the turnstile remote control.**

Buttons sequence	Command
Button <b>A</b> pressed once	Opens the turnstile for a single exit event.
Button <b>B</b> pressed once	Opens the turnstile for a single entry event.
<b>Stop</b> button pressed once	<ol style="list-style-type: none"> <li>1. Immediately locks the turnstile; the turnstile remains locked while the button is pressed.</li> <li>2. When released, disables free access.</li> </ol>
The <b>Stop</b> button is pressed and held, then Button <b>A</b> is pressed and then both buttons are released	Free <b>exit</b> . To switch the turnstile in its normally locked state, press the <b>Stop</b> button once.
The <b>Stop</b> button is pressed and held, then Button <b>B</b> is pressed and then both buttons are released	Free <b>entry</b> . To switch the turnstile in its normally locked state, press the <b>Stop</b> button once.
The <b>Stop</b> button is pressed and held, then Buttons <b>A</b> and <b>B</b> are pressed and then all the buttons are released	Free <b>entry and exit</b> . To switch the turnstile in its normally locked state, press the <b>Stop</b> button once.

## 15. Troubleshooting

This section provides a short list of possible issues and recommended troubleshooting tips.

### 15.1. Troubleshooting power supply and controller startup issues

1. **If the DC IN indicator on the controller is off (i.e., no voltage on 0V and 12V terminals of the controller), check for the following issues:**
  - Failure of the fuse of the power supply unit or the power supply unit itself.
  - Incorrect connection to the power source. Please refer to the [Power supply of the controller](#) section of this document.
2. **If the DC IN indicator on the controller is on (i.e., there is voltage on 0V and 12V terminals), but the PWR indicator on the controller board is off, check for the following issues:**
  - Incorrect polarity of the supply voltage on "+" and "-" terminals. Reconnect the power source and make sure to observe the correct polarity.
  - The supply voltage exceeded 15V. Fix the voltage.
3. **If the power source is overheated or turns off due to overloads, check for the following issues:**
  - The threshold of the current consumption from the source is exceeded: compare the current consumption with the maximum output current of the power source (it is recommended to have 30% current-carrying capacity to ensure uninterrupted operation) and, if necessary, replace the power supply unit with a more suitable one.
  - The nominal voltage of the connected readers, locks, etc. is exceeded. Match the voltage of the power supply unit and the connected devices by either replacing the power supply unit or the incompatible devices.
4. **If the controller launches (+12V and PWR LEDs light up on the board) and immediately starts playing the series of beeps:**

Please see the [Sound indication of the controller](#) appendix to find out the error details.
5. **If the controller starts (the PWR LED lights up on the board), but other LEDs on the board are off and the controller does not respond to any actions (presenting an authorized card, pressing a connected button, etc.):**

Make sure that the controller configuration is selected (**Access Points** tab > select the respective access point > press **Settings**) and that all the necessary roles are assigned and the controller terminals used are mapped.

## 15.2. Troubleshooting Ethernet connection

**If no connection is established between the server and the controllers, you may consider one of the following issues:**

- Incorrect IP parameters of the controller (IP address, subnet mask, default gateway, server address).
- Incorrect network parameters of the controller in the **Client** software.
- Incorrect routing of data between the controller and the server or the data transfer is prevented by the current firewall settings (including Windows Firewall).

**In any case, check the following:**

- The status of the Ethernet connection indicator (green LED of the Ethernet port).
- The status of the data transmission indicator (yellow LED of the Ethernet port) while attempting to reach out to the controller.
- Network performance by sending ICMP PING requests (ping command).
- Settings of the firewall.

## 15.3. Troubleshooting server connection issues

Sometimes events fail to get through from the controllers of the system. Interacting in any way with the controller in the software (such as changing the controller parameters, selecting access rules, etc.) can solve the issue temporarily and all events stored in the autonomous controller memory are synchronized with the server.

**Solution:** Disable any firewalls, antiviruses, etc. on the server or grant necessary permissions to ensure proper communication with the ports used by the system. If interacting with the server computer does not help, make sure to contact your system administrator to run diagnostics of the network (packages from the controller should not be lost when sent to the server computer).

