



Controller
CT/L-14

ASSEMBLY AND OPERATION MANUAL

CE EAC



CT/L-14 Controller

Assembly & Operation Manual

CONTENTS

1	APPLICATION	3
2	OPERATING CONDITIONS.....	4
3	TECHNICAL SPECIFICATIONS	4
4	DELIVERY SET	4
4.1	Standard delivery set.....	4
4.2	Optional equipment	5
5	DESCRIPTION.....	5
5.1	Design and operation	5
5.2	Controller boards.....	6
5.3	IP-address setting	8
5.4	Input signals parameters	9
5.4.1	<i>IN1 – IN6</i> inputs	9
5.4.2	<i>DUA, DUS_t, DUB, FA</i> inputs.....	10
5.5	Output signals settings	10
5.5.1	<i>OUT1 – OUT4</i> relay outputs.....	10
5.5.2	Outputs <i>OC1, OC2</i> and <i>OC3</i>	11
5.5.3	<i>LdA, LdSt, LdB</i> outputs	11
5.6	Readers connection	11
5.6.1	Connection via <i>RS-485</i> interface.....	11
5.6.2	Connection to <i>Wiegand</i> interface.....	12
6	MARKING AND PACKAGING.....	12
7	SAFETY REQUIREMENTS.....	12
7.1	Installation safety requirements.....	12
7.2	Operation safety requirements	13
8	INSTALLATION.....	13
8.1	Cable lengths	13
8.2	Installation order.....	14
8.2.1	Controller installation.....	14
8.2.2	Door control configuration	16
8.2.3	Turnstile and electromechanical gates configuration	18
8.2.4	Vehicle checkpoint configuration	20
8.2.5	RC-panel connection.....	22
8.2.6	<i>Fire Alarm</i> device connecting	22
8.2.7	Optional equipment connection	22
9	CONFIGURATION	24
10	UPDATE OF EMBEDDED SOFTWARE.....	26
11	OPERATION.....	26
11.1	ACS operating modes	26
11.2	Indication of ACM, events and controller configurations	27
11.3	Troubleshooting	28
11.3.1	The controller does not work	28
11.3.2	Communication failure between controller and PC	28
12	MAINTENANCE.....	29
13	TRANSPORTATION AND STORAGE.....	30
	Appendix 1. Instruction on connection of the card capture reader	31
	Appendix 2. Instruction on connection of the <i>CT/L-14</i> through <i>PoE</i> -splitter.....	33
	Appendix 3. Instruction on connection of the controller for lock-chamber management	34
	Appendix 4. <i>CT/L-14</i> Controller Web-interface. User Manual	37

Dear Customer!

*Thank you for purchasing a controller manufactured by PERCo.
Please follow the instructions given in the Manual carefully,
and this quality product will provide many years of trouble-free use.*

This **Operation Manual** for the **CT/L-14 Controller** (hereinafter – the Manual) provides information on operation, installation, maintenance, storage and transportation of the **CT/L-14** controller. The Manual aims to provide correct operation of the controller and complete use of its technical capabilities. The Manual contains data on installation and maintenance, and also a reference section.

The Manual is active together with Technical description of **PERCo-Web** and also with certificates of devices connected to the controller.

Abbreviations adopted in the Manual:

- ACM – access control mode;
- ACS – access control system;
- LAN – local area network;
- OD – operating device;
- PS – power supply;
- RC– remote control;
- RTC – real-time clock;
- WRC – wireless remote control.

1 APPLICATION

CT/L-14 Controller (hereinafter – the controller) is a part of **PERCo-Web** ACS.



Attention!

The internal memory of the controller features special **PERCo-Web** Software version, allowing arranging ACS based on this controller, without a server on a separate PC.

In order to start operating the embedded ACS, the administrator is to use the system manager, to do so, enter the controller Web-interface using computer via *Ethernet* (Appendix 4, p. 2) and in browser address bar add the port number:49000 to controller IP-address (login-password for initial entering: *admin-admin*). After this Web-server and system server are to be initiated. For the future enters one can only enter the controller Web-interface and add the port number (initially :8080) to controller IP-address in browser. When entering the system for the first time, the user will be requested to create login-password pair for sanctioning subsequent system entrances.

The capabilities of **PERCo-Web** embedded security system are limited¹.

Software licensing order, settings, characteristics and operation algorithm is described in details in the operational documentation for **PERCo-Web** system. The current version of the files is available in electronic format on the **PERCo** web-site: www.perco.com, in **Support > Downloads** section.

The controller supports connection of (Sect. 5.6): up to 8 different **PERCo** readers with interface *RS-485*, up to eight *Wiegand* readers using four **AC-02.1** converters, and enables to organize up four one-way or two-way passages.

Depending on the configuration (Appendix 4, p. 4) the controller can control the following ODs:

- up to four electromagnetic or electromechanical locks that support one-way or two-way passage;
- up to two turnstiles or gates;

¹ Embedded **PERCo-Web** system limitations: number of employees – up to 500, visitors – up to 500, departments – up to 100, events – up to 1 mln, maximum number of controllers in the system – 10. Use **PERCo-Web** access control system that can be installed on a separate server for a wider range of options.

- up to two boom barriers or automatic gates of vehicle checkpoint;
- turnstile / gate or boom barrier (automatic gate) in combination with locks: the total number of ODs is max. 3 ODs.

The controller also supports the ability to control OD double-check combinations (see Appendix 3).

2 OPERATING CONDITIONS

The controller, with regard to resistance to environmental exposure complies to GOST 15150-69 category NF4 (operation in premises with climate control).

Operation of the controller is allowed at ambient air temperature from +1°C to +40°C and relative air humidity up to 80% at +25°C.

3 TECHNICAL SPECIFICATIONS

Operating voltage	12±1.2V DC
Consumption current (12V)	max. 0.25 A
Power consumption	max. 3 W
Communication interface standard	<i>Ethernet</i> (IEEE 802.3)
<i>Ethernet</i> data transfer speed	10/100 Mbps
Interface of reading devices	<i>RS-485, Wiegand</i> ¹
Number of reading devices:	
via <i>RS-485</i> interface	up to 8
via <i>Wiegand</i> ² interface.....	up to 8
Number of users	min. 50,000
Event memory capacity	up to 150,000
Number of access cards for each employee	up to 5
Number of managed ODs	up to 4 ³
Number of relay outputs for OD control	4
Number of additional “open collector” outputs	3
Number of inputs controlled by “dry contact” outputs	13
Number of remote control inputs	up to 6
Number of remote control indication outputs	6
Electric shock protection class	III (IEC 61140)
Mean lifetime	8 years
Dimensions	208×235×45 mm
Weight	max. 1.8 kg

4 DELIVERY SET

4.1 Standard delivery set

Controller	1
Jumper	9
15-18 V suppressor	4
Mounting kit:	
plastic dowel	3
screw	3
self-adhesive cable tie mount	3
nylon cable tie 100 mm	5
Package	1
Certificate	1
Operation manual	1

¹ *Wiegand* (26, 34, 37, 40, 42, 56, 58) when using **AC-02.1** interface converters.

² Up to 8 readers when using four **AC-02.1** interface converters.

³ Depending on the selected controller configuration template (see Appendix 5, p. 4).

4.2 Optional equipment

Power supply	1
PoE-splitter ¹	1
Siren	1
WRC kit ²	2
AU05 system time display	1
PERCo readers	up to 8
AC-02.1 interface converter	up to 4

5 DESCRIPTION

5.1 Design and operation

The controller is produced in the form of electronics module in metal housing with a removable cover. The cover features a power supply indication.

The controller features:

- non-volatile memory;
- non-volatile RTC-timer (real time clock);
- housing opening sensor (the “tamper switch”).

The controller is able to store in non-volatile memory:

- no less 50,000 card identifiers;
- up to 150,000 events in the event log with the date and time of the event³.

The controller provides:

- connection via Ethernet (*IEEE 802.3*) interface;
- support of *TCP/IP* protocol suite (*ARP, IP, ICMP, TCP, UDP, DHCP*);
- support of application layer of communications protocol of **PERCo-Web** system;
- updating of embedded software via *Ethernet*.

By default, the controller features:

- unique MAC-address (specified in the certificate and on the item board);
- IP-address (specified in the certificate and on the item board);
- Subnet mask (255.0.0.0);
- gateway IP-address (0.0.0.0).

Following ways to set up IP-address, gateway and subnet mask are provided at the stage of system configuration:

- operation with default settings;
- manual input;
- receipt from DHCP server.

It is possible to connect the following equipment:

- up to eight readers via *RS-485* interface;
- up to eight readers via *Wiegand* interface;
- up to four door sensors (reed switches);
- up to four passage sensors (PASS outputs of the turnstile);
- up to four RC buttons (“Exit”) for the lock;
- up to two turnstile (gate) RC-panels;
- up to ten devices sending commands to additional inputs;
- **AU05** system time display;
- *Fire Alarm* emergency unlocking (emergency passage opening) device.

¹ PoE-splitter – allows energizing the controller via *Ethernet* network. Splitter can be used with network switches that support *PoE* technology and that are compatible with *IEEE 802.3af* standard.

² WRC kit consists of a receiver and transmitters (fobs) with operating range of up to 40 m.

³ In case of event log overflow the oldest events will be replaced with the new ones (events are deleted by blocks consisting of 256 events).

As a part of ACS, the controller provides:

- operation in ACM: “Open”, “Control”, “Security” ¹, “Closed”;
- saving the set mode in the non-volatile memory in order to avoid the turn-off of the mode in case of power failure;
- support of local and global control of zonality, double-check and verification;
- connection of light and sound alarm devices;
- possibility of arming and disarming of the protected zone;
- sending alarm notifications to the central surveillance panel.

5.2 Controller boards

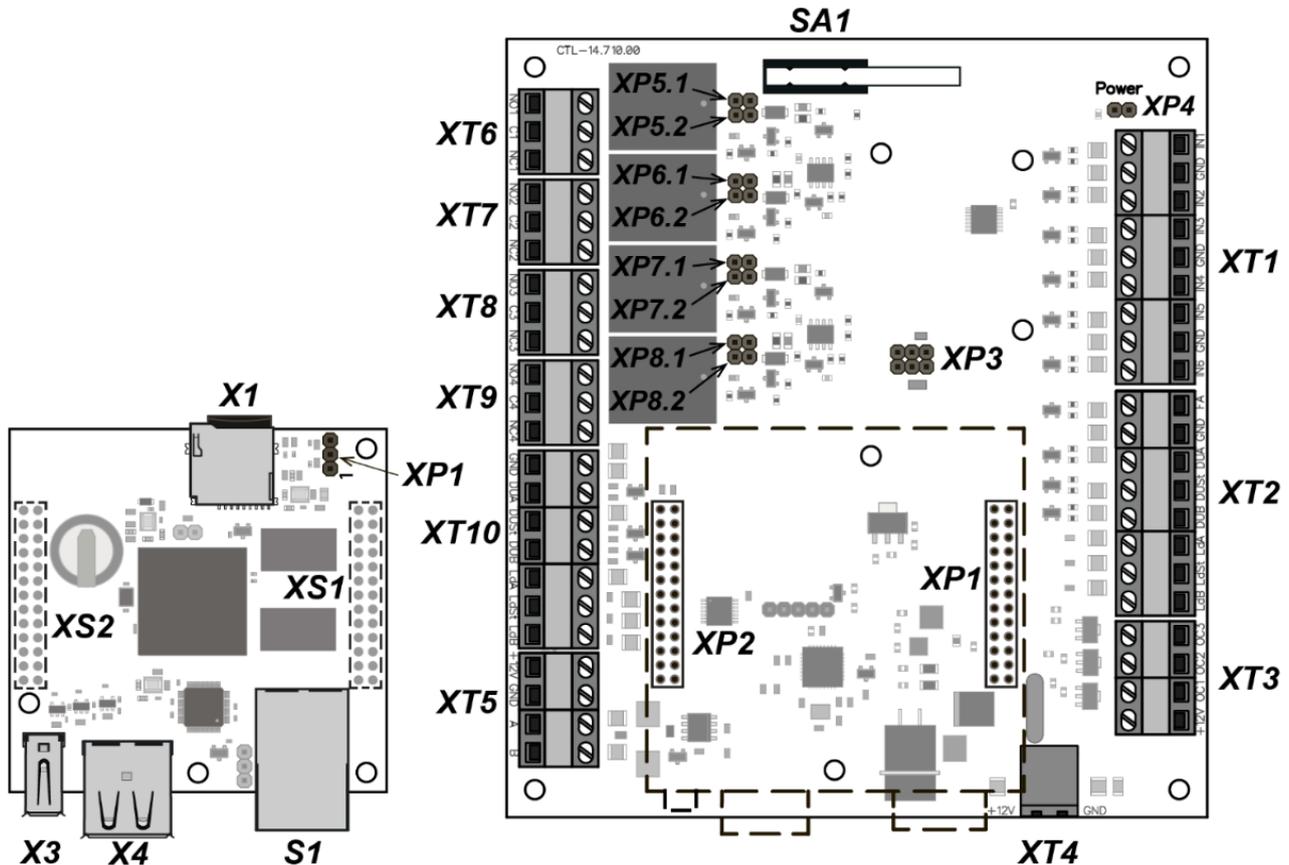


Figure 1. The upper and lower controller boards

The controller features two boards – upper board (processor module) and lower board (process execution module). The **XS1 – XS2** terminal blocks of the upper board are connected to the **XP1 – XP2** connectors of the lower board. The controller boards are shown in Fig. 1. The terminal blocks application is given in the Table 1.

The upper board of the controller features:

- **X1** – microSD-card slot;
- **S1** – connector for the *Ethernet* cable;
- **X3** – connector for USB0 equipment;
- **X4** - connectors for USB1 and USB2 equipment;
- **XP1** – connector to choose the method of the IP-address of the controller; by default, the jumper is not installed - user mode (Sect. 5.3);
- **XS1, XS2** – connectors for connecting to the lower board.

The lower board of the controller features:

- **XP1, XP2** – connectors for connecting to the upper board;

¹ The mode “Security” is available only for “Controller for lock control” configurations and connected **CL-201** lock controllers.

- **XP4** – power indicator connector on the controller housing;
- **XP5.1, XP5.2 – XP8.1, XP8.2** – connectors (in pairs) to select the type of connected lock (see Sect. 8.2.2):
 - jumpers are removed – standard electromechanical or electromagnetic lock is to be connected to the corresponding output,
 - jumpers are installed – locks of **LB-** or **LBP-**series are without installed door sensor (reed switch). The controller traces the passage on condition of the contact group of the lock.

Table 1. Lower board terminal blocks designation

Contact	Contact name in the Web-interface	Designation	
XT1 (IN) connector			
<i>IN1</i>	In 1	"Door sensor #1" or "Input for PASS A signal from the turnstile #1"	
<i>GND</i>	–	"Common"	
<i>IN2</i>	In 2	"Door sensor #2" or "Input for PASS B signal from the turnstile #1" or "Additional input IN #2"	
<i>IN3</i>	In 3	"Door sensor #3" or "Input for PASS A signal from the turnstile #2" or "Additional input IN #3"	
<i>GND</i>	–	"Common"	
<i>IN4</i>	In 4	"Door sensor #4" or "Input for PASS B signal from the turnstile #2" or "Additional input IN #4"	
<i>IN5</i>	In 5	"Additional input IN #5"	
<i>GND</i>	–	"Common"	
<i>IN6</i>	In 6	"Additional input IN #6"	
XT2 (RC1) connector			
<i>FA</i>	<i>FA</i>	"Input for emergency unlocking (passage opening) <i>Fire alarm</i> "	
<i>GND</i>	–	"Common"	
<i>DUA</i>	<i>DUA 1</i>	"Control input of the OD1 from the RC-button" or "Control input of direction A from the RC-panel #1"	
<i>DUS_t</i>	<i>DUS_t 1</i>	"Input STOP from the RC-panel #1" or "Additional input IN #8"	
<i>DUB</i>	<i>DUB 1</i>	"Control input of the OD2 from the RC-button" or "Control input of direction B from the RC-panel #1" or "Additional input IN #9"	
<i>LdA</i>	<i>LdA 1</i>	"Output for indication of direction A on the RC-panel #1"	
<i>LdSt</i>	<i>LdSt 1</i>	"Output for indication STOP on the RC-panel #1"	
<i>LdB</i>	<i>LdB 1</i>	"Output for indication of direction B on the RC-panel #1"	
XT3 (OC) connector			
<i>OC3</i>	OK3	"Additional output OUT #7 (open collector)"	
<i>OC2</i>	OK2	"Additional output OUT #6 (open collector)"	
<i>OC1</i>	OK1	"Additional output OUT #5 (open collector)"	
<i>+12V</i>	–	"Output of +12VDC power for outputs OC1, OC2 and OC3"	
XT4 (+12VDC) connector			
<i>+12V</i>	–	"Input of controller + 12VDC power from external PS"	
<i>GND</i>	–		
XT5 (RS-485) connector			
<i>+12V</i>	–	"Output of +12VDC power for readers"	
<i>GND</i>	–		
<i>A</i>	–	"Connection of line A via RS-485"	
<i>B</i>	–	"Connection of line B via RS-485"	
XT6 (OUT1) connector			
<i>NO1</i>	<i>NO1/C1/NC1</i>	normally open contact	"Relay control output OD #1"
<i>C1</i>		central contact	
<i>NC1</i>		normally closed contact	

Contact	Contact name in the Web-interface	Designation	
XT7 (OUT2) connector			
NO2	NO2/C2/NC2	normally open contact	“Relay control output OD #2” or “Additional output OUT #2”
C2		central contact	
NC2		normally closed contact	
XT8 (OUT3) connector			
NO3	NO3/C3/NC3	normally open contact	“Relay control output OD #3” or “Additional output OUT #3”
C3		central contact	
NC3		normally closed contact	
XT9 (OUT4) connector			
NO4	NO4/C4/NC4	normally open contact	“Relay control output OD #4” or “Additional output OUT #4”
C4		central contact	
NC4		normally closed contact	
XT10 (RC2) connector			
GND	–	“Common”	
DUA	DUA 2	“Control input of the OD3 from the RC-button” or “Control input of direction A from the RC-panel #2” or “Additional input IN #10”	
DUS _t	DUS _t 2	“Input STOP from the RC-panel #1” or “Additional input IN #11”	
DUB	DUB 2	“Control input of the OD4 from the RC-button” or “Control input of direction B from the RC-panel #2” or “Additional input IN #12”	
LdA	LdA 2	“Output for indication of direction A on the RC-panel #2”	
LdSt	LdSt 2	“Output for indication STOP on the RC-panel #2”	
LdB	LdB 2	“Output for indication of direction B on the RC-panel #2”	

5.3 IP-address setting

The way of IP-address setting is selected by installing or removing the jumper on **XP1** connector on the controller upper board.

Following ways of IP-address setting are possible (see Table 2):

1. User mode. Jumper is removed.
 - If the user does not change the IP-address (gateway, subnet mask), the controller operates with default settings: IP-address and MAC-address are specified in the certificate of IP-stile and on the controller board; subnet mask is 255.0.0.0; gateway IP-address is 0.0.0.0.
 - If the user changes the IP-address (gateway, subnet mask), the controller starts operating with the new settings immediately without switching the power supply.



Note:

It is possible to change network settings of the controller on PC via Web-interface or software. The controller and PC must be on the same subnet.