## 15.4. Troubleshooting lock connection issues

1. **If you have issues with a normal sequence of unlocking and locking when access is granted:**  
Please, make sure that the lock, door open sensor or lock button are connected correctly and that you selected the respective normal state for the door open sensor.
2. **If the fuse on the power supply unit of the lock trips immediately when the controller starts or access is granted:**  
Make sure to check the lock power supply line since it might have short-circuited and check the polarity of the protective diode connected to the lock (if used instead of a varistor).

## 15.5. Troubleshooting reader connection issues

1. **The reader does not respond to a presented card (the LED on the reader does not light up and no sound is played):**
  - The reader is not powered up.
  - The reader does not support this type of cards.
  - The reader is not properly connected to the controller (i.e., DATA0 and DATA1 lines are mixed up).
  - The output interface of the reader is not properly configured. Please verify that the suitable configuration is selected (see the user guide of your reader).
  - The reader is malfunctioning.
2. **When a credential is read, the reader indication is activated but the access point does not unlock:**
  - The reader is not properly connected to the controller (i.e., DATA0 and DATA1 lines are mixed up).
  - The output interface of the reader is not properly configured. Please verify that the suitable configuration is selected (see the user guide of your reader).
  - The credential presented is not authorized in the system or the applicable access rules do not allow this cardholder to access the premises.
3. **Unstable operation of the reader, sometimes the reader fails to authenticate cards:**
  - The current consumption of the readers connected to the controller exceeds the operating range.
  - A blacklisted reader is used.
  - The reader is malfunctioning.

## 15.6. Troubleshooting turnstile connection issues

Below are possible issues you can face when operating a turnstile. First, we recommend to find the issue that matches your situation the most and only then follow the recommended steps.

1. **When a cardholder passes through the turnstile, the system registers an access event in an opposite direction (i.e., a card was presented at the entrance and the turnstile was unlocked to allow entry but the system recorded exit after the access event has been completed).**

Follow the steps below:

1. Swap the directions for the entrance and exit readers by swapping the lines on the PORT1 READER and PORT2 READER terminals of the controller or by mapping the terminals accordingly in the software.
2. Reassign the commands **open to enter** and **open to exit** by swapping the lines on relay terminals 1 and 2 of the controller or by mapping the terminals accordingly in the software.
3. Fix the access control sensor connections (if there are two of them) by swapping the lines on terminals PASS PORT1 and PASS PORT2 of the controller or by mapping the terminals accordingly in the software.

2. **When a cardholder passes through the turnstile, the system registers a break-in or break-out event (i.e., a card was presented at the entrance and the turnstile was unlocked to allow entry but the system recorded a break-in event).**

Follow the steps below:

1. Swap the directions for the entrance and exit readers by swapping the lines on the PORT1 READER and PORT2 READER terminals of the controller or by mapping the terminals accordingly in the software.
2. Reassign the commands **open to enter** and **open to exit** by swapping the lines on relay terminals 1 and 2 of the controller or by mapping the terminals accordingly in the software.

3. **When access is granted, the turnstile opens in an opposite direction and after the stiles rotate in this direction, the system registers an access events in the correct direction (i.e., a card was presented at the entrance, the turnstile unlocked to exit, the stiles rotated and the system recorded entry).**

Follow the steps below:

1. Reassign the commands **open to enter** and **open to exit** by swapping the lines on relay terminals 1 and 2 of the controller or by mapping the terminals accordingly in the software.

2. Swap the access control sensor directions (if there are two of them) by swapping the lines on terminals PASS PORT1 and PASS PORT2 of the controller or by mapping the terminals accordingly in the software.
4. **When a cardholder passes through the turnstile, the system registers unauthorized access in the opposite direction (i.e., the system registers entries as break-outs).**

Swap the access control sensor directions (if there are two of them) by swapping the lines on terminals PASS PORT1 and PASS PORT2 of the controller or by mapping the terminals accordingly in the software.