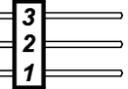
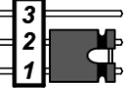
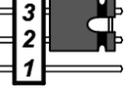
2. “IP MODE”. Jumper is in the position 1–2.
 - Operation in networks with dynamic allocation of IP-addresses, the controller can receive IP-address (gateway, subnet mask) from DHCP-server.
3. “IP DEFAULT”. Jumper is in the position 2–3.
 - The controller operates with default settings: IP-address and MAC-address are specified in the certificate of IP-stile and on the controller board; subnet mask is 255.0.0.0; gateway IP-address is 0.0.0.0.
 - To access the controller, the password is not required. Installing the jumper into the “IP DEFAULT” mode allows changing the password.



Note:

User settings of IP-address (gateway, subnet mask), if they were set, are saved during the switch into “IP DEFAULT” mode. The controller will operate with them at next turn-on, if jumper is not installed.

Table 2. Jumper installation on *XP1* connector

N	Jumper position on <i>XP1</i>	Method of specifying IP address
1	<i>XP1</i> 	User mode
2	<i>XP1</i> 	"IP MODE"
3	<i>XP1</i> 	"IP DEFAULT"

5.4 Input signals parameters

5.4.1 *IN1* – *IN6* inputs

The controller provides status control of four inputs controlled by “dry contact” or “open collector” (OC): *IN1* – *IN6*. Connection to the outputs is performed via *XT1* terminal block of the controller lower board (Fig. 1 and 3).



Note:

To create a high-level signal on all input contacts *IN1* – *IN6*, 2 kOhm resistors connected to +3.3V power line are used.

Inputs can be used for following connections:

- *IN1*:
 - door sensor 1 (reed switch),
 - PASS output of a turnstile 1,
 - intrusion detectors of a vehicle checkpoint 1;
- *IN2*:
 - door sensor 2 (reed switch),
 - PASS output of a turnstile 1,
 - optional equipment (IN #2);
- *IN3*:
 - door sensor 3 (reed switch),
 - PASS output of a turnstile 2,
 - intrusion detectors of a vehicle checkpoint 2,
 - optional equipment (IN #3);
- *IN4*:
 - door sensor 4 (reed switch),
 - PASS output of a turnstile 2,
 - optional equipment (IN #4);
- *IN5, IN6*:
 - optional equipment (IN #5, IN #6).

Signals activation depends on description of their default status in **Normal status of contact** parameter in *PERCo-Web* software:

- If the input is described as **Open**, it is activated by a turn-on of low-level signal relative to *GND* contact. In such case a normally open relay contact or an open collector output circuit may be a control element.
- If input is described as **Closed**, it is activated by a turn-off of low-level signal relative to *GND* contact. In such case a normally closed relay contact or an open collector output circuit may be a control element.



Note:

- *IN1* input is configured as “Closed” by default.
- If according to the configuration of the controller *IN2, IN3* or *IN4* input is used to connect the door sensor / intrusion detectors / PASS, by default it is configured as **Closed** with the possibility of further changes.

“Relay contact” control element is to provide following signals characteristics:

Minimum commutating current	max. 1 mA
Closed contact resistance (with resistance of the connection cable)	max. 300 Ohm

Circuit control element with open collector output is to provide following signals characteristics:

Voltage at the closed contact (low-level signal at input of the controller)	max. 0.8 V
---	------------

5.4.2 DUA, DUS_t, DUB, FA inputs

The controller provides status control of four inputs under control of “dry contact” or “open collector” (OK): *DUA*, *DUS_t*, *DUB*, *FA*. Connection to the inputs is performed via **XT2** and **XT10** terminal blocks of the controller lower board.



Note:

To create a high-level signal on all input contacts *DUA*, *DUS_t*, *DUB*, *FA*, 1 kOhm resistors connected to +3,3V power line are used.

Inputs can be used for following connections:

XT2 terminal block:

- *FA*: emergency unlocking devices (passage opening) *Fire Alarm*,
- *DUA*: button “A” on the RC-panel #1 (WRC #1) or RC-button for OD1,
- *DUS_t*: button “Stop” on the RC-panel #1 (WRC #1) or optional equipment (IN #8),
- *DUB*: button “B” on the RC-panel #1 (WRC #1) or RC-button for OD2 or optional equipment (IN #9).

XT10 terminal block:

- *DUA*: button “A” on the RC-panel #2 (WRC #2) or optional equipment (IN #10),
- *DUS_t*: button “Stop” on the RC-panel #2 (WRC #2) or optional equipment (IN #11),
- *DUB*: button “B” on the RC-panel #2 (WRC #2) or optional equipment (IN #12).

Activation and signals characteristics of the control element are specified in the Sect. 5.4.1.



Notes:

- Input *FA* is uniquely configured as “Closed”.
- Input *DUA* is uniquely configured as “Opened”.
- If according to the configuration of the controller input *DUS_t* or *DUB* used to connect RC-buttons, it is uniquely configured as “Opened” without any possibility being modified.

5.5 Output signals settings

5.5.1 OUT1 – OUT4 relay outputs

The controller is equipped with four *OUT1* – *OUT4* relay outputs. Connection to the outputs is performed via **XT6** – **XT9** terminal blocks of the controller lower board. Each output has a complex group of contacts: normally open *NO*, normally closed *NC* and common output *C*.

Outputs may be used for (Fig. 3):

- *OUT1*: as a control output of OD #1;
- *OUT2*, *OUT3*, *OUT4*:
 - as a control output of OD #2, OD #3 and OD #4,
 - as outputs to control optional equipment (*OUT #2*, *OUT #3*, *OUT #4*).

Output signals characteristics:

Maximum commutating voltage of direct current	max. 30 V
Maximum commutating voltage of alternating current	max. 42 V
Maximum commutated direct/alternating current	max. 5 A
Resistance of closed contact	max. 0.15 Ohm

Control outputs support potential and pulse operating modes of OD. Selection of mode is performed with **Operating mode of control output** parameter of OD.

In **potential** mode of OD:

- In case of single passage relay output is activated for a period of time, set in software by **Holding in unlocked state period** software parameter or till the moment of end of passage.
- In case OD is set into “Open” mode relay output is activated till the mode change.

In **pulse** mode of OD:

- In case of single passage relay output is activated for a period of time, set by **Control pulse duration** parameter of OD. In such case OD remains unlocked until the passage is performed.
- In case OD is set into “Open” mode output is activated for a period of time, set by **Control pulse duration** parameter of OD, and after that it will be activated each time for the same period in one second after the normalization of OD.

Activation of *IN1 – IN4* inputs, configured as door sensor or signal PASS, define that the passage was performed in the set direction.

5.5.2 Outputs *OC1*, *OC2* and *OC3*

The controller is equipped with two “open collector” outputs: *OC1*, *OC2* and *OC3* (in configuration OUT #5, OUT #6, and OUT #7, Fig. 3). Connection to the outputs is carried out via **XT3** terminal block of the controller lower board. +12VDC supply is derived to the same terminal block for easy connection.



Note:

The maximum current through this block must not exceed 0.5A.

Outputs can be used for following functions:

- connection of light and sound alarm devices,
- sending alarm notifications to central surveillance panel,
- connection of other optional equipment.

Output signals characteristics:

Maximum commutation voltage of direct current	max. 30 V
Maximum commutated current	max. 0.25 A

5.5.3 *LdA*, *LdSt*, *LdB* outputs

The controller is equipped with three “TTL” type outputs: *LdA*, *LdSt*, *LdB*. Connection must be performed through the **XT2** terminal block contacts of the controller lower board.

Outputs can be used (Fig. 3):

- **XT2** terminal block: as outputs of connection of indication of the RC-panel #1,
- **XT10** terminal block: as outputs of connection of indication of the RC-panel #2.

Output signals characteristics:

- Maximum voltage of direct current max. 3 V
- Maximum current max. 0.01 A

5.6 Readers connection

5.6.1 Connection via *RS-485* interface

Readers, card capture readers, **AI-01** display unit with infrared-receiver and **AU-05** system time display are connected to the controller via *RS-485* interface. *RS-485* interface communication line is to be connected to all devices consequently.

End-of-line resistors of 120 Ohms are to be mounted at the ends of the communication line of *RS-485* interface. On the products with built-in end-of-line resistor, which are not end devices of the communication line, it is necessary to cut the “*disconnection of end-of-line resistor*” jumper with wire cutters. The position of jumper is indicated in the operational documentation of a specific product. If the controller is located at one of the ends of the communication line, the end-of-line resistor of 120 Ohms is to be installed between A and B contacts of **XT5** terminal block.

When connecting to RS-485 interface, follow the instructions of the connected device and the layout presented in Fig. 3. To connect a communication line of RS-485 to the controller, the #2 cable type is to be applied (Table 3).

Following variants of reader connection are possible (Fig. 3):

- Up to eight **IR03.1**, **IR04.1**, **IR10** card readers (in any combination).
- One or two **IR04**, **IRP01** readers (in any combination) and correspondingly together with up to seven or six **IR03.1**, **IR04.1** or **IR10** card readers (in any combination).
- Up to eight **MR07.1** card readers.
- Up to two **IR07** card readers.
- One or two indication blocks with **AI01** IR-receiver to any of the above options.



Note:

+ 12V and **XT5** terminal block GND contacts can be used in order to power the readers, provided that max. load current must not exceed 0.5 A.

When installing readers (card capture readers, indication blocks), different numbers (addresses) are to be set, otherwise readers with the same addresses will not work. The number (address) is determined by the state of the “reader number” jumper (jumpers) on the case or on the product board (see the operational documentation for this product).

5.6.2 Connection to *Wiegand* interface

When using the **AC-03** interface converter, up to four readers with the Wiegand interface can be connected to the controller, and when using four **AC-02.1** converters, up to 8 readers can be connected. The connection layout and description of the reader indication in this case are given in the operational documentation for the interface converter.



Note:

To power the readers, one can use the +12 V and terminal blocks GND contacts of the **AC-03 (AC-02.1)** interface converter, while the total current consumption of the readers must not exceed 0.5 A.

6 MARKING AND PACKAGING

The marking label of the controller is placed on the back plate of the housing. The marking label provides following information concerning the controller:

- trade mark and contact details of the manufacturer;
- name and number of model;
- serial number;
- date and month of manufacture;
- allowed power voltage range;
- consumption current.

The controller board contains labels with default MAC-address and IP-address of the controller.

The controller is packed into a paperboard box, preventing it from damages during transportation and storage.

7 SAFETY REQUIREMENTS

7.1 Installation safety requirements

Installation and technical maintenance of the controller should be performed by qualified staff, after getting acquainted with the Operation manual and safety rules. Installation should be performed in accordance with general electrical and work safety rules.

**Attention!**

- All connections and jumper installations should be carried out only when the equipment is powered off and power supply is disconnected.
- During mounting use only proper tools.
- Cabling should be performed in accordance with general requirements for electrical equipment.
- Do not use the controller if it is not properly installed and connected.

7.2 Operation safety requirements

Operation should be performed in accordance with general electrical and work safety rules.

**Do not use!**

- The controller under conditions that do not comply with the requirements of Sect. 2 of this Manual.
- The controller at supply voltage that does not comply with the requirements of Sect. 3 of this Manual.
- The device in hostile environment that contains acids, alkalis, oils etc.

Power supply should be used accordingly to safety rules given in the Operation manual.

8 INSTALLATION

Installation should be performed in accordance with work safety noted in Sect. 7.1.

Installation should be done in accordance with local building requirements.

8.1 Cable lengths

Cables for installation are shown in Table 3.

Table 3. Cables used for installation

N	Equipment	Cable length, m, max	Cable type	Cross section, mm ² min.	Cable example
1	Ethernet (IEEE 802.3)	100	Four twisted pairs (starting from Category 5)	0.2	4×2×0.52 F/UTP2-Cat5e
2	Reader, card capture reader, AI-01 indication block CL-201 lock controller, AU-05 system time display	50 (total) 1200 (total)	Twisted pairs (starting from Category 5)		2×2×0.52 F/UTP2-Cat5e
3	Power source	10	Twin cable	0.75	Flat cord with sheath and outer sheath of PVC
4	RC-button ("Exit"); Door sensor (reed switch); Additional equipment	30	Twin cable	0.2	RAMCRO SS22AF-T 2x0.22 CQR-2
5	Remote control	40	Eight-core cable	0.2	CQR CABS8 8x0.22c
7	Lock	30	Double-core cable	0.75	PVC twin cable 2×0.75
8	Turnstile	30	Six-core cable	0.2	CQR CABS6 6x0.22c
9	Vehicle checkpoint	30	Four-core cable	0.2	CQR CABS4 4x0.22c

Recommendations:

- Mounting of communication lines should comply with *EIA/TIA RS-422A/485* standards.
- Do not lay cables at a distance less than 50 cm from a source of electromagnetic interference.

- Crossing of all cables with power cables is allowed only at a right angle.
- Cable growth is to be performed by soldering only.
- All cables, entering controllers, should be fixed with plastic ties to self-adhesive cable tie mount, included into delivery set and installed inside the housing. Lay and fix cables using plastic fixing brackets, if necessary.
- After cables are laid, check if there are no line breaks and short circuits at all lines.
- It is not allowed to lay lock power cables, detector cables, remote control cables and reader cables at a distance more than 1 m from ground cables.

8.2 Installation order

Connection to the controller is performed in accordance with layout shown in Fig. 3 - 11 with the use of cables from Table 3. The terminal blocks positioning on the controller's board is presented in Fig. 1.

Installation of connected devices (turnstiles, locks, power supply, etc.) is performed according to the instructions given in technical documents of corresponding devices.

8.2.1 Controller installation

1. Unpack the box and check completeness of package contents according to Sect. 4. Make sure that the equipment is not mechanically damaged.
2. Determine the place for installation of the controller. Location of the controller should comply with operating conditions. When choosing a location, make sure that it will be convenient to perform service maintenance of the controller.



Attention!

Do not install the controller at a distance less than 1 m from a source of electromagnetic interference.

3. Mark and drill holes in the surface to install the controller and connect cables in accordance with Fig. 2. Lead the communication cables, power cables and *Ethernet* cables to the location.

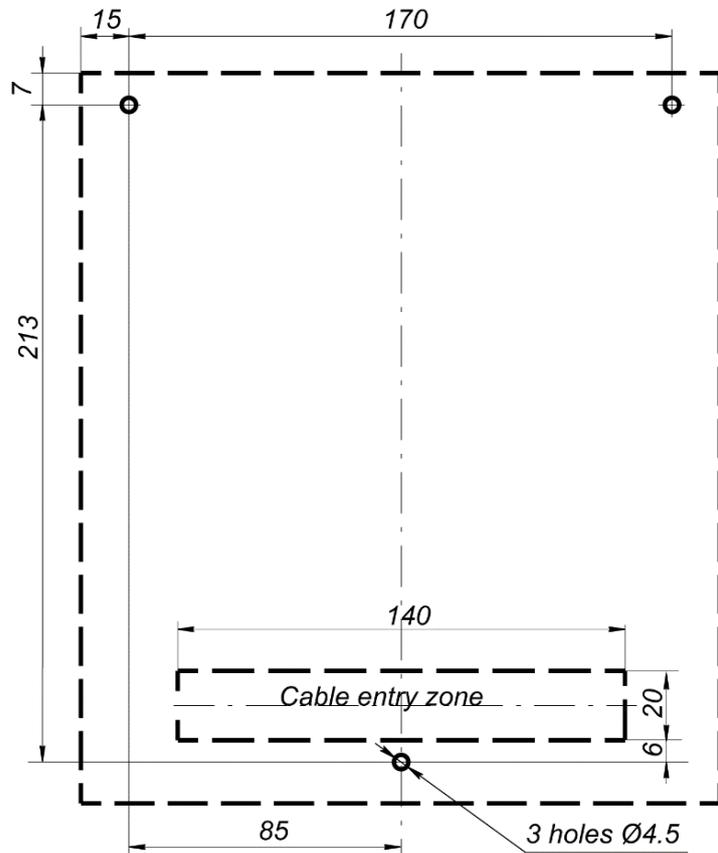


Figure 2. Hole marking for controller installation

4. Fix the controller with three screws through holes in the controller housing (use dowels from the delivery set, if necessary).
5. Select the way to set IP-address of the controller (Sect. 5.3) and install a jumper on **XP1** connector in accordance with the Table 2), if necessary.
6. Connect *Ethernet* cable to **X2** connector of the controller upper board.
7. Connect power source cable to **XT4** terminal block of the controller lower board in accordance with the layout, shown in Fig. 3.



Note:

The order of power supply connection of the controller via *PoE*-splitter is described in Appendix 2.

8. Connect necessary equipment to *RS-485* controller interface (Sect. 5.6).

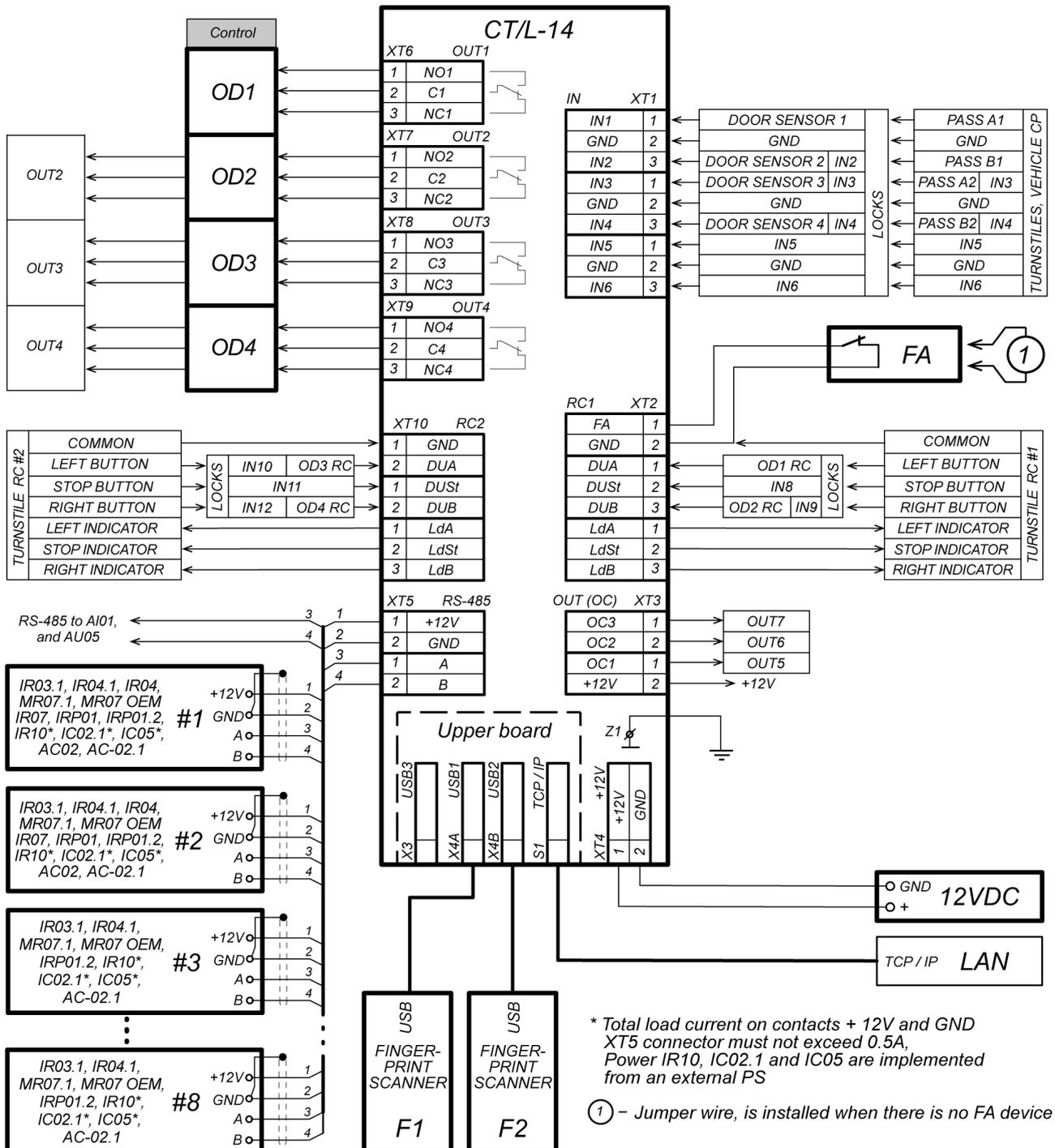
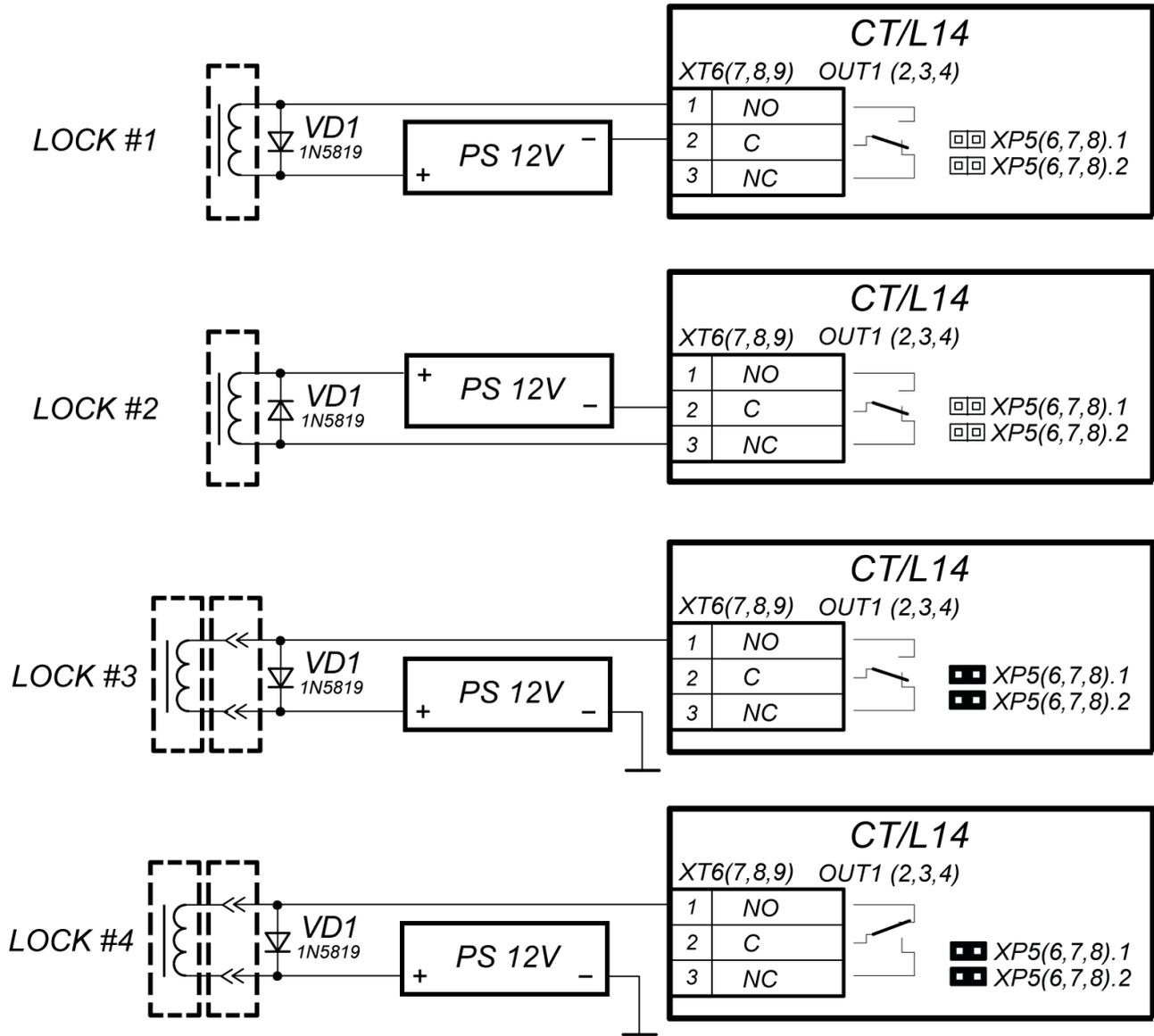


Figure 3. Common connection layout

9. Connect the rest of necessary equipment:
- electromechanical (electromagnetic) locks (Sect. 8.2.2);
 - turnstile (Sect. 8.2.3);
 - vehicle checkpoint (Sect. 8.2.4);
 - RC-panel (WRC) (Sect. 8.2.5);
 - emergency unlocking devices *Fire Alarm* (Sect. 8.2.6);
 - other optional equipment (Sect. 8.2.7).

8.2.2 Door control configuration



Examples of connections:

LOCK #1 - normally closed electromechanical lock that opens when power is supplied.

LOCK #2 - normally open electromechanical / electromagnetic lock that closes when power is supplied.

LOCK #3 - normally closed lock series LB (LBP), that opens when power is supplied.

LOCK #4 - normally open lock series LB (LBP), that closes when power is supplied.

(«Normal state of the CLOSED» parameter of the output of OD must be in the value "Energized").

Figure 4. Lock connection layout

When connecting the lock (latch) to the controller, follow the next recommendations:

1. To dissipate static electricity, it is recommended to ground the housing or locking bar of the lock. In case of lock installation on a metal door, it is recommended to ground the door leaf. It is necessary to use the cable with cross section of min. 0.75 mm².



Attention!

- If the connected lock *is not equipped with built-in spark protection circuit*, it is necessary to use the suppressor from the delivery set or Schottky diode for operating current not less than 1A (1N5819). The suppressor is to be installed close to the lock (**VD1** in Fig. 4).
- If the connected electromagnetic lock *is not equipped with demagnetizing circuit*, it is necessary to install a bidirectional suppressor from the delivery set (**VD1** in Fig. 4).
- If the controller is connected via *PoE-splitter*, it is recommended to use only electromechanical locks with spark protection diodes (**VD1** in Fig. 4), type 1N5819. The use of suppressor in such case is **FORBIDDEN**.

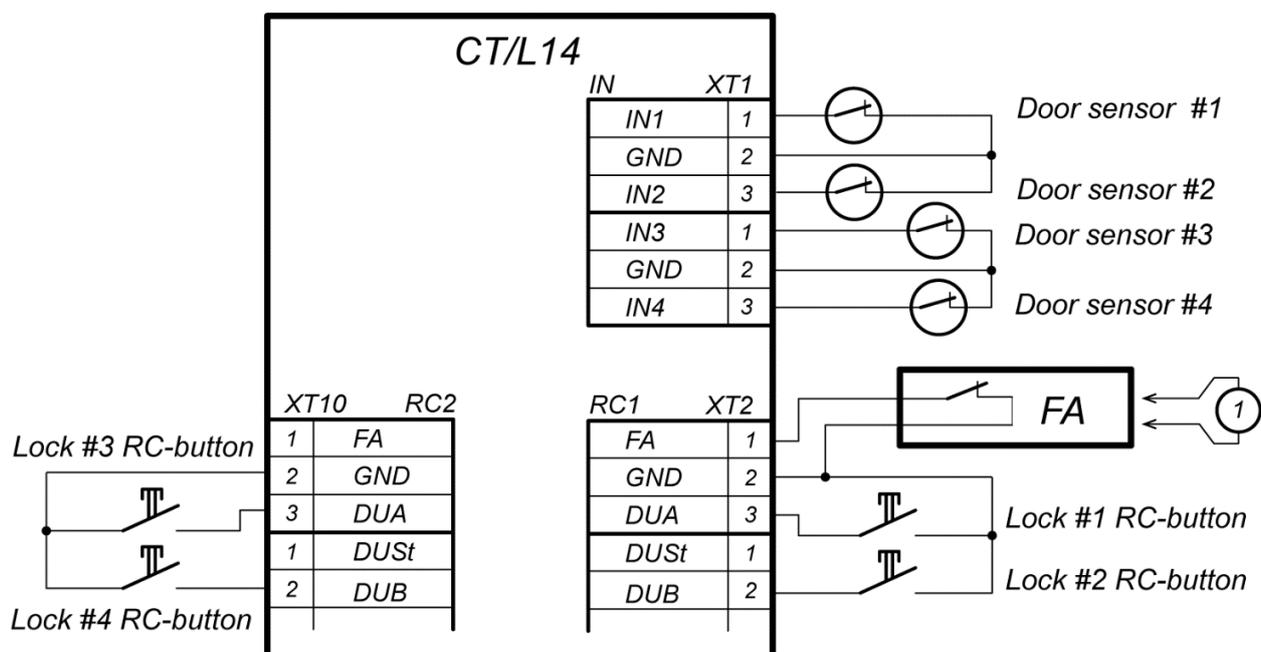
2. Connection of the lock (the latch) to **XT6** or **XT9** terminal blocks on the lower board of the controller is performed in accordance with layout (Fig. 3 - 5).
3. If connection of an “Exit” lock RC button is required, connect it to **XT2 (XT10)** of controller lower board (Fig. 5).
4. The reed switch is connected to **XT1** terminal block of the lower board (Fig. 5). The door sensor with the lock controlled by **OUT1** is connected to **IN1** input, **OUT2** to **IN2**, etc. The door sensor is to be mounted so as the door is closed, the sensor can always actuate.



Note:

LB-, LBP-series locks do not require mounting the door sensor (the **CT/L14** controllers can trace the door opening based on the contact group of the lock). In this case, it is necessary to install jumpers on the controller lower board: for **OUT1 – XP5.1** and **XP5.2**, for **OUT2 – XP6.1** and **XP6.2**, for **OUT3 – XP7.1** and **XP7.2**, for **OUT4 – XP8.1** and **XP8.2** (Fig. 1).

5. **Fire Alarm** emergency devices are connected to **XT2** terminal block of the controller lower board (in this case it is necessary to cut the jumper by wire cutters), Fig. 5 and Sect. 8.2.6.
6. Fix cables with plastic ties to self-adhesive cable tie mount, included into delivery set by installing them inside of the controller housing.



① – jumper wire, is installed when there is no FA device

Figure 5. Connection layout for RC-buttons and door sensors

8.2.3 Turnstile and electromechanical gates configuration

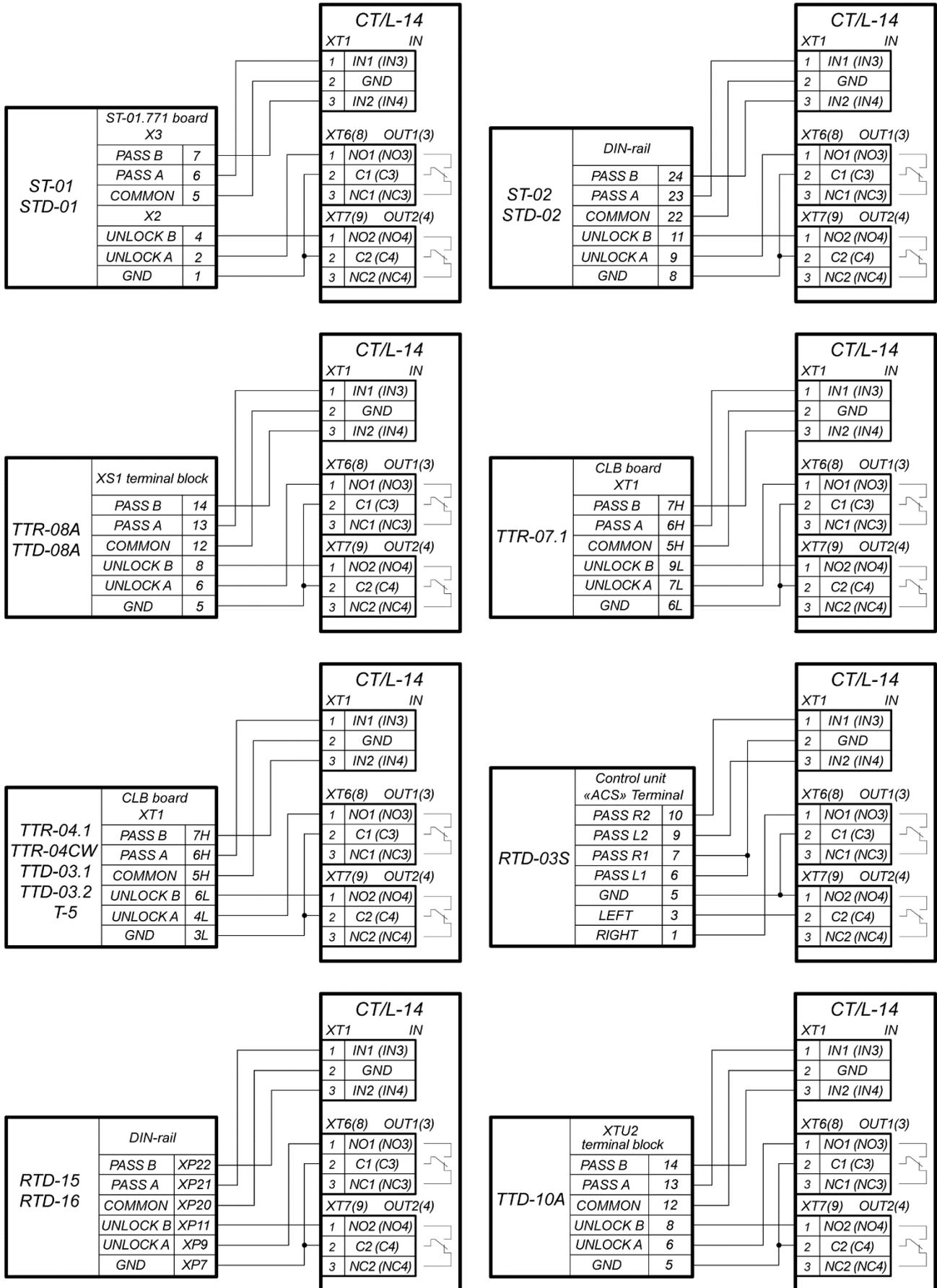


Figure 6. Connection layouts of "Turnstile control" configuration



Note:

- The **Device output operating mode OD** parameter is to be in **Potential** for **PERCo** turnstiles.
- The **Registration of the passage after ID card presentation OD** parameter is to be in **Yes** for **WMD-05S** and **WMD-06** swing gate.

Follow the next recommendations to connect the turnstile (the gate) to controller:

1. To dissipate static electricity, it is recommended to ground the turnstile housing. It is necessary to use the cable with cross section of minimum 0.75 mm².



Note:

Connection layout of power circuit of the controller and the turnstile (the gate) in case of connection via *PoE*-splitter is given in Fig. 17.

2. Connect the turnstile (the control unit of the turnstile) #1 to **XT1**, **XT6**, **XT7** terminal blocks of the controller lower board in compliance with the layout (Fig. 6).
3. Connect the turnstile (the control unit of the turnstile) to **XT1**, **XT8**, **XT9** terminal blocks of the controller lower board in compliance with the layout (Fig. 6).
4. Connect the swing gate (the control unit of the turnstile) to **XT1**, **XT6**, and **XT7** terminal blocks of the lower board of the controller in compliance with the layout (Fig. 7).
5. Connect the swing gate (the control unit of the turnstile) to **XT1**, **XT8**, and **XT9** terminal blocks of the lower board of the controller in compliance with the layout (Fig. 7).
6. Connect RC-panel (or WRC) #1 to **XT2** terminal block of the lower board of the controller in compliance with the layout (Fig. 10).
7. Connect RC-panel (or WRC) #2 to **XT10** terminal block of the lower board of the controller in compliance with the layout (Fig. 10).
8. Fix cables with plastic ties to self-adhesive cable tie mount, included into delivery set, by installing them inside the controller housing.

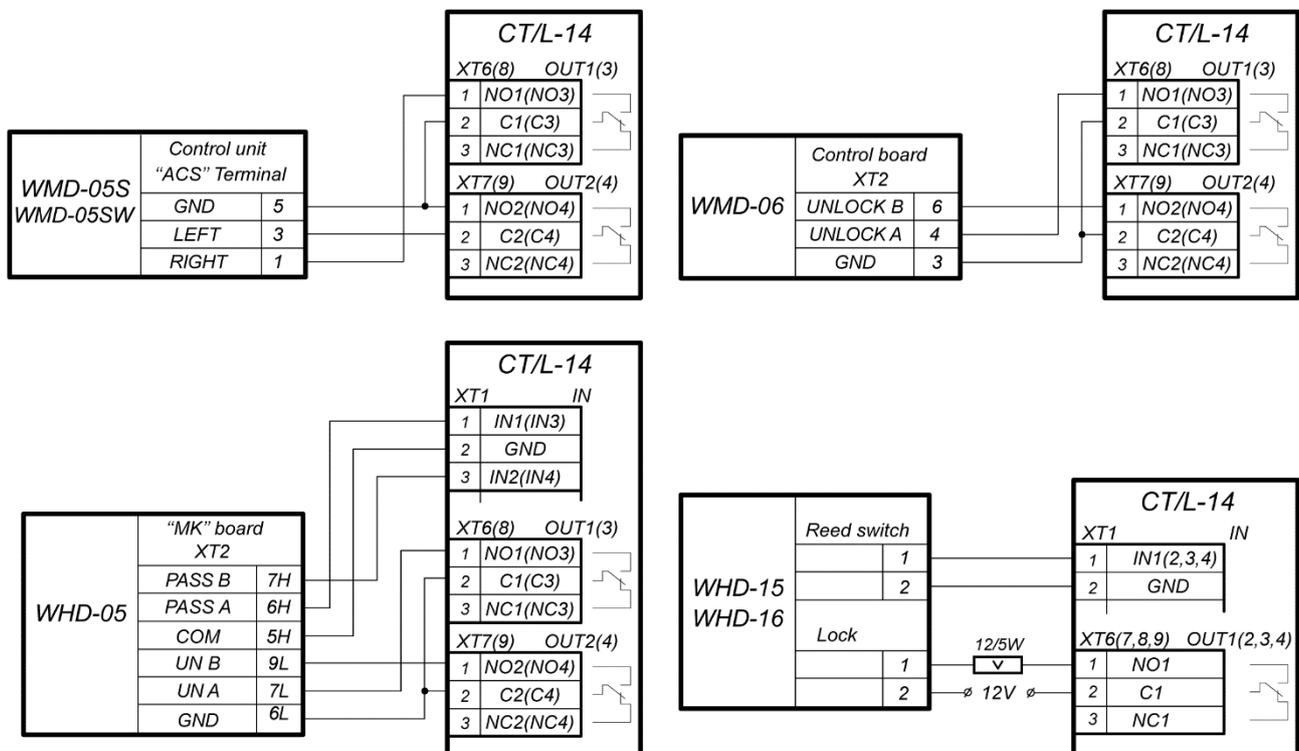


Figure 7. Connection layouts of the gates

8.2.4 Vehicle checkpoint configuration

When installing a controller, it is necessary to correspond with operation logic of control unit of vehicle checkpoint (in parentheses – the output number for vehicle checkpoint #2):

- Operation of control unit of vehicle checkpoint is performed via two relays – when passage is allowed *OUT1 (OUT3)* relay is activated and held, sending “Open” signal. After a vehicle has passed through the checkpoint (detected by intrusion detector), or after waiting period is over, *OUT1 (OUT3)* relay switches to normal, after that *OUT2 (OUT4)* relay is activated for 1 sec, sending “Close” signal. Also, *OUT2 (OUT4)* relay is activated for 1 sec by **Close** button of RC-panel.
- If **Automatic closing** function is turned on in the control unit of vehicle checkpoint OD, operation from vehicle checkpoint is performed via one relay. When passage is allowed *OUT1 (OUT3)* relay is activated and held, sending “Open” signal. After a vehicle has passed through the checkpoint (detected by intrusion detector), or after waiting period is over, *OUT1 (OUT3)* relay switches to normal, after that boom barrier is closed automatically (it is recommended to set a minimum possible waiting period for automatic closing). In such case *OUT2 (OUT4)* relay is not used.