5. **After unlocking (by the remote control or card), the turnstile remains unlocked until the controller is restarted (when a card is tapped on the reader, no response follows, no events are shown on the Monitoring tab, if the reader indication is connected to the controller, you will receive three short Access Denied signals).**

If the controller responds as described above, it means that one or both access control sensors of the turnstile remain activated and the controller is waiting for the completion of the access event

Follow the steps below:

1. Please make sure that the access control sensors of the turnstile are connected correctly to the Sigur system and review the settings (the connection diagrams and settings are provided in the sections dedicated to the respective turnstiles).
2. Make sure that when the turnstile is locked, both access control sensors are deactivated (both are closed or both are open, depending on the turnstile model) and check the levels at the Sigur PASS PORT1 and PASS PORT2 terminals (0V for the closed state of the sensors or 3.3V for the open state of the sensors).
6. **A break-in or break-out event is registered when access is granted from a remote control.**

Please make sure that the remote control buttons are connected to the ACS controller and not to the turnstile. If for any reason you choose not to connect the buttons to the controller, go to the access point settings and change the **Turnstile No.1 break-out response** and **Turnstile No.1 break-in response** parameters to **Register exit permitted by button** and **Register entry permitted by button** respectively.

## 16. Appendix. Sound indication of the controller

The controller can produce the following sound indications using its integrated loudspeaker.

### Sound indication of the controller.

Sequence of beeps	Frequency	Description
Short beep	Single	If the startup of the controller is successful, when it is powered on with the configured IP parameters.
Two short beeps	Single	If the startup of the controller is successful, when it is powered on without configured IP parameters.
Beep (0.5sec), pause (0.5sec)	Repeated	If the controller has started successfully, indicates one of the issues below: <ul style="list-style-type: none"> <li>• The device has switched to battery;</li> <li>• The supply voltage exceeded the tolerated range;</li> <li>• Failure of the power source battery (if the battery health control is used).</li> </ul>
Short beep, pause (~2sec)	Repeated	Hard reset has been initiated. Please wait for the process to complete.
Long beep		Hardware failure. The controller does not work properly and must be replaced.

Note: Unless otherwise specified, a long beep lasts 1sec, a short beep lasts 0.2sec and a pause between the signals lasts 0.5sec.

## 17. Appendix. LED indication of the controller

If enabled, the controller uses three-level integrated LED indication:

- MAIN is a first-level indicator that communicates basic information about the controller status.
- PWR, LNK, P1, P2, AS, FA are second-level indicators that show the detailed controller status.
- The third-level indicators are located near the inputs and outputs of the controller. They indicate the status of the respective inputs and outputs.

In the tables below, unless otherwise is indicated, “blinking” means a repetitive signal where the LED first lights up for 0.5 seconds and then is off for 0.5 seconds.

MAIN	Indication	Description
White	Solid	The device is operating normally.
	Blinking	If the controller has started successfully, indicated one of the issues below: <ul style="list-style-type: none"> <li>• No server connection (Ethernet);</li> <li>• No connection to readers (OSDP);</li> <li>• Fire alarm is activated;</li> <li>• Security alarm is activated.</li> </ul>
Yellow	Solid	The firmware is being uploaded for update.
	Blinking (0.5 sec)	The firmware of the device is being updated.
	Blinking (0.2 sec)	Hard reset is in progress.
Red	Solid	If the controller has started successfully. indicates one of the issues below: <ul style="list-style-type: none"> <li>• The device has switched to battery;</li> <li>• The supply voltage exceeded the tolerated range;</li> <li>• Failure of the power source battery (if the battery health control is used).</li> </ul>
	Blinking	Failure of the hardware. The controller does not work properly and must be replaced.
No light		No supply voltage on the controller. Check the status of the power source and / or power supply line.

Indicator	Color	Indication	Description
PWR	White	Solid	The device is operating normally.
		Blinking	If the controller has started successfully, indicates one of the issues below: <ul style="list-style-type: none"> <li>▪ The device has switched to battery</li> <li>▪ The supply voltage exceeded the tolerated range;</li> <li>▪ Failure of the power source battery (if the battery health control is used).</li> </ul>
LNK	White	Solid	Connected to the server.
		Blinking	Connection to the server is lost.
AS	White	Solid	The security system is activated and operating normally.
		No light	The security system is not activated.
		Blinking	The security system is activated and there is an alarm event / emergency.
FA	White	Solid	Emergency door release is enabled, the fire alarm cable is operating normally.
		No light	Emergency door release is disabled, the cable status is not monitored.
		Blinking	Emergency door release is enabled, the fire alarm is activated.

Indicator	Color	Indication	Description
P1/P2	White	Solid	PORT1/2 relay is active.
		No light	PORT1/2 relay is not active.
		Blinking	No connection to the reader (OSDP) assigned to control this relay.
TX	Red	X	OSDP status indicator, sending queries.
RX	Yellow	X	OSDP status indicator, receiving responses.

If the miscellaneous indicators (third-level indicators) glow GREEN, it can mean the following:

Terminals	Description
DC IN	The voltage of correct polarity is supplied to the board.
RTE, PASS, IN	0V is supplied to the input (ground).
LEDR, LEDG, BEEP, RELAY (NO COM-NC), OUT	The output is active (0V for open collector outputs, NO connected to COM for relays).
EMC UNLOCK	F+ has voltage relative to F-; the connected circuit is closed.
ALARM SENSORS	The indicator behavior is similar to the AS indicator.

## 18. Appendix. Controller configuration parameters and values

The table below lists all possible Sigur controller parameters. If you do not see any of the parameters in the controller configuration window, this can be due to the following reasons:



1. The value of this parameter cannot be changed by the user. You will see an asterisk (\*) next to these parameters. The names of the parameters in the Sigur interface appear below in italics.
2. An outdated version of the software and / or hardware of the controller is installed. In this case, install the newest versions of the software and firmware of the controller.
3. This parameter is not applicable to controllers of this model.

### Controller configuration parameters and values.

Parameter	Description	Default value, milliseconds
D0002*	Sensor activation time, i.e. how long it should remain in the new state for it to be registered by the controller.	200
D0003	Lock control pulse duration.	300
D0004	Maximum time the door can remain open, after which the controller will activate the respective indication on the reader. Delay before the Door Held Open signal.	off
D0005	Max. waiting time for the door to be opened; when expired, the controller will lock the door. Wait time for open door.	5.000
D0006*	Fire alarm activation time, i.e. how long the fire alarm should be active to trigger the emergency door release on the controller.	1.000
D0007	Duration of the control pulse on the M and S lines of a third-party gate controller. Gate control pulse duration.	500

<b>Parameter</b>	<b>Description</b>	<b>Default value, milliseconds</b>
D0008	Guaranteed idle time immediately after the start of the controller in the Gates configuration. Idle time after gate controller activation.	500
D0009*	Guaranteed delay after the pulse is sent via the M line to the third-party gate controller.	3.000
D0010*	Guaranteed delay after the pulse is sent via the S line to the third-party gate controller.	1.000
D0011	Max. time it takes for the gate wings to move from one end position to the other in third-party gate controller configurations. Max. gate opening / closing time.	60.000
D0012	Time it takes for the gate wings to move from one end position to the other when controlled directly (without limit switches). Gate opening / closing time if controlled directly.	20.000
D0013	Delay between activation of the motors of the first and second wings of the gate when controlled directly. Delay between activation of motors when controlled directly.	1.000
D0014*	Guaranteed delay between the motor shutdown and restart.	1.000
D0015	Max. idle time before the gate starts closing. The countdown starts when the gate is fully open up until the closing movement starts. Time before automated closing.	10.000
D0016	Duration of the guaranteed gate idle time after the Stop button has been released on the remote control. Delay after Stop button release.	1.000

Parameter	Description	Default value, milliseconds
D0017*	Access event registration delay. The time during which the central vehicle presence sensor has to be inactive after the activation for the access event to be registered. Delay of gate sensor activation.	5.000
D0018*	Push button activation time. The time during which the push button state shall remain unchanged to be registered by the controller.	100
D0020	Turnstile idle time before timeout for a single-time access event.	5.000
D0021	Pulse duration at general-purpose outputs.	300
D0022*	Max. Wiegand pause duration.	21
D0023*	Max. Wiegand bit length.	2
D0024	Turnstile control pulse duration.	200
D0025	Operator intervention wait time.	10.000
D0031	Turnstile through-beam sensor filter time.	30
D0032	Access Allowed / Access Denied pulse duration.	1.000
D0033	Locking delay.	0
D0039	Auto-opening of the doors after a person has entered the room (interlocking door).	60.000
D0042	Collect / Return Card pulse duration.	600
D0043	Time before closing interrupted by sensor activation resumes.	1.000
D0052	Wait time for the supervisor.	10.000
D0053	Breathalyzer wait time.	40.000