Connection of vehicle checkpoint OD to the controller is performed in accordance with instructions, given in technical documents of corresponding devices. Follow the following recommendations (the positioning of the terminal blocks on the controller board, Fig. 1):

1. To dissipate static electricity, it is recommended to ground the housing of the OD. Grounding should be performed with a cable with cross section of min. 0.75 mm².
2. General connection layouts of vehicle checkpoint OD are given in Fig. 8.



Notes:

- **Output normalization** parameter of OD should be set into **After closing** mode.
 - If operation is performed via one relay, **Automatic closing** function should be turned on in the control unit of vehicle checkpoint OD, in such case a minimum waiting period for automatic closing is to be set - **Regulation T.C.V.** (for CAME) and **PAUSE TIME** (for NICE).
3. Connect intrusion detector to **XT1** terminal block of the lower board of the controller in accordance with the layout, shown in Fig. 9. Use cable #4 for connection (Table 3). If several sensors are connected, their outputs should be turned on successively.

For *CAME* and *GENIUS* boom barriers infrared safety sensors should be used as intrusion detectors, connected to the control unit of vehicle checkpoint ODs in a standard way. In such case they are connected to the controller of vehicle checkpoint with parallel connection.

For *NICE* and *FAAC* boom barriers the general principle of connection of infrared sensor to the controller of vehicle checkpoint is depicted in examples of connection layouts for control unit of corresponding model. Instead of **VD1** diode some other decoupling circuit might be necessary.



Attention!

- To ensure correct passage detection of a vehicle with a trailer or other parts transparent for intrusion detectors, it is recommended to install several spaced-apart detectors, or to set value of **Recovery delay of intrusion detector** parameter sufficient for passage of transparent part of a vehicle by the detector.
 - If there is no intrusion detector, it is necessary to tick **Absence of intrusion detector** parameter box in the software. In such case malfunction of OD of vehicle checkpoint is possible, due to the impossibility to choose the optimal passage period.
4. Fix cables with plastic ties to self-adhesive cable tie mount, included into delivery set, by installing them inside the housing of the controller.

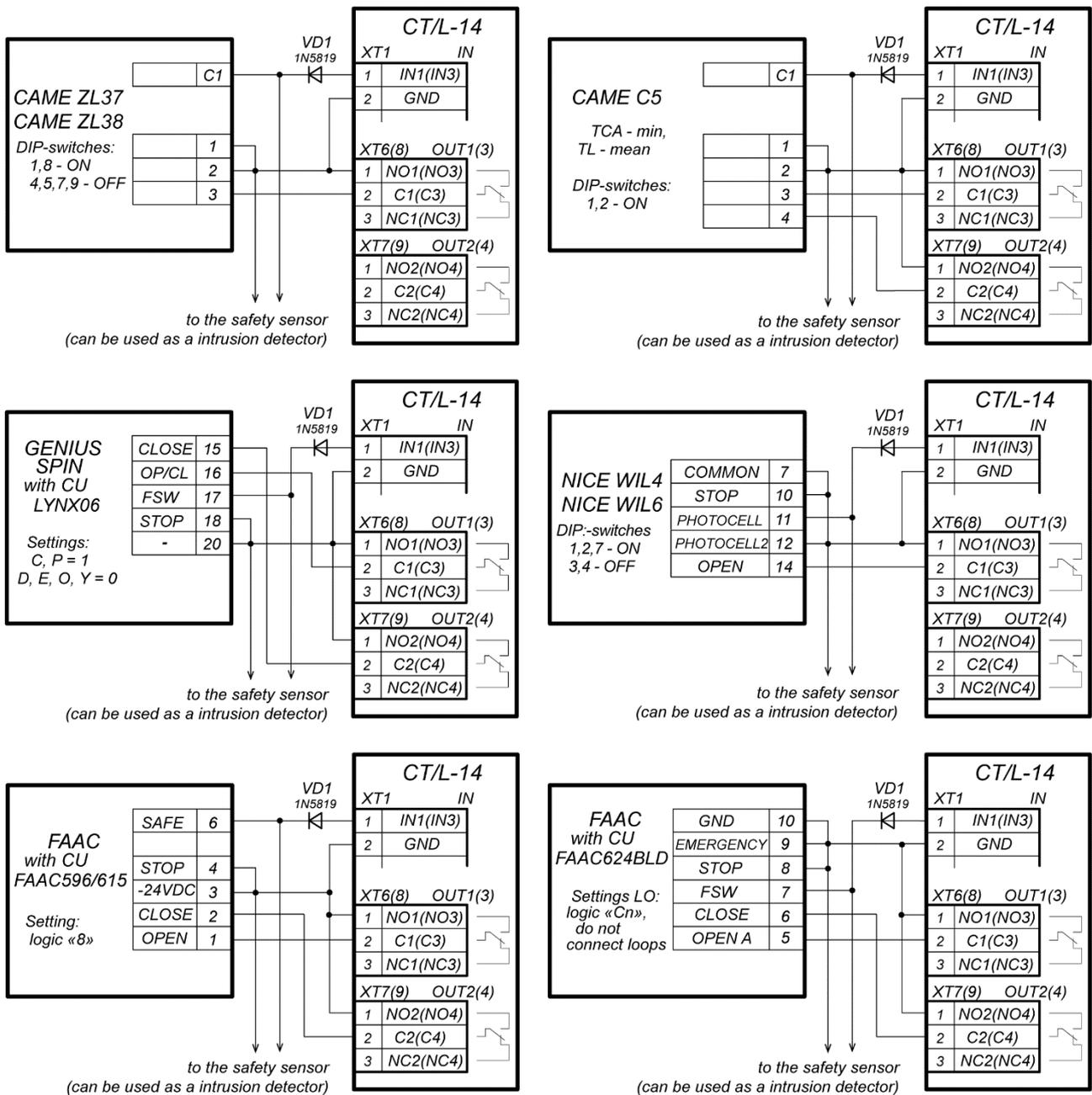


Figure 8. Connection layouts of boom barriers to the controller of vehicle checkpoint

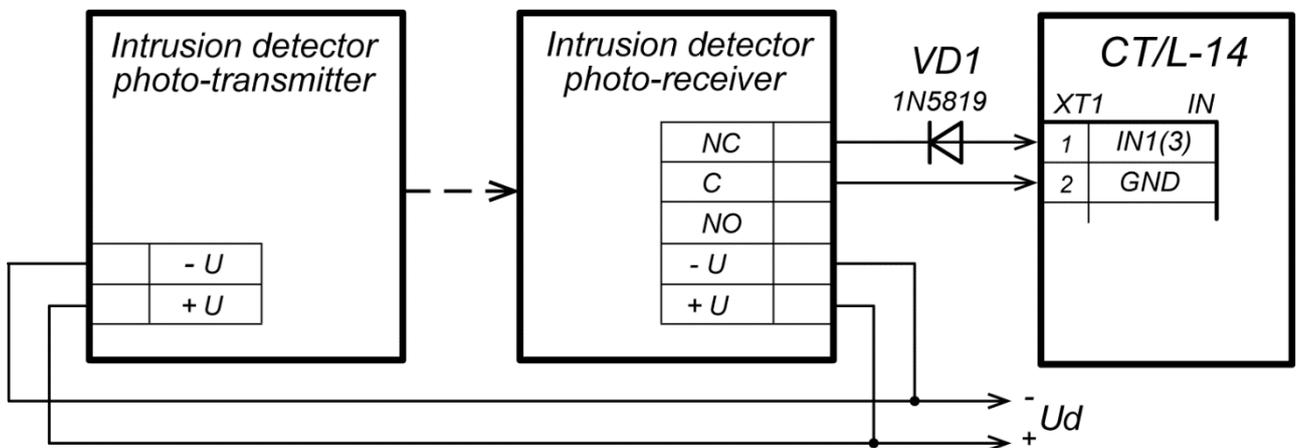


Figure 9. Connection layout of intrusion detectors

8.2.5 RC-panel connection

The controller in the relevant configuration allows connecting up to two RC-panels to control turnstiles, swing gates or vehicle checkpoint ODs. To connect each RC-panel to the controller the following inputs can be used:

- Three inputs to control the passage: *DUA, DUS_t, DUB*;
- Three outputs to control the RC-panel indication: *LdA, LdSt, LdB*.

The RC-panel #1 is to be connected to the contacts of the **XT2** terminal block, the RC-panel #2 is connected to the contacts of the **XT10** terminal block (Fig. 10).

The *DUA, DUS_t* and *DUB* inputs in these configurations of the controller are activated by low-level signals (normally open contact) relative to *GND* contact. Signal settings that can be used for connection of the RC-panel are specified in Sect. 5.4.2 and 5.5.3.

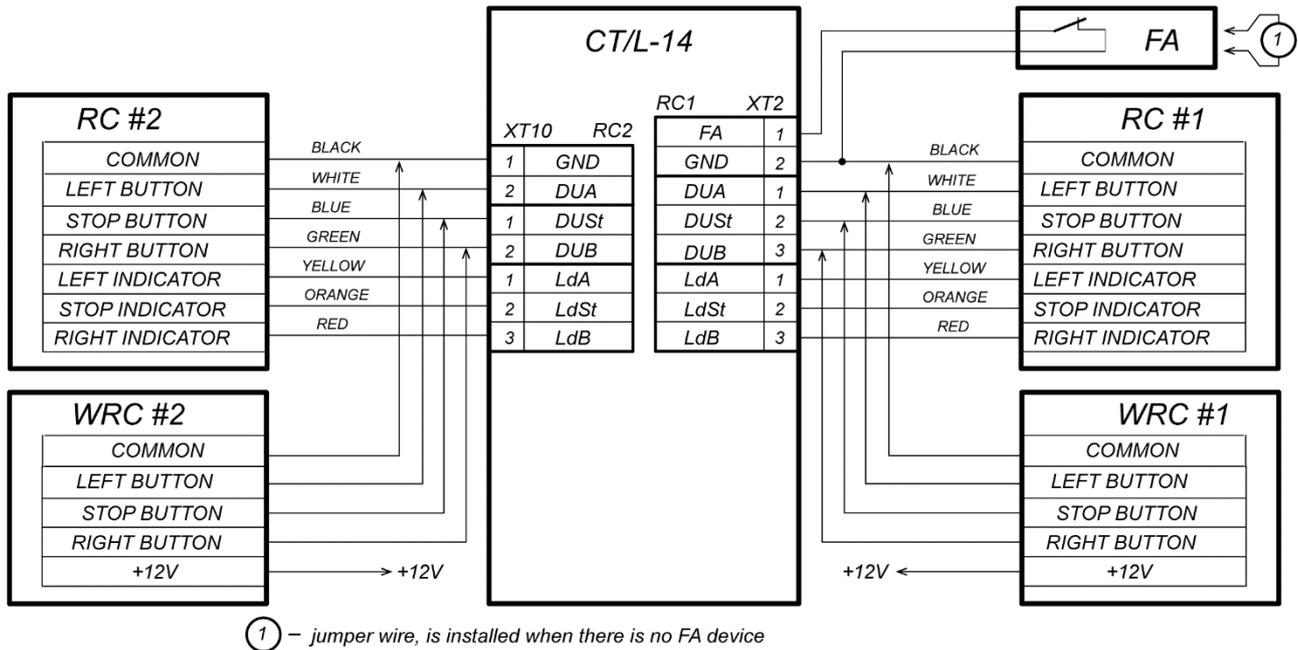


Figure 10. Connection layout of RC-panel or WRC of “Turnstile control” and “Vehicle checkpoint control” configurations

8.2.6 Fire Alarm device connecting

In case of fire alarm or other emergency situation, there is possibility of automatic unlocking (passage opening) of all ODs connected to the controller board and the controllers of the second level except ODs which are in “Security” operating mode (the possibility of emergency unlocking is to be configured at the configuration).

Emergency release (emergency passage opening) of ODs is produced by the command of the *Fire Alarm* emergency device. The *Fire Alarm* emergency device is connected to the *FA* input of the controller (*FA* contacts and *GND* of **XT2** terminal block contacts, Fig. 3, 5, 10). If the device *Fire Alarm* is not used, wire jumper (installed by default) is to be installed at the input. Settings for *FA* signal are indicated in Sect. 5.4.2. When the control signal is applied to the *FA* input, the controller operates in the *Fire Alarm* mode. In this mode, all connected devices open for passage in both directions. Other control commands are ignored.

8.2.7 Optional equipment connection

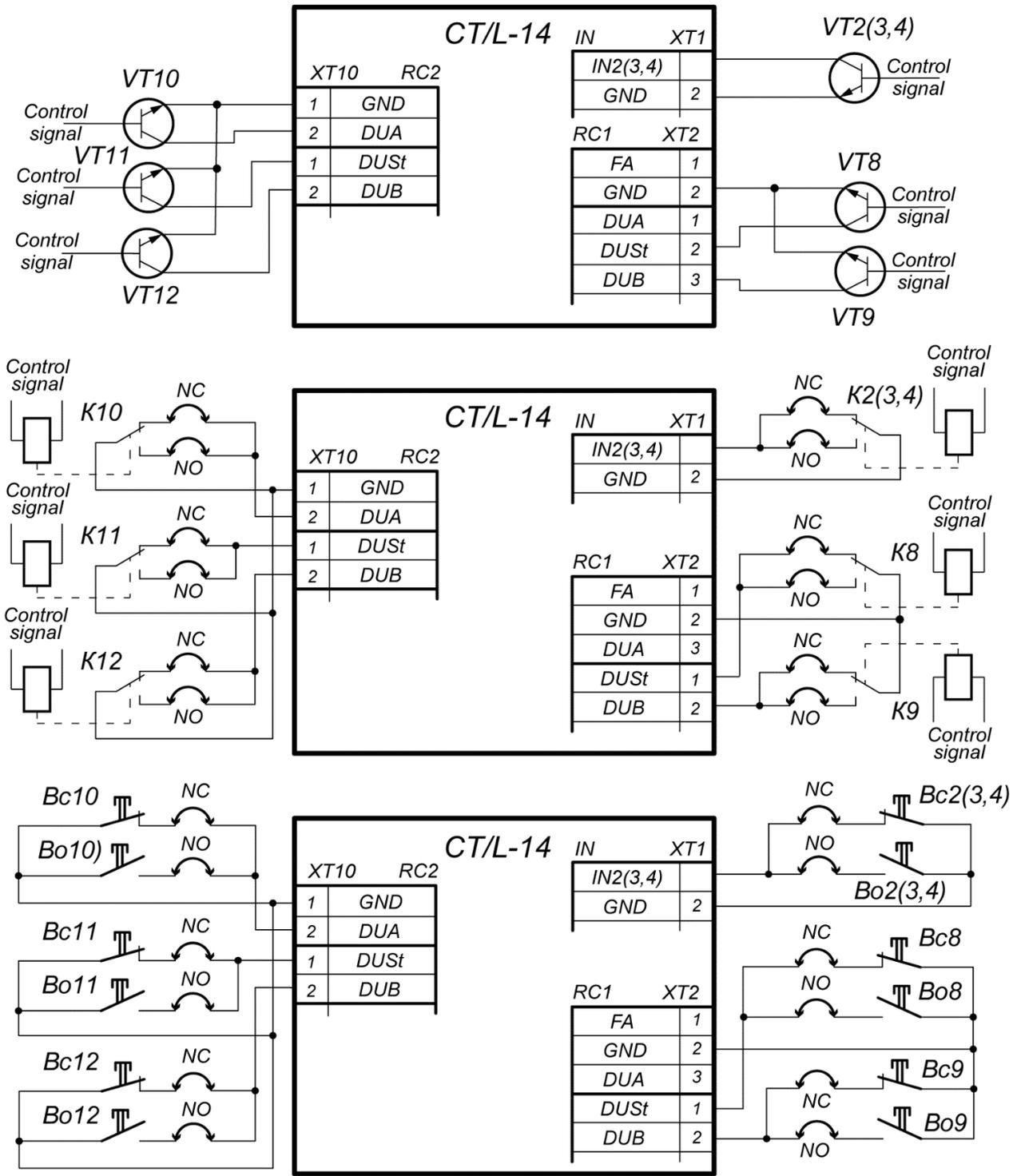
To connect optional equipment, follow the following recommendations:

1. The typical connection layouts of the optional equipment are shown in Fig. 11, 12, 13.
2. To connect the optional equipment, use cable type #4 (Table 3).
3. Fix cables with plastic ties to self-adhesive cable tie mount, included into delivery set, by installing them inside the controller housing.



Attention!

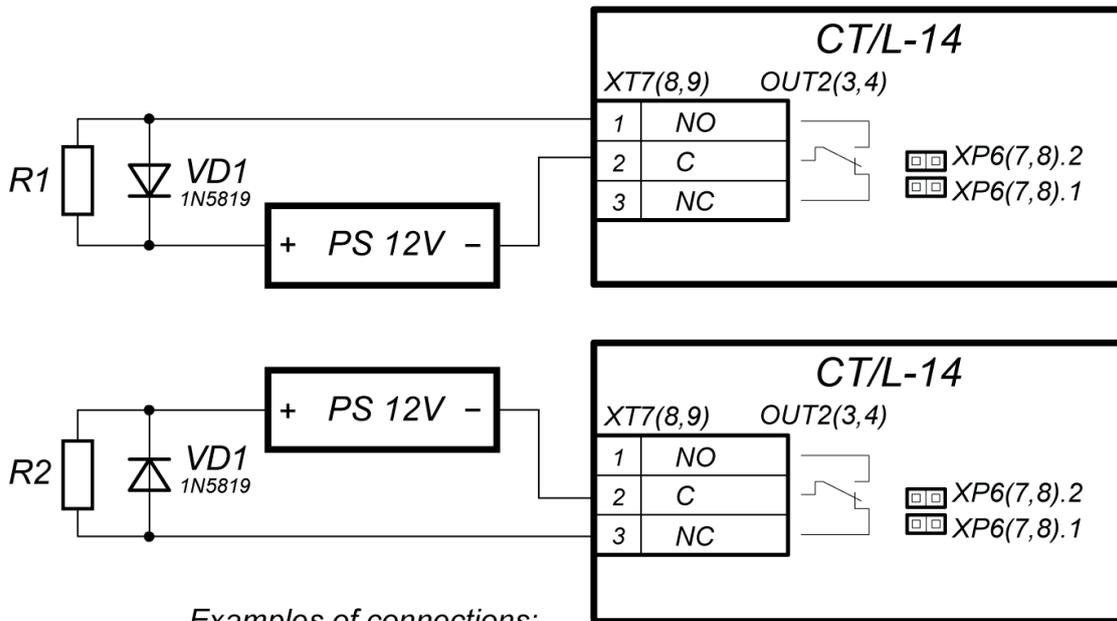
To connect the optional equipment with inductive load (R_n) to the outputs, it is necessary to use spark protection diode (**VD1** in Fig. 12). For example, Schottky diode for operating current of min. 1A (1N5819).



Connection versions:
 NC - if the input is configured as "normally closed";
 NO - if the input is configured as "normally open".

Connection examples for:
 VT - n-p-n transistor control;
 K - relay control;
 Bc - control of a normally closed button;
 Bo - control of a normally open button.