## 19. Appendix. Recommended cable choices

Cable description	Recommendations
<p>Controller power supply (from the power supply unit to the controller).</p>	<p>The following wire types can be used for internal wiring: vinyl-vinyl bare cord (vinyl-vinyl bare fire-resistant cord), flat vinyl-vinyl cord, vinyl connection cord. The following wire types can be used for external wiring: vinyl-vinyl bare cord (vinyl-vinyl bare fire-resistant cord). The cable cross-section depends on the length of the power supply line. Generally, for a 50m line and shorter, a cable with cross-section of at least 0.75mm<sup>2</sup> can be used. For longer lines, we recommend using cables with cross-section of 1.5 to 2.5mm<sup>2</sup>.</p>
<p>Power supply lines for locks</p>	<p>The following wire types can be used for internal wiring: vinyl-vinyl bare cord (vinyl-vinyl bare fire-resistant cord), flat vinyl-vinyl cord, vinyl connection cord. The following wire types can be used for external wiring: vinyl-vinyl bare cord (vinyl-vinyl bare fire-resistant cord). The cable cross-section depends on the length of the power supply line and the current consumption. Generally, for a 50m line and shorter, a cable with cross-section of at least 1.0mm<sup>2</sup> can be used. For longer lines, we recommend using cables with cross-section of 1.5 to 2.5 mm<sup>2</sup>.</p>
<p>Connection of readers to the controller (Wiegand)</p>	<p>If the readers are placed not far from the controller (up to 50m), it is recommended to use cables with cross-section of 0.22 to 0.5mm<sup>2</sup>. Any types of signal cables can be used, including indoor signal cables 8x0.5. If the readers are located far from the controller (50 to 100m), a cable with a higher cross-section value (0.75 to 1.0mm<sup>2</sup>) is recommended at least for the power supply of the reader. You can use a twisted pair cable, but the wires from different pairs must be used to connect the data lines. The second wire from each pair can be used as a power supply line (i.e., one pair = DATA0 and GND, the second pair = DATA1 and "+" terminal). Please read the instructions provided by the manufacturer of your readers carefully before connecting the devices.</p>

Cable description	Recommendations
<p>Connection of readers to the controller (OSDP)</p>	<p>Use UTP5 cable type or specialized cables (i.e., shielded PE or EPE/PVC interface cables for internal wiring or shielded PE or EPE/PE interface cables for external wiring). The existing on-site vacant communication lines can be used provided that the cable is at least Cat.3 (LAN, phone line). Never locate your communication lines in the vicinity of AC power cables or control cables for high-demand machinery. If all the installation considerations are followed, the electrical properties of the RS485 interface make it possible to build sections of communication lines up to 1,200m long.</p>
<p>Signal lines from sensors to controllers and control lines from controllers to access points</p>	<p>Use cables with the cross-section of 0.22 to 0.5mm<sup>2</sup>. You can use any types of standard signal cables, including indoor signal cables 8x0.5. It is not recommended to use twisted pairs for connection purposes. This type of cables provides increased distributed capacity between the twisted wires, which can result in lower signal transmission speed (e.g., when transmitting signals from photoelectric sensors to the controller).</p>

## 20. Appendix. Character encoding for readers with a keypad

**Wiegand 4 interface (4 bits for each keypress).**

Symbol	Code	Symbol	Code
0	0000	6	0110
1	0001	7	0111
2	0010	8	1000
3	0011	9	1001
4	0100	*	1010
5	0101	#	1011

**Wiegand HID interface (6 bits for each keypress).**

Symbol	Code	Symbol	Code
0	0 0000 1	6	1 0110 0
1	0 0001 0	7	1 0111 1
2	0 0010 0	8	1 1000 1
3	0 0011 1	9	1 1001 0
4	1 0100 1	*	1 1010 0
5	1 0101 0	#	1 1011 1

**Wiegand-Motorola interface (8 bits for each keypress).**

Symbol	Code	Symbol	Code
0	11110000	6	10010110
1	11100001	7	10000111
2	11010010	8	01111000
3	11000011	9	01101001
4	10110100	*	01011010
5	10100101	#	01001011

## 21. Contacts

For any inquiries or assistance, please contact us using the provided information.

Website: [www.sigur.com](http://www.sigur.com)

General Inquiries: [info@sigur.com](mailto:info@sigur.com)

Technical Support: [support@sigur.com](mailto:support@sigur.com)