Figure 11. Connection layout of optional equipment to controller inputs



Examples of connections:
 R1 - optional equipment is activated when the power is applied
 R2 - optional equipment is activated when the power is removed

Figure 12. Connection layout of optional equipment to relay outputs

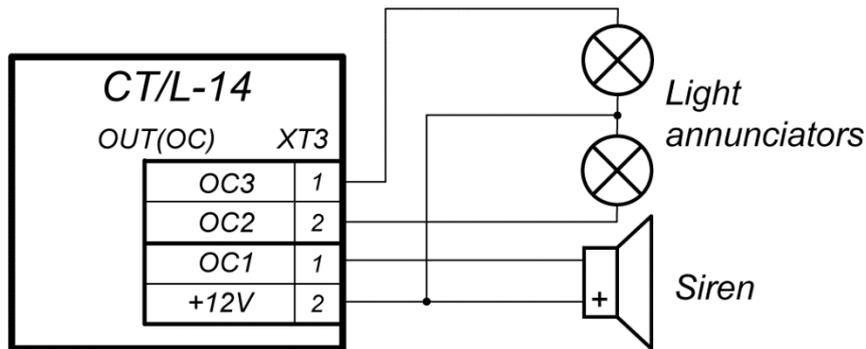


Figure 13. Connection layout of optional equipment to “Open collector” outputs

9 CONFIGURATION

The principal controller configuration (setting the configuration, adding and removing controllers of the second level and optional readers) is possible only via the controller Web-interface (Appendix 4).

The controller configuration order:

- 1 Verify all connections (Sect. 8.2). Connect the power supply to the circuit with voltage and frequency indicated in its operational documentation. Turn on the power source, the LED indication is to light up on the controller housing. It means that the controller is switched on.
- 2 Connect to the controller Web-interface via *Ethernet* network (Appendix 4, p.2).



Note:

The computer should be in the same subnet with the controller. At first turn-on, it might be necessary to change network settings of the computer. The controller is equipped with IP-addresses from 10th subnet by default. Add IP-address: 10.x.x.x (x- random numbers) and subnet mask 255.0.0.0. to TCP/IP additional settings of the computer. No such servers or services like DNS and WINS are required. After turn-on network settings of the controller can be changed to settings recommended by system administrator in the software or via the Web-interface.

- 3 Via the Web-interface perform the initial configuration of the controller according to the connected equipment:
 - select the controller configuration template, see Appendix 4, p. 4.1;
 - if necessary, add to the configuration lock controllers of the optional readers, Appendix 4, p. 4.2.
- 4 Further configuration of the controller and devices connected to it can be changed either via Web-interface or with optional software installed on the computer:
 - Network software **PERCo-Web**.

You can buy optional software from official **PERCo** distributors. Also, specified software, the procedure of his licensing and electronic versions of the operation manual are available on the website of the company **PERCo** <http://www.perco.com> in the **Support > Software** section.



Attention!

The internal memory of the controller features special **PERCo-Web** software version, allowing arranging ACS based on this controller, without a server on a separate PC.

In order to start operating the embedded ACS, the administrator is to use the system manager, to do so, enter the controller Web-interface using computer via *Ethernet* (Appendix 4, p. 2) and in browser address bar add the port number:49000 to controller IP-address (login-password for initial entering: *admin-admin*). After this Web-server and system server are to be initiated. For the future enters one can only enter the controller Web-interface and add the port number (initially :8080) to controller IP-address in browser. When entering the system for the first time, the user will be requested to create login-password pair for sanctioning subsequent system entrances.

The capabilities of **PERCo-Web** embedded security system are limited¹.

Software licensing order, settings, characteristics and operation algorithm is described in details in operational documentation for **PERCo-Web** system. The current version of the files is available in electronic form at **PERCo** web-site: www.perco.com, in **Support > Downloads** section.

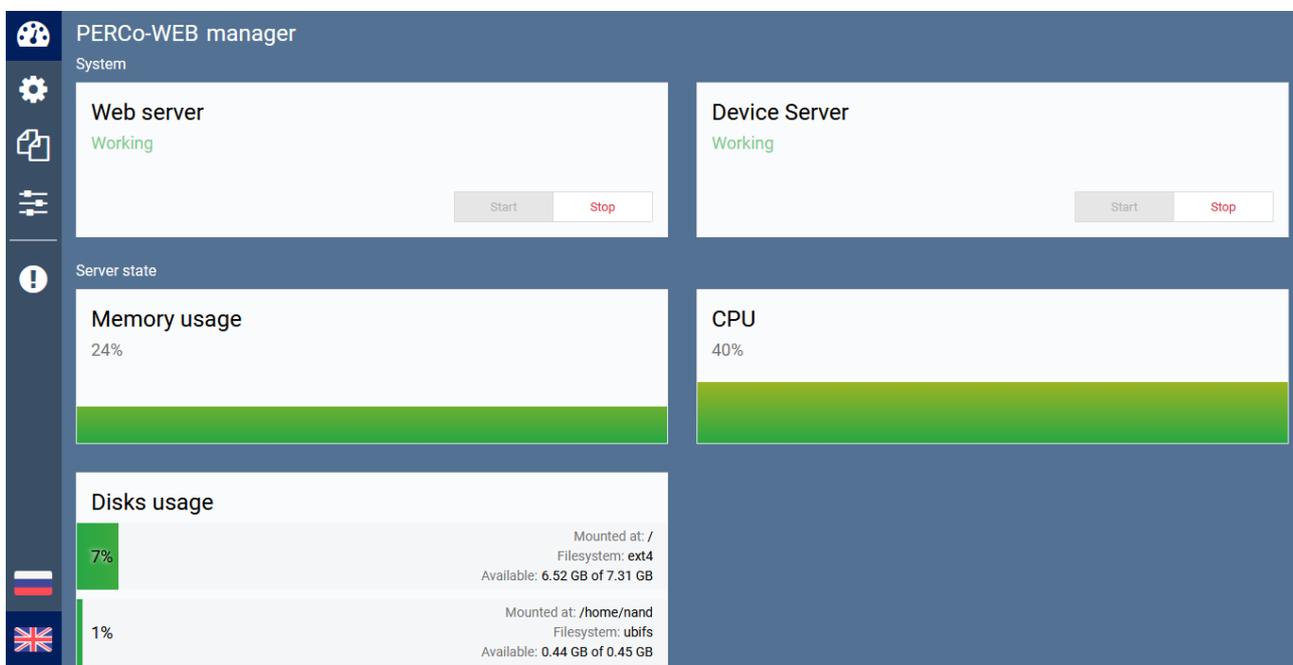


Figure 14. Interface of the PERCo-Web system manager integrated in the controller

¹ Embedded **PERCo-Web** system limitations: number of employees – up to 500, visitors – up to 500, departments – up to 100, events – up to 1 mln, maximum number of controllers in the system – 10. Use **PERCo-Web** access control system that can be installed on a separate server for a wider range of options.

10 UPDATE OF EMBEDDED SOFTWARE

Update the embedded software and format the memory is possible using the controller Web-interface in the **Diagnostic** section (Appendix 4, p.9).

11 OPERATION

When operating the controller, follow the safety measures indicated in Sect. 7.2.

After the configuration, the controller can operate in the following modes:

Without connection to the security system server.

If connection to *Ethernet* network and PC is also unavailable, the controller can perform the following functions:

- Reads identifiers of the presented cards sent from the reader, and grants or denies access, depending on their presence in the list.
- Controls connected ODs.
- Arms and disarms the protected zone; controls alarm line and ODs in “*Security*” mode; activates additional outputs in “*Alarm*” mode.
- Records events in the event log in the controller memory.
- Supports functions of local location monitoring, T&A and double-check access.

If the controller is connected to the network and other controllers of the system, the function of global location monitoring is available.

When connected to the security system server.

Besides those that are supported in the stand-alone mode, the following functions are available:

- Data from event log are automatically transferred to the database on security system server.
- Availability of verification function depends on installed extensions of network software.

11.1 ACS operating modes

The change of operating mode is carried out by the command of software or Web-interface.



Note:

- In configuration “*Controller for one two-way lock*” and “*Controller for vehicle checkpoint*” should be made simultaneously for both directions.
- Operating mode in “*Controller for turnstile*” configuration versions is to be set independently for each direction

The following ACM are provided by the controller, that operates as a part of ACS, (ACM indication is given in the Table 4):

“*Open*” operating mode – free passage mode.

- OD remains unlocked until the operating mode is changed.
- Pressing the buttons of RC-panel and RC-button (“*Exit*”) is ignored.

“*Control*” operating mode – basic operating mode as a part of ACS.

- OD is locked.
- When an access granting card is presented to the reader, OD is unlocked for **Holding in unlocked state period**.

“*Closed*” operating mode – passage denial mode.

- OD remains locked until the operating mode is changed.
- Pressing the buttons of RC-panel and RC-button (“*Exit*”) is ignored.
- When a card is presented, an access violation event is registered.

“*Security*”¹ operating mode.

- OD remains locked until the operating mode is changed.
- Pressing the buttons of RC-panel is ignored.

¹ Operating mode is available only for “*Controller for the locks*” configuration and for connected **CL-201** lock controllers.

- Protected zone is armed including the selected OD.
- Passage through the OD (forced entry) sets the system into the “Alarm” mode.

11.2 Indication of ACM, events and controller configurations

Connected to the controller remote readers and indication blocks display the indication of ACMs, states and responses of the controller upon presented identifiers. See Table 4 for possible indication variants.



Note:

- When reading an access control card in any operating mode, an audible signal of 0.2 seconds is performed, yellow indicator changes its state for 0.2 seconds. The state of the other indicators is not changed.
- After the access is granted, indication is turned on for **Holding in unlocked state period** or until the passage is performed. When access is denied indication is turned on for 1 second.

Table 4. Controller indication

Card presentation		ACM	Indicators			
			Green	Yellow	Red	Sound
Configuration is not selected		No	5 Hz	5 Hz	5 Hz	off
Activation of the <i>Fire Alarm</i> input		Any card	1.3/0.2 ¹	off	off	off
No		“Open”	on	off	off	off
		“Control”	off	on	off	off
		“Security”	off	1 Hz	1 Hz	off
		“Closed”	off	off	on	off
Card is not authorized for access		“Open”	on	off	off	0.2 sec
		“Control”	off	off	on	0.5 sec
		“Security”				
Any card		“Closed”				
Card is authorized for access		“Open”	on	off	off	0.2 sec
		“Control”	off	off	on	0.5 sec
		“Security”				
Card is authorized for access and for arming/disarming		“Open”	on	off	off	0.2 sec
		“Control”				
		“Security” ²				
Re-presenting a card with the right to arming	Change to the “Security” mode	“Security”	off	1 Hz	1 Hz	0.2 sec
	In case of failure ³ (before to return to initial mode)	“Open”	off	off	1 sec	1 sec
		“Control”				
Waiting for verification		Any	off	2 Hz	off	0.2 sec

¹ Blinking (going off briefly) – 1.3 seconds is on, 0.2 seconds is off.

² In the “Security” mode after presentation of access card with the right to disarming the following occurs: OD disarming and OD unlocking for **Holding in unlocked state period**. After this time expires, the OD switches to the operating mode set before OD arming (“Open” or “Control”, if the previous mode was “Closed”, it will switch to the “Control” operating mode).

³ Sound and light indication turns on for 1 sec.

11.3 Troubleshooting

The elimination of possible malfunctions listed below is made by the Client. If the fault persists, we recommend you to contact one of the service centers of **PERCo** company. A list of service centers is given in the Certificate.

Before the diagnostics the user should open the controller housing.

Each controller relay output is equipped with diagnostics LED indicator for convenience. The turn on/off of LED indicators identifies that relay is activated/deactivated.

Possible faults:

11.3.1 The controller does not work

Possible causes of the controller malfunction:

1. **Loosening of the wires in the terminal blocks of the controller board** – tighten the screws of the terminal blocks with a screwdriver.
2. **Power source malfunction** of the controller – check the power source.
3. **Malfunction of connection lines** used to connect various devices (reader, indication block with infrared detector, lock, turnstile, door sensor, RC-panel, siren, etc.) to the controller – check connection lines.
4. **Identical addresses of connected devices are set** – set different addresses. Check the connection of address lines.
5. **Failure of devices connected to the controller** – check the operation of the devices.
6. **Failure of radioelectronic components**, installed on the controller board – contact **PERCo** service in order to replace this board.

11.3.2 Communication failure between controller and PC

Possible causes of this malfunction:

1. **Network settings in the computer are missing** – set IP-address and subnet mask of the computer. The controller should be connected either directly to network connector of network card of the computer or to the same Hub / Switch the computer is connected to.
2. **Invalid password of the controller**. Check the password entered in the software.
3. **Malfunctions of the computer** (software, databases etc.).

To detect this malfunction, start the command:

```
ping x.x.x.x, where x.x.x.x is the IP-address of the controller.
```

If there is communication, you will see lines similar to the following:

```
Reply from x.x.x.x: bytes=32 time<10ms TTL=128
```

If there is no communication (response), check router settings of your network.

4. **Malfunctions of equipment of Ethernet network**, installed between the computer and the controller: hub, switch and other network equipment including communication cables.

To detect this malfunction, start the command:

```
ping x.x.x.x -l 576, where x.x.x.x is the IP-address of the controller.
```

If there is communication and standard minimal packets (576 bytes) are not fragmented, you will see lines similar to the following:

```
Reply from x.x.x.x: bytes=576 time<10ms TTL=128
```

In such case IP-packets are not fragmented to the size less than 576 bytes and the selected connection must be operational.

If the positive answer is not received, the problem may be related to the network switching equipment that fragments IP-packets to the size less than 576 bytes. Check settings of this equipment, enlarge the size of *MTU*. This parameter is usually related to as *MaxMTU* or *IPMTU*.

5. **If several variants of switching are possible**, use command:

```
ping x.x.x.x -l 576 -t
```

By switching with various variants, look at response time and choose the connection with the fastest response.

6. **Malfunctions of the controller.** Failure of elements providing connection via *Ethernet* interface (*IEEE 802.3*).

To detect this malfunction, have a look at two indicators, installed on the *8P8C (RJ45)* connector of *Ethernet* connection:

- *LINK* – connection:
 - Green light is on – the controller detects connection to *Ethernet* network,
 - Green light is off – the controller does not detect connection to *Ethernet* network;
- *ACT* – data exchange:
 - Yellow light is blinking – the controller detects data exchange via *Ethernet* network,
 - Yellow light is off – the controller does not detect data exchange via *Ethernet* network.

If the controller does not detect connection to *Ethernet* network (light indicators are off), connect it to the cable that connects the other controller or computer.

If the controller still does not detect connection to *Ethernet* network or the communication is not reestablished, contact **PERCo** service in order to repair this controller.

12 MAINTENANCE

Technical staff performing maintenance of the controller should be acquainted with construction and operating procedures of the controller.

All works should be done by high-skilled electricians.

Information about scheduled maintenance is recorded in the log of maintenance and monitoring of the technical condition of means of the security fire alarm system.

Respecting of periodicity, technological order and methods of execution of maintenance work are required.

Please refer to Sect. 7 “Safety requirements” of this Manual when performing technical maintenance.

Following types and periodicity of maintenance work should be provided:

- planned work according to the regulation #1 – once in three months;
- planned work according to the regulation #2 – receiving of two or more false alarms from the protected object within 30 days.

List of work for the regulations is shown in Tables 5 and 6.

De-energize the controller prior to maintenance.

All control instrumentations should be calibrated.

Maintenance of other devices of the system, such as locks, turnstiles, swing gates, security detectors, power supply, etc. refer to operation manuals for these devices.

Table 5. List of maintenance works according to the regulations #1 (checklist #1)

Work	Procedure	Devices, instrument, equipment	Norms and events
1 External inspection, cleaning of the controller	1.1 Disconnect power supply from AC, clean up the controller and power supply surface from dust, dirt and damp.	Rags, brush, flat brush	There should not be traces of dirt and damp.
	1.2 Remove the controller and power supply housing, clean up surface from dust and damp. Measure the voltage of the extra power supply. If needed, you may charge or replace the battery.	Screwdriver, rags, flat brush, measuring device	Voltage should correspond to certificate on the battery (min. 12,6V)

Work	Procedure	Devices, instrument, equipment	Norms and events
1 External inspection, cleaning of the controller	1.3 Remove dust, dirt, corrosion from the surface of terminal blocks, jumpers and fuses.	Rags, flat brush, grease	There should not be corrosion and dirt
	1.4 Verify compliance of the denomination and the condition of the fuses		
	1.5 Verify connection of external circuits to terminal blocks of the controller	Screwdriver	It should conform to the layout of the external connections is loosen. Restore connection, if the wire is broken off. Replace the wire, if insulation is damaged
	1.6 Tighten the screws on the terminal blocks where the mount	Screwdriver	Wires and insulation should not be damaged
2 Functionality test	2.1 Check the controller by simulating the actuation of detectors in accordance with the resources configuration.		Indication on the controller corresponding to events is on. Formation of signals at the outputs according to their configuration.

Table 6. List of maintenance works according to the regulations #2 (checklist #2)

Work	Procedure	Norms and events
1. External inspection, cleaning of the controller	1.1 Complete on 1.1-.6 of checklist #1.	
2. Functionality test	2.1 Check the operation under Sect. 11 in accordance with selected configuration.	Switching on of indication on the controller according to Sect. 11.2. Forming signal at relay outputs according to their configuration.

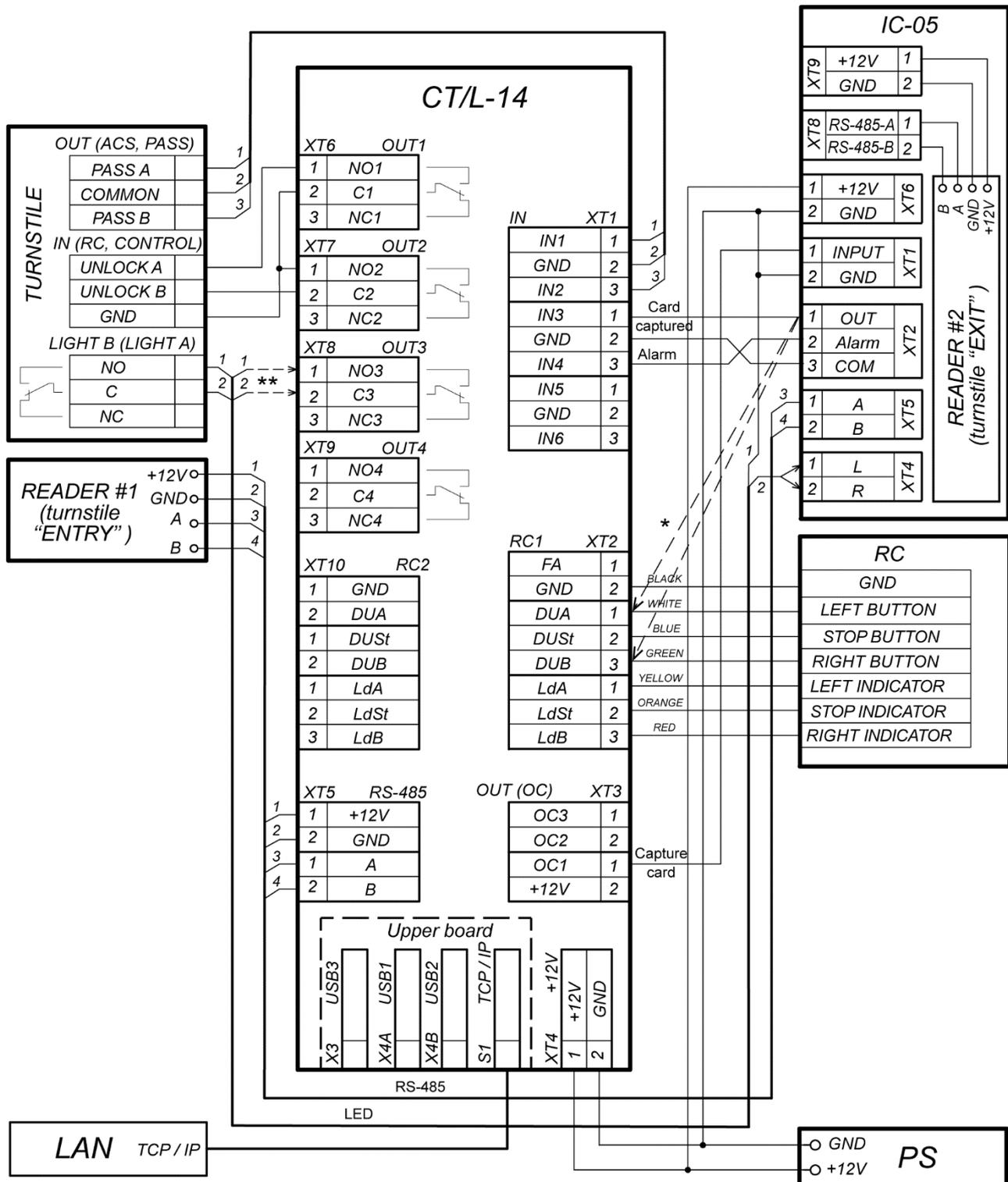
13 TRANSPORTATION AND STORAGE

The controller in the original package should be transported in closed freight containers or in other closed type cargo transport units.

The storage of the controller is allowed indoors at ambient temperature from -20°C to +40°C and at relative air humidity up to 98% at +25°C.

APPENDICES

Appendix 1. Instruction on connection of the card capture reader



* If all additional inputs of the controller are occupied, then the output of the card reader OUT (signal "Card captured") can be connected in parallel with the remote control to the control input of the controller DU A or DU B, depending on the direction of passage.

** If a third-party turnstile that does not have external indication control outputs is used as a OD, then the input of the CT/L-14 controller can be connected to the input of the XT4 "LED" card capture reader ("L" pin - "left arrow" or "R" pin - "right arrow"), as well in the software it must be configured to control the indication of permission of the card capture reader.

Figure 15. IC-05 card capture reader connection layout

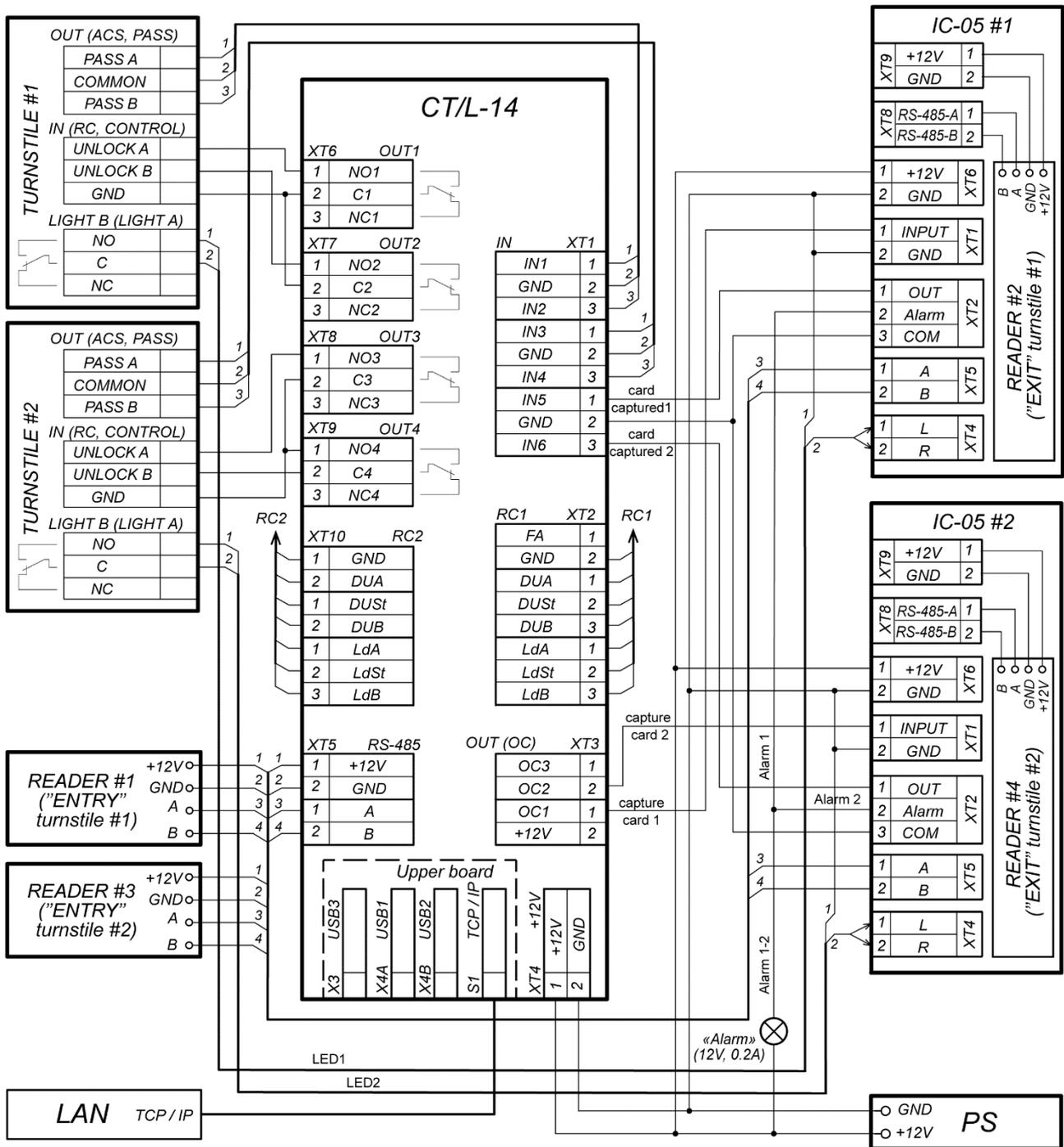


Figure 16. Connection layout for two turnstiles with IC-05 card capture readers

The card capture reader is designed to operate as a device for reading, capturing and keeping *Proximity* cards issued to visitors and meant for withdrawal at exit.

In **PERCo-Web** system the **CT/L-14** controller operates with the **IC05** card capture reader, built-in card capture readers of the **PERCo** turnstiles, connection of third-party card capture readers is possible. The procedure of configuring the controller and the **IC05** card capture reader is described in the *Administrator's Guide* of these systems and also in the **IC05** Operation Manual.

An example of connection of the **PERCo** card capture readers is shown in Fig. 15. Any available inputs and outputs are used in the current controller configuration.

The controller controls the card capture reader by sending the "Capture card" input signal to the card capture reader board. One of the additional outputs of the controller, which connects the "Capture card" input, should be configured in software so that upon presentation of the card to the proper card reader, the output is activated (input type – "EVD confirmation input").

After card capturing, the card capture reader passes the “*Card captured*” signal, which the controller uses as the confirmation of passage permission in the required direction through the OD. One of additional controller inputs should be configured in software that when it is activated by the “*Card captured*” signal, the controller opens the operating device in the required direction.

The card capture reader can generate “Alarm” signal (*Alarm* output) regarding to trouble in its operation, signal of filling container) that can be applied to the free inputs of the controller by configuring them to required responses (activation of appropriate sirens, etc.).

The settings of the card capture reader inputs and outputs should correspond to the settings of the controller inputs and outputs (Sect. 5.4, 5.5).

When two turnstiles are connected to the controller, it is possible to control two card capture readers - one for each turnstile. An example of such a connection is presented in Fig. 16. *IN5* input must be configured as a confirmation input from EVD for resource #1, and *IN6* input as a confirmation input from EVD for resource #2. In this example, the Alarm outputs of both card capture readers are interconnected and connected to one common “Alarm” siren (12V / 0.2A). The input signals indicating the passage direction of the **IC-05** card capture readers receive control signals directly from the turnstile control boards.

Appendix 2. Instruction on connection of the CT/L-14 through PoE-splitter



Attention!

- Provided instruction refers to the splitters included in optional equipment delivery set.
- Total power consumption of the controller and of all the devices powered by it must not exceed 12 W. It is also recommended to leave min 10% reserve power.

Splitter description

PoE-splitter (hereinafter – *splitter*) is designed for energizing equipment, connected via *Ethernet* network. Splitter operates with any network commutators (hereinafter – *Switch*), supporting technology of electric power transmission via *PoE* twisted pair wire and compatible with *IEEE 802.3af* standard.

Splitter is designed as a block of electronics in a plastic housing featuring the following outputs:

- Con 1** – output for *Ethernet* cable from *Switch* connection;
- Con 2** – output for *Ethernet* controller cable connection;
- Con 3** – power output for controller power cable connection.



Note:

For some models of splitters output voltage is chosen with a switch. Operating **PERCo** equipment it is necessary to place the switch in “12V” mode.

Requirements for connecting devices

The characteristics of power consumption of the controller when connected through splitter should meet the following requirements:

Admissible value of supply voltage	12±1.2 V
Minimum total current	min. 120 mA
Maximum total current consumption (12V)	max 1 A
Maximum total power consumption	max 12 W

In order to avoid exceeding the total power consumption, providing power from the controller to connected optional equipment (siren, intrusion detector, etc.) and to controllers of the second level is not recommended. Up to four readers and ODs can be connected to the controller powered from the splitter. Up to four electromechanical locks or two turnstiles (see Table 7) can be connected as ODs.

Table 7. OD powered through PoE-splitter

Types of controller configurations	OD
“Controller to operate the locks”	Electromechanical lock (LC , LB and LBP – up to 4pcs).
“Controller to operate the turnstile”	Turnstile with power consumption no more than 9W T-5, TTR-04.1, TTD-03.1, TTD-03.2

Procedure of controller connection

Cables used in installation are mentioned in Table 3. When connecting the controller through the splitter, proceed as follows:

1. Determine the installation location of the splitter. It is recommended to install the splitter inside of controller housing (do not install the splitter at a distance of more than 2m away from the controller).
2. Connect controller *Ethernet* cable to the splitter **Con2** connector.
3. Connect the power supply to **Con3** connector. If necessary OD can be connected to **Con3** connector as well. Connection layout is shown in Fig. 17 (plug for connection to connector included into splitter delivery set).

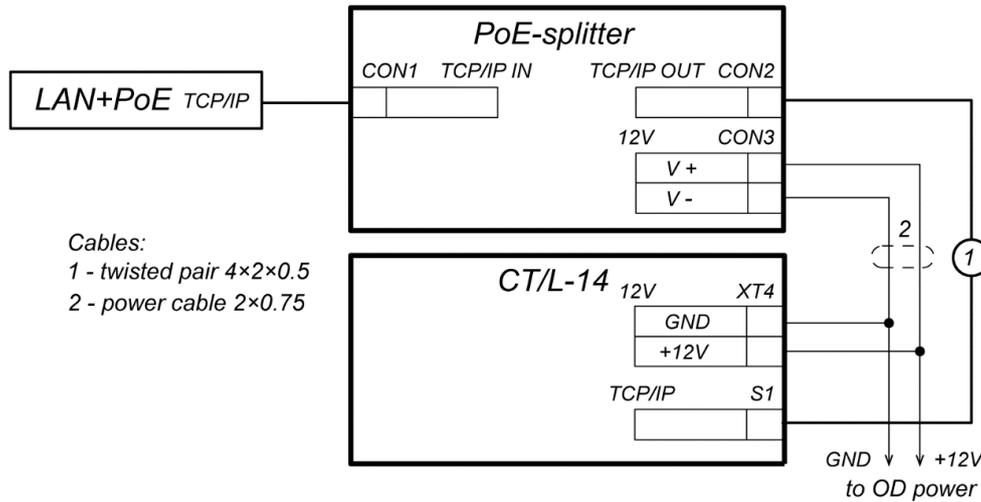


Figure 17. Connection layout of the controller through PoE-splitter

4. Connect *Ethernet* cable from *Switch* to the splitter **Con1** connector.
5. Connected device will be powered after verification between *Switch* and the splitter.

In case you need to deenergize the controller, it is sufficient to disconnect *Ethernet* cable (from *Switch*) from the splitter **Con1** connector.

Appendix 3. Instruction on connection of the controller for lock-chamber management

Lock-chamber is intermediate detached space (passage through an OD) which excludes a possibility of a pass-through without additional verification (visual identification, verification, all the types of double-check verification etc.) and the person passing through the passageway is locked inside while being verified. Lock-chamber is provided with two check-points equipped with operating devices: hereinafter OD1 and OD2. It is possible to enter lock-chamber only if there is nobody in the zone. While there is a person in the lock-chamber zone, external readers (RC buttons) are blocked until the person leaves the lock-chamber.

CTL-14 controller can operate different types of lock-chambers:

1. Two-lock lock-chamber (double-sided locks).
2. **RTD-15, RTD-16, RTD-20** full-height rotor turnstile lock-chamber.
3. Turnstile-and-lock lock-chamber.
4. Two-turnstile lock-chamber.



Attention!

When the controller is connected to an ACS, the full lock-chamber configuration is carried out by the system software.

To operate this kind of lock-chambers, the controller should be configured according to one of the web-interface models, which automatically set necessary internal responses and cross links in the settings of the controller, and also will set associated events.

Types of lock-chambers operated by the CT/L-14 controller

- Two-lock lock-chamber is intermediate space with a free passage through two doors. Each lock-chamber door is operated by two internal and external readers (in regard to the lock-chamber). Reader can be replaced or duplicated by the RC button (see below the lock-chamber OD settings). To provide the lock-chamber operation two door sensors are required: #1 for OD1 and #2 for OD2.

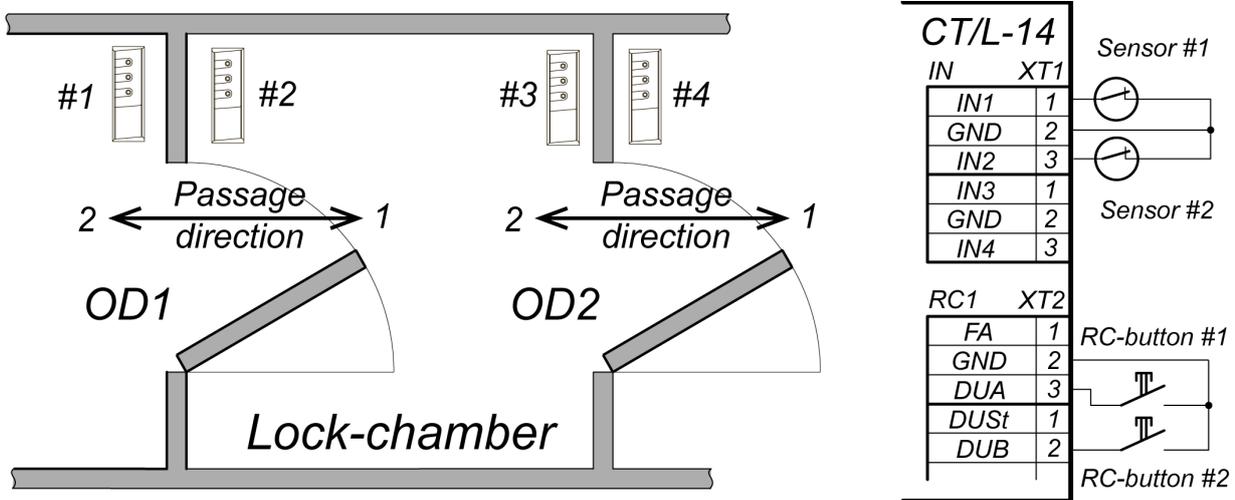


Figure 18. Layout of the lock lock-chamber

- Rotor turnstile lock-chamber is a **RTD-15, RTD-16, RTD-20** full-height turnstile with a rotor set in a lock-chamber mode. Entrance and exit are operated by two internal and external readers (in regard to the lock-chamber). Reader can be replaced or duplicated by the RC button (see below the lock-chamber OD settings). For comfort of use in the Web-interface of the controller the lock-chamber is presented as 4 single-sided locks (OD1 and OD3 for a passage in one direction through the turnstile, OD2 and OD4 in the opposite direction). To operate the lock-chamber passageway control sensors are activated: PASS A for the direction of the passage 1, PASS B for the direction of the passage 2.

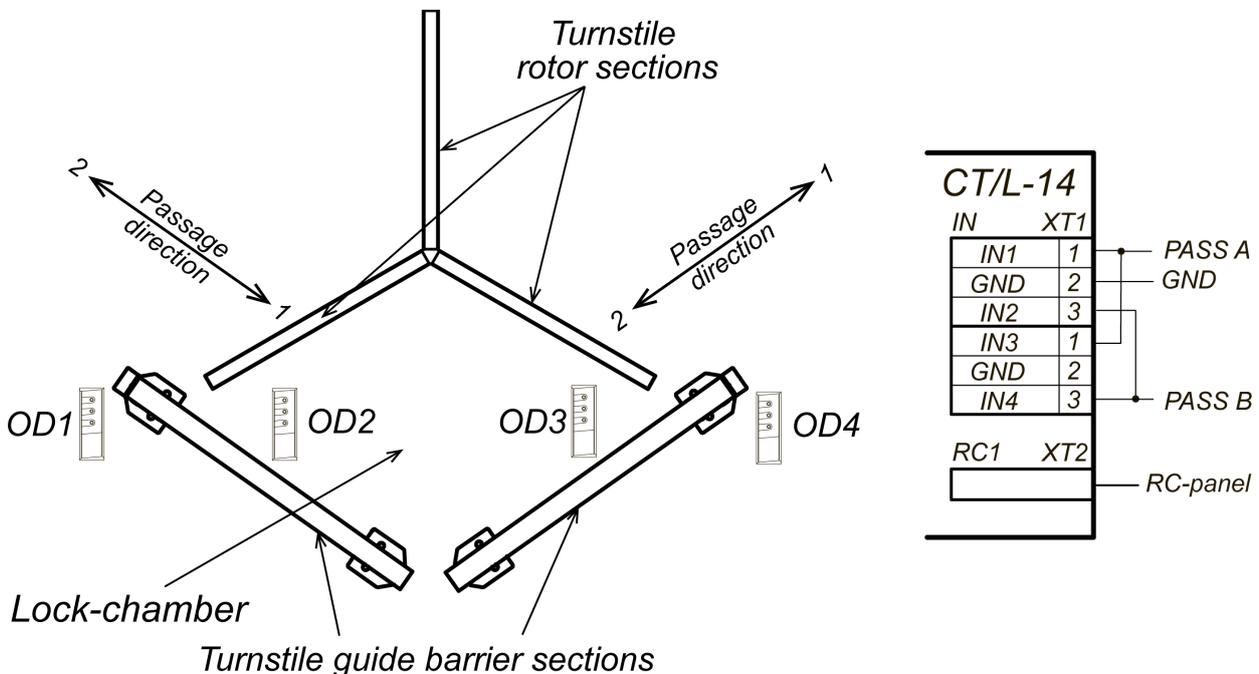


Figure 19. Layout of the rotor turnstile lock-chamber

- Turnstile-and-lock lock-chamber is intermediate space between the turnstile and the intermediate door with a free passage through the zone. The turnstile and door lock are operated by two internal and external readers each (in regard to the lock-chamber). Reader can be replaced or duplicated by the RC button or RC (see below the lock-chamber OD

settings). To operate the lock-chamber passageway control sensors are activated: PASS A for direction of the passage 1 through OD1, PASS B for direction of the passage 2 through OD1 and the door sensor (for both directions through OD2).

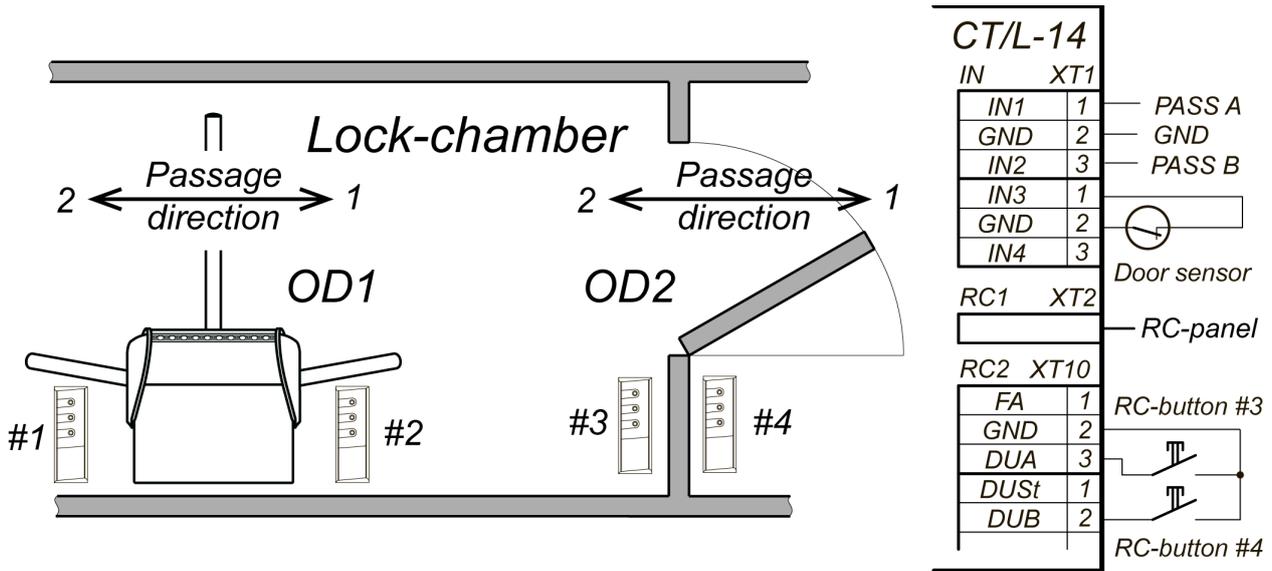


Figure 20. Layout of the turnstile-and-lock lock-chamber

- Two-turnstile lock-chamber is a zone between two turnstiles standing one behind the other in the passage direction. Each turnstile is operated by two internal and external readers (in regard to the lock-chamber). Reader can be replaced or duplicated by the RC button (see below the lock-chamber OD settings). To operate the lock-chamber passageway control sensors are activated: PASS A and PASS B of turnstile 1 for direction of the passages 1 and 2 through OD1, PASS A and PASS B of turnstile 2 for direction of the passages 1 and 2 through OD2.

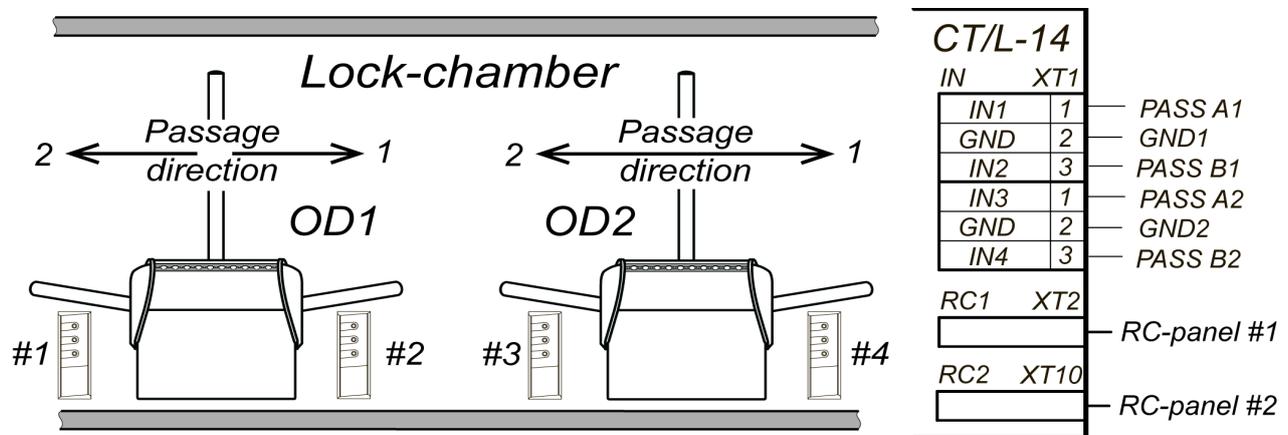


Figure 21. Layout of the two-turnstile lock-chamber

The parameters for lock-chamber ODs set in the Web-interface:

- Access algorithm:
 - soft – leaving the lock-chamber in both directions,
 - hard – leaving the lock-chamber only in a pass-through direction.
- Access mode:
 - by a reader,
 - by RC,
 - by a reader and RC.
- Position (in regard to the lock-chamber placement (zone)):
 - outdoors,
 - indoors.
- The maximum time spent in the lock-chamber – when the time is finished, the controller will generate the event about exceeding the allotted time of staying in the lock-chamber zone.

Appendix 4. CT/L-14 Controller Web-interface. User Manual

CONTENTS

1.	WEB-INTERFACE OPPORTUNITIES.....	38
2.	CONNECTION TO WEB-INTERFACE OF THE CONTROLLER.....	38
3.	SETTINGS.....	39
3.1	Change of controller system time.....	39
3.2	Change of controller network setting.....	40
3.3	Change of server settings.....	40
3.4	Setting of the controller access password.....	40
3.5	Reading format of the card identifiers.....	40
4.	CONFIGURATION.....	41
4.1	Controller configuration template.....	41
4.2	Configuration of the controller resources settings.....	42
4.2.1	Operating devices.....	42
4.2.2	Physical contacts (inputs and outputs).....	42
4.2.3	Readers.....	44
4.2.4	Internal responses.....	45
4.2.5	Events filter.....	46
5.	ACCESS CRITERIA.....	47
5.1	Time access criteria.....	47
5.1.1	Time zones.....	47
5.1.2	Holidays.....	48
5.1.3	Weekly schedule.....	49
5.1.4	Flexible daily schedule.....	50
5.1.5	Flexible weekly schedule.....	50
5.2	Users.....	51
6.	OPERATING DEVICE CONTROL.....	52
7.	EVENTS.....	53
8.	STATUS.....	54
9.	SERVICE.....	55

1. WEB-INTERFACE OPPORTUNITIES

Using Web-interface without installation of additional software allows performing following steps for the controller and connected devices:

- Change network settings, access password and time of built-in clocks of the controller.
- Configure settings of operating device, readers and other equipment of the controller.
- Set ACM for operation devices.
- Record the access card numbers in the controller memory, assign them the rights for arming or disarming.
- Monitor event log of the controller and save them as a file.
- Control the status of the controller and connected devices, monitor the event log.
- Troubleshoot the controller, format the memory and update the embedded software.



Attention!

It is possible only with the Web-interface:

- Select controller configuration template.
- Add and delete optional readers in configuration.

2. CONNECTION TO WEB-INTERFACE OF THE CONTROLLER

Connection between the controller and the computer is performed via *Ethernet* interface (IEEE 802.3). Make sure that the computer and the controller are on the same subnet *Ethernet*. It may become necessary to change network settings of the computer, browser settings and to check operation of the network. IP-address of the controller is specified in the certificate and the controller board.

To connect the controller to Web-interface:

1. Open Web-browser (e.g. *Internet Explorer*).



Attention!

Web-interface was tested with the Web-browsers: *Microsoft IE* version 10 or higher, *Google Chrome* version 32 or higher, *Mozilla Firefox* version 32 or higher, *Opera* version 30 or higher, *Microsoft Edge* and for *MacOS Apple Safari* 9 or higher. If other browsers and outdated versions are used, malfunctions of the Web-interface can appear.

2. Enter IP-address of the controller in the address bar and press the **Enter** button on the keyboard. If necessary, enter the access password to the controller. By default, there is no password.
3. After that the main Web-page of the controller interface will be opened. Version, configuration, network settings of the controller and embedded software version will be displayed on the main page. At each opening of the page, current controller data will be displayed. The page looks as follows:

Gateway default	0.0.0.0
IP default	10.1.214.117
MAC	00:25:0B:01:D6:75
Mask default	255.0.0.0
Product	PERCo-CTL14
Template	Turnstiles
Version app	2.2.17
Version of Image	2.1.0.19
Version of S30	(2.2.17)
Version of S30web	(2.2.2)

A callout bubble '3' points to the 'Version of S30' and 'Version of S30web' rows.

On the page the user can select the following elements:

1. The page title bar contains **PERCo** trademark and buttons to select the language of Web-interface. By clicking on the **PERCo** company logo the user will navigate to the main page from other sections of Web-interface.
2. Sidebar of the Web-interface navigation. The panel has the following structure:

<i>“Settings”</i>	<i>“Time”</i>	
	<i>“Network”</i>	
	<i>“Server”</i>	
	<i>“Password”</i>	
	<i>“Cards format”</i>	
<i>“Configuration”</i>	<i>“Template”</i>	<i>“Operating devices”</i>
	<i>“Edit”</i>	<i>“Physical contacts”</i>
		<i>“Readers”</i>
		<i>“Internal responses”</i>
		<i>“Events filters”</i>
<i>“Access”</i>	<i>“Time access criteria”</i>	<i>“Time zones”</i>
		<i>“Holidays”</i>
		<i>“Weekly schedule”</i>
		<i>“Shift-day”</i>
		<i>“Flexible weekly”</i>
	<i>“Users”</i>	
<i>“Operating device control”</i>		
<i>“Events”</i>		
<i>“Status”</i>		
<i>“Service”</i>		

3. Page working area.

3. SETTINGS

3.1 Change of controller system time

To change the time:

1. Click **Settings** → **Time** in the Web-interface menu. The page with working area will be opened:

Date:

Time: : :

Time zone:

Sync with PC:

2. In the **Date**, **Time** input fields change the set values.
3. Select the desired value for the **Time Zone** parameter.
4. If necessary, tick the **Synchronize with PC** box to synchronize the time and date of the controller with the computer connected to the Web-interface.
5. Click the **Save** button.

3.2 Change of controller network setting

The controller has the following configurations by default (they are specified in the certificate of the device and on the labels on the controller):

- MAC-address 00-25-0B-xx-xx-xx, where xx – is a number from 00 to FE;
- IP-address 10.x.x.x, where x – is a number from 0 to 254;
- Subnet mask 255.0.0.0.

To change network settings of the controller:

1. Click consistently **Settings** → **Network** in the Web-interface menu. The page with working area will be opened:

IP-address: . . .
Mask: . . .
Gateway: . . .

2. In the **IP-address**, **Mask**, **Gateway** input fields set the new values of controller network settings.
3. Click the **Save** button. New network settings will be saved in the controller.

3.3 Change of server settings

In order to change the server settings, proceed as follows:

1. Click **Settings** → **Server** in the Web-interface menu. The page with working area will be opened:

Server address:
Encryption:

2. In the opened window make the necessary changes for the parameters:
 - **Server address** parameter sets the server address.
 - **Encryption** parameter sets the encryption method: **No** or **SSL**.
3. Click the **Save** button. New network settings will be saved in the controller.

3.4 Setting of the controller access password

By default, access password of the controller is not specified. To change or set the new password:

1. Click **Settings** → **Password** in the Web-interface menu. The page with working area will be opened:

New password:
Confirm password:

2. In the **New password** field enter the new password of the controller, in the **Confirm password:** field enter the password again to confirm the correct input.
3. Click the **Save** button. The new password will be saved in the controller.

3.5 Reading format of the card identifiers



Attention!

- Change of this parameter, after the access cards having already been registered, results in the passage on these cards being denied.

- When connecting to the controller operating under software of **PERCo** systems, the current format may not be shown (nothing is selected from the formats). In this case change of the card identifiers reading format is **PROHIBITED**.

To select the reading format of card identifiers:

1. Click consistently **Settings** → **Card format** in the Web-interface menu. The page with working area will be opened:

Readers operation mode: 

2. Using the drop-down **Readers operating mode** list select one of offered formats and click the **Save** button.

4. CONFIGURATION

4.1 Controller configuration template



Attention!

If the configuration template is updated, the previous configuration will be reset to the default template parameters. The list of recorded access cards identifiers, related user information, access rights and parameters remain the same.

To change the configuration of the controller:

1. Click **Settings** → **Template** in the Web-interface menu. The page with working area will be opened:

Settings

Configuration

Template

Edit

Access

Operating device control

Events

Status

Service

Template

Vehicle checkpoint
Vehicle checkpoint and locks
Vehicle checkpoint and turnstile
Gateway from the rotor turnstile
Gateway from the turnstile and the lock
Lock gateway
Locks
Turnstile and locks
Turnstile gateway
Turnstiles

The following configuration templates are available for the **CT/L-14** controller:

- **Vehicle checkpoint;**
- **Vehicle checkpoint and locks;**
- **Vehicle checkpoint and turnstile;**
- **Locks;**
- **Turnstile and locks;**
- **Turnstiles;**
- **Lock lock-chamber;**
- **Rotor turnstile lock-chamber;**
- **Turnstile-and-lock lock-chamber;**
- **Turnstile lock-chamber.**



Note:

The plural number of ODs in the name of the configuration template means that when applying the template, the maximum quantity of OD data will be configured, based on the resources of the controller. After selecting a template, unnecessary ODs can be deleted.

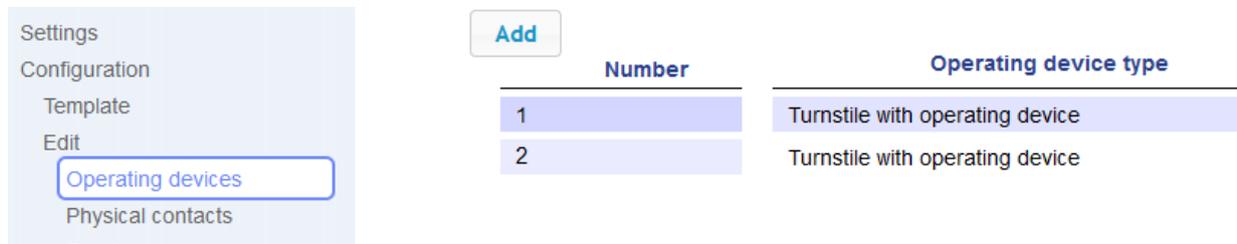
2. Select the desired configuration option. Changing the configuration template can take up to 30 seconds.

4.2 Configuration of the controller resources settings

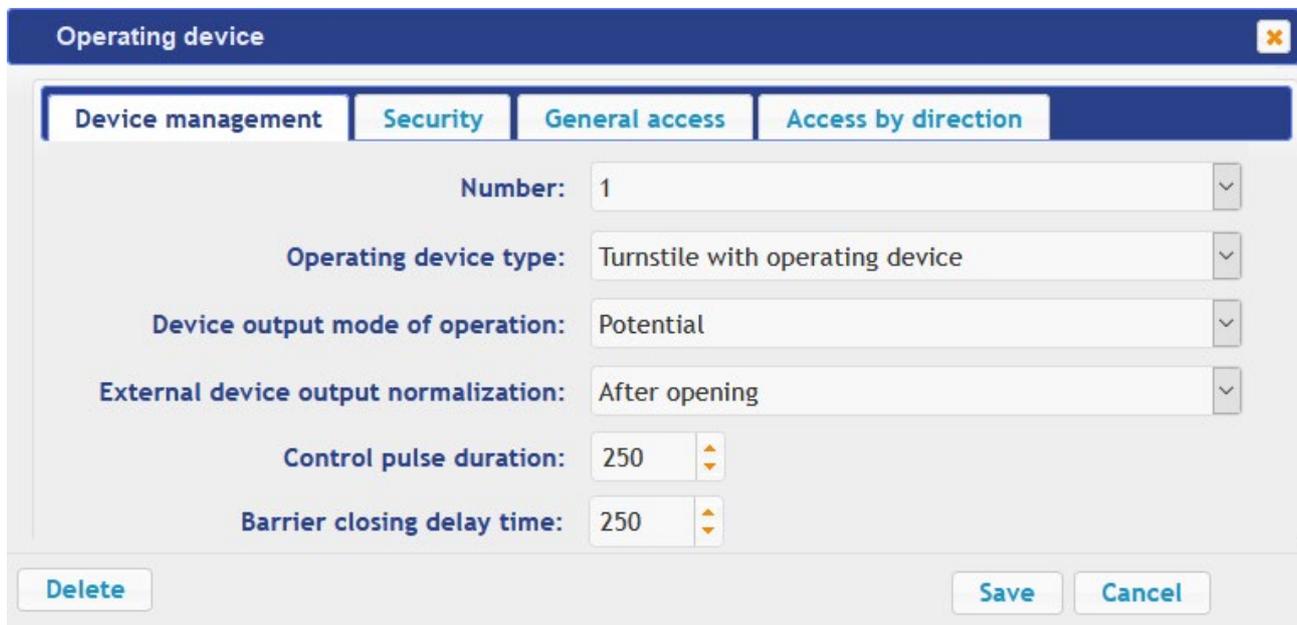
4.2.1 Operating devices

To configure settings of the controller resources to control OD:

1. Click consistently **Configuration** → **Edit** → **Operating devices** in the Web-interface menu. The page with working area will be opened:



2. To add the new ODs to the list, click the **Add** button; To change OD settings, click the title bar in the page working area. The **OD** window will be opened:



3. In the opened window on the **Device management**, **Security**, **General access**, **Access by direction** tabs make the necessary changes of the settings for corresponding resources.
4. Click the **Save** button. The window will be closed, changed settings will be passed to the controller.
5. To exit the **OD** window without saving the changes, click the **Cancel** button or the **Close** button .
6. To remove the OD from the configuration, in the window with this OD click the **Delete** button. The OD will be deleted.

4.2.2 Physical contacts (inputs and outputs)

To configure the settings of the controller inputs and outputs:

1. Click consistently **Configuration** → **Edit** → **Physical contacts** in the Web-interface menu. The page with working area will be opened:

	Contact	Function	Operating device	Direction	Normal	Status
Settings						
Configuration						
Template	DUA 1	Remote control	1	1	Cut	Normal
Edit	DUA 2	Remote control	2	1	Cut	Normal
Operating devices	DUB 1	Remote control	1	2	Cut	Normal
Physical contacts	DUB 2	Remote control	2	2	Cut	Normal
Readers	DUS1 1	Remote control	1		Cut	Normal
Internal reactions	DUS1 2	Remote control	2		Cut	Normal
Events filter	FA	Fire alarm input	256	1	Closed	Normal
Access	In1	Pass input	1	1	Closed	Active
Operating device control	In2	Pass input	1	2	Closed	Active
Events	In3	Pass input	2	1	Closed	Active
Status	In4	Pass input	2	2	Closed	Active
Service	In5	Input	1	1	Cut	Normal
	In6	Input	2	1	Cut	Normal
	LdA 1	Remote control indication output	1	1	Energized	Normal
	LdA 2	Remote control indication output	2	1	Energized	Normal
	LdB 1	Remote control indication output	1	2	Energized	Normal
	LdB 2	Remote control indication output	2	2	Energized	Normal
	LdSt 1	Remote control indication output	1		Energized	Normal
	LdSt 2	Remote control indication output	2		Energized	Normal
	NO1/C1/NC1	Operating device control output	1	1	Not energized	Normal
	NO2/C2/NC2	Operating device control output	1	2	Not energized	Normal
	NO3/C3/NC3	Operating device control output	2	1	Not energized	Normal
	NO4/C4/NC4	Operating device control output	2	2	Not energized	Normal
	OK1	Output	1	1	Not energized	Normal
	OK2	Output	2	1	Not energized	Normal
	OK3	Output	3	1	Not energized	Normal

The page lists all the controller inputs and outputs.

When selecting the template (p. 4.1) the inputs and outputs that are involved in the OD control of this template, corresponding functions are stated (for inputs – PASS / RC, for outputs – OD control / RC-panel indication) and the number and OD direction, which the physical contact is attached to, are to be set. Inputs and outputs that are not involved in the template, the value is **Input / Output**. These inputs and outputs are available for the task (and changes in the future) of its functions.

- To add an input or output, click the **Add Input** or **Add Output** button; to change parameters or delete an input or output, click the title bar in the page working area. The **Physical Contact** window will be opened:

Physical contact - input
✕

Contact:

Function:

Operating device:

Direction:

Normal:

Anti-Bounce: MC

Delete
Save
Cancel

- In the opened window, make the necessary changes for the parameters.
 - Contact** parameter sets the contact;

- **Function** parameter sets the contact function;
 - **Resource** parameter sets the contact resource;
 - **Direction** parameter sets the direction of a reader OD;
 - **Normal contact** parameter sets the normal contact status – open or closed for inputs, powered or not powered for outputs;
 - **Anti-Bounce parameter** sets the contact Anti-Bounce time (for inputs).
4. Click the **Save** button. The **Physical contact** window will be closed, the changed settings of inputs (outputs) will be passed to the controller.
 5. To exit the **Physical contact** window without saving changes, click the **Cancel** button. Also, it is possible to close the window using the **Close** button .
 6. To remove input or output from the list, click the title bar in the page working area, the **Physical contact** window will be opened. Click the **Delete** button. The **Physical contact** window will be closed; the selected physical contact will be deleted.

4.2.3 Readers

In all controller configurations to each direction of every OD one reader or one infrared-panel (hereafter – *reader*) is assigned. If necessary, it is possible to add into the configuration optional readers for the passage directions through the OD. For one direction two or three readers working in parallel can be installed. It can be useful, for example, when connecting a card capture reader, organizing the vehicle checkpoint to install the readers at different levels (for cars and trucks), etc.

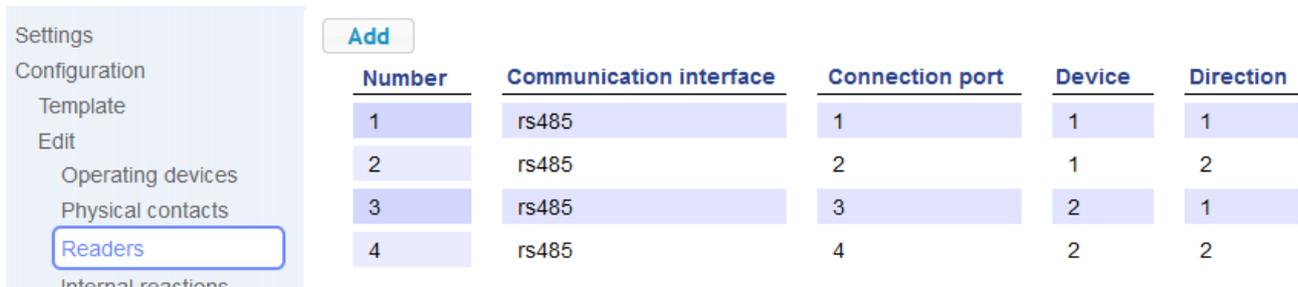


Note:

When adding optional readers, they are configured similarly to card capture readers attached to the same OD directions. In this regard, added readers are not shown in network and local software of **PERCo-Web** system.

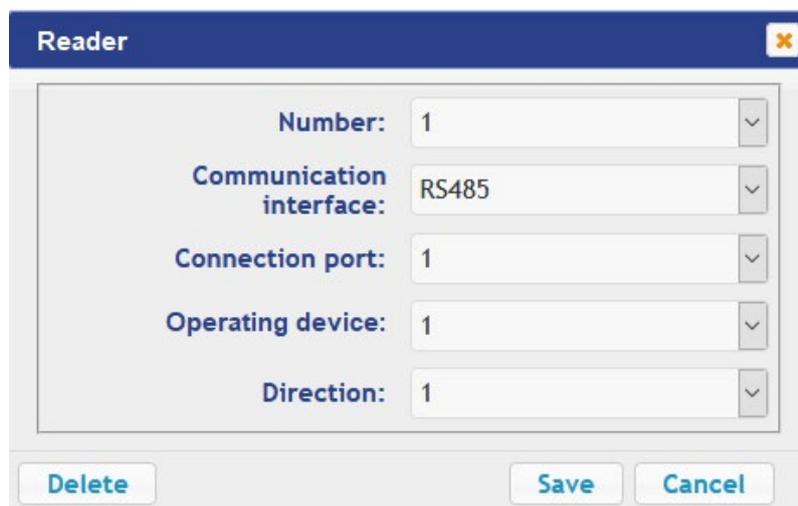
To configure the reader settings:

1. Click consistently **Configuration** → **Edit** → **Readers** in the Web-interface menu. The page with working area will be opened:



Number	Communication interface	Connection port	Device	Direction
1	rs485	1	1	1
2	rs485	2	1	2
3	rs485	3	2	1
4	rs485	4	2	2

2. To add a reader to the list, click the **Add** button. To change the parameters or delete the reader, click the title bar in the page working area of the reader. The **Reader** window will be opened:



3. In the opened window make the necessary changes of the settings:
 - **Number** parameter sets the number of the added reader;
 - **Communication interface** parameter sets the interface or reader type;
 - **Connection port** parameter sets the port of the interface or the address on the bus (RS-485 / Wiegand);
 - **Operating device** parameter sets the number of the OD to which the reader is attached;
 - **Direction** parameter sets the direction of the OD to which the reader is attached;

“Morpho” fingerprint scanner:

 - **Sensor position** parameter sets the position in which the reader will identify and verify the finger, taking into account its possible rotation;
 - **Possibility of an unauthorized access** parameter sets the probability of unauthorized access (error of the first kind), expressed as a percentage of the number of access of unauthorized persons by the system;
 - **Fingerprint format** parameter sets fingerprint formats.

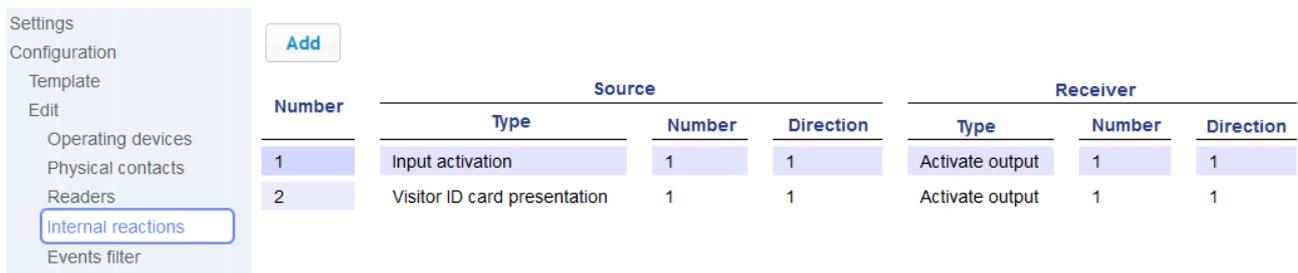
Trassir

 - **SSL** parameter sets the exchange coding initiation with Trassir server.
 - **Address** parameter sets line with Trassir server IP-address.
 - **Port** parameter sets Trassir server port number.
 - **Password** parameter sets Trassir server authorization password.
 - **Movement line** parameter sets the number of the movement line for this OD direction;
 - **Channel** parameter sets the line with Trassir server channel ID.
4. To add the reader with the assigned number and transfer the changed parameters to the controller, click the **Save** button. The **Reader** window will be closed.
5. To exit the window **Reader** without saving changes, click the **Cancel** button. Also, it is possible to close the window using the **Close** button .
6. In order to delete the reader from the list, click the title bar in the page working area, the **Reader** window will be opened. Press the **Delete** button. The **Reader** window will be closed; the chosen reader will be deleted.

4.2.4 Internal responses

To set internal responses of the controller:

1. Click consistently **Configuration** → **Edit** → **Internal responses** in the Web-interface menu. The page with working area will be opened:



Number	Source			Receiver		
	Type	Number	Direction	Type	Number	Direction
1	Input activation	1	1	Activate output	1	1
2	Visitor ID card presentation	1	1	Activate output	1	1

2. To add the new response, click the **Add** button, to change the settings of internal response or delete it, click the title bar in the page working area. The **Internal response** window will be opened:

3. In the opened window make the necessary changes of the settings:
 - **Number** parameter sets the response number in the controller database (from 1 to 40);
 - **Source type** parameter sets the launch condition of the controller response;
 - **Source (Receiver) number** and **Source direction (Receiver direction)** parameters set numbers and directions of corresponding resources of the controller which are response sources (receivers);
 - **Receiver type** parameter sets the controller response under condition of the response launch;
 - **Response time** and **Response characteristics** parameters set corresponding response settings.
4. Click the **Save** button. The **Internal response** window will be closed; the changed settings will be passed to the controller.
5. To exit the **Internal response** window without saving changes, click the **Cancel** button. Also, it is possible to close the window using the **Close** button
6. To remove the response from the list, click the **Delete** button. The window **Internal response** will be closed; the internal response will be deleted.

4.2.5 Events filter

To configure events filter, proceed as follows:

1. Click consistently **Configuration** → **Edit** → **Events filter** in the Web-interface menu. The page with working area will be opened:

2. To add a new filter, click the **Add** button; to change parameters or delete a filter, click the title bar in the page working area. The **Filter** window will be opened.
3. In the opened window set the necessary values for the event parameters that need to be filtered from the general list.
 - **Number** parameter sets the filter number (from 1 to 20);
 - **Category** parameter sets the event category;
 - **Code** parameter sets the event code;
 - **Operating device** parameter sets the reader OD number;
 - **Direction** parameter sets the reader OD direction;
 - **Access** parameter sets the user's validity: prohibited or expired;
 - **User** parameter sets the user type: visitor / employee / vehicle;
 - **Suspicious events** parameter sets the suspicious events presence: yes or no;
 - **Time violation** and **location violation** parameter sets the time violation and location violation possibility: yes or no;
 - **Identification violation** parameter sets the identification violation reason: no card / no finger / card not identified / unknown finger / user's fingerprints are not in the database;
 - **Confirmation** parameter sets the confirmation method: single / double / no UID violation / wrong UID violation / double no UID violation / double wrong UID violation / break-in violation / prohibited by RC-panel command;
 - **Verification** parameter sets the verification: confirmation / passage counter denial / RC-panel denial / EVD denial / Software denial / verification timeout / no response from passage counter / no response from RC-panel / no response from EVD / no response from software / break-in violation;
 - **Save** parameter sets the option of saving an event in the database, if it passes through the filter (if all the set filter fields coincide with all the event fields (if a filter field is not set, then the comparison is not performed)). If "yes" is set in the "Save" field, then the event will be saved in the database, otherwise it will not be saved.
4. To save the filter, click the **Save** button. The **Filter** window will be closed.
5. To exit the **Filter** window without saving changes, click the **Cancel** button. Also, it is possible to close the window using the **Close** button .
6. To remove the response from the list, click the **Delete** button. The **Filter** window will be closed; the filter will be deleted.

5. ACCESS CRITERIA

5.1 Time access criteria

5.1.1 Time zones

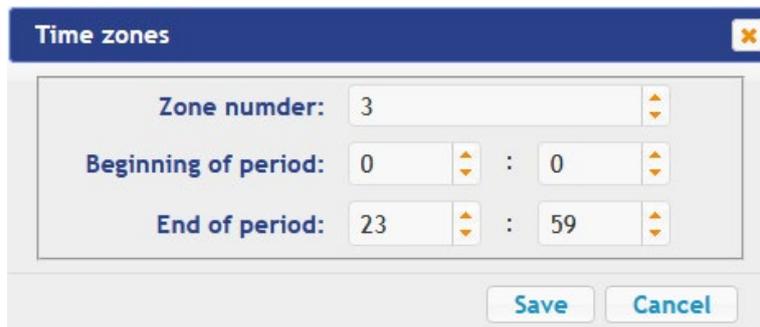
There are two preconfigured time zones - #1 – "Never" and #2 "Forever".

To set the time zone parameters, proceed as follows:

1. Click consistently **Access** → **Timing criteria** → **Time zone** in the Web-interface menu. The page with the following working area will be opened:

Add	Zone number	Validity
	1	Never
	2	Always

2. To add a new time zone, select the **Add** parameter; to change or to delete time zone parameters, click the title bar in the working area. The **Time zones** window will be opened:



3. In the opened window effect all necessary changes of the parameters:
 - **Zone number** parameter sets the time zone number;
 - **Beginning of period** parameter sets the beginning of period;
 - **End of period** parameter sets the end of period.
4. To save the time zone and send the parameters to the controller, click the **Save** button. The **Time zones** window will be closed.
5. To exit the **Time zones** window without saving the changes, select the **Cancel** button. Also, it is possible to close the window by clicking **Close** .
6. To delete the time zone from the list, click the title bar in the working area, the **Time zones** window will be opened. Select the **Delete** parameter. The **Time zones** window will be closed, the selected zone will be deleted.

5.1.2 Holidays

To set holidays, proceed as follows:

1. Click consistently **Access** → **Time access criteria** → **Holidays** in the Web-interface menu. The window with the working area will be opened:



2. To add a new holiday, select the **Add** parameter; to change or delete a holiday, click the title bar in the working area. The **Holidays** window will be opened:

3. In opened window select the date and the **Type** of the holiday.
4. To save all changes and send the set parameters to the controller, click the **Save** button. The **Holidays** window will be closed.
5. To exit the **Holidays** window without saving the changes, select the **Cancel** button. Also, it is possible to close it by clicking **Close** .
6. To delete a holiday from the list, click the title bar in the working area; the **Holidays** window will be opened. Click the **Delete** button. The **Holidays** window will be closed and the selected day will be deleted.

5.1.3 Weekly schedule

To configure weekly schedule, proceed as follows:

1. Click consistently **Access** → **Time access criteria** → **Weekly schedule** in the Web-interface menu. The window with the working area will be opened.

Settings	Add	Schedule number	Day	Time zone
Configuration		1	Monday	2
Access		1	Tuesday	2
Time access criteria		1	Thursday	3
Time zones		1	Wednesday	3
Holidays		1	Friday	2
Weekly schedule		1	Saturday	4
Shift-day		1	Sunday	4
Flexible weekly				
Users				
Operating device control				

2. To add a new weekly schedule, click the **Add** button; to change or delete the weekly schedule parameters, click the title bar in the working area. The **Weekly schedule** window will be opened:

3. In the opened window perform the necessary changes for the parameters:
 - **Schedule number** parameter sets the schedule number;
 - **Day** parameter sets the day of the week;
 - **Time zone** parameter sets the time zone number for the selected schedule.
4. To save the changes and send the parameters to the controller, click the **Save** button. The **Weekly schedule** window will be closed.
5. To exit the **Weekly schedule** window without saving the changes, click the **Cancel** button. Also, it is possible to close the window by clicking **Close** .
6. To delete the weekly schedule from the list, click the title bar in the working area; the **Weekly schedule** window will be opened. Click the **Delete** button. The **Holidays** window will be closed and the selected schedule will be deleted.

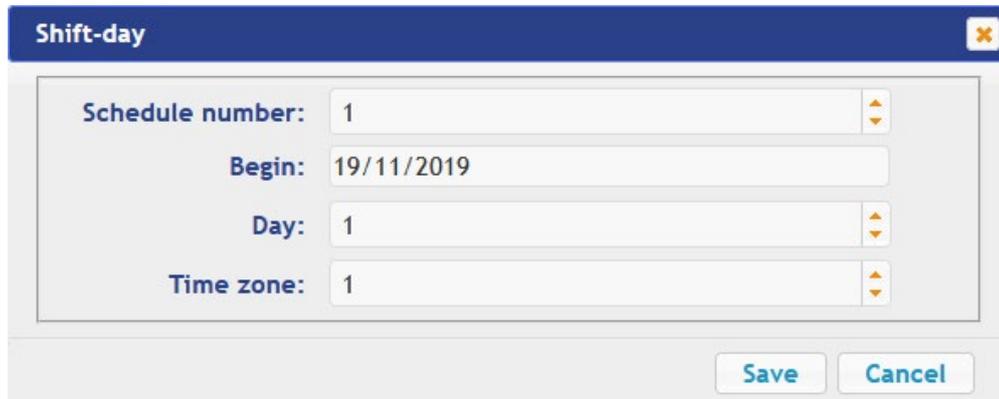
5.1.4 Flexible daily schedule

To configure flexible daily schedule, proceed as follows:

1. Click consistently **Access** → **Time access criteria** → **Flexible daily schedule** in the Web-interface menu. The window with the working area will be opened:



2. To add a new flexible daily schedule, click the **Add** button; to change or delete the Flexible daily schedule parameters, click the title bar in the working area. The **Flexible daily schedule** window will be opened:



3. In the opened window perform the necessary changes:
 - **Schedule number** parameter sets the schedule number;
 - **Beginning** parameter sets the beginning of the schedule;
 - **Day** parameter sets the number of days for the schedule;
 - **Time zone** parameter sets the time zone number for the selected day.
4. To save the changes and send the parameters to the controller, click the **Save** button. The **Flexible daily schedule** window will be closed.
5. To exit the **Flexible daily schedule** window without any changes, select the **Cancel** button. Also, it is possible to close the window by clicking **Close** .
6. To delete the shift-day schedule from the list, select the title line on the working area; the **Flexible daily schedule** window will appear. Select the **Delete** button. The **Flexible daily schedule** window will be closed and the selected schedule will be deleted.

5.1.5 Flexible weekly schedule

To configure flexible weekly schedule, proceed as follows:

1. Click consistently **Access** → **Time access criteria** → **Flexible weekly schedule** in the Web-interface menu. The window with the working area will be opened:

Add		
Schedule number	Week	Weekly schedule
1	1	1

- To add a new flexible weekly schedule, click the **Add** button; to change or delete the flexible weekly schedule parameters, click the title bar in the working area. The **Flexible weekly schedule** window will be opened:

Flexible weekly
✕

Schedule number:

Begin:

Week:

Weekly schedule:

- In the opened window perform the necessary changes:
 - Schedule number** parameter sets the schedule number;
 - Begin** parameter sets the beginning of the schedule;
 - Week** parameter sets the number of weeks for the schedule;
 - Weekly schedule** parameter sets the time access criteria number of weekly schedules for the schedule.
- To save the changes and send the parameters to the controller, click the **Save** button. The **Flexible weekly schedule** window will be closed.
- To exit the **Flexible weekly schedule** window without saving the changes, select the **Cancel** button. Also, it is possible to close the window by clicking **Close** ✕.
- To delete the flexible weekly from the list, click the title bar in the working area; the **Flexible weekly schedule** window will be opened. Click the **Delete** button. The **Flexible weekly schedule** window will be closed and the selected flexible weekly schedule will be deleted.

5.2 Users

To configure the users' information, proceed as follows:

- Click consistently **Access** → **Users** in the Web-interface menu. The window with the working area will be opened:

Add	Reset Antipass
Account	Full name
2019-11-13T11:25:17	Meinz G.
2019-11-11T08:37:53	Worster M.

- To add a new user, click the **Add** button; to change or delete the user's information, click the user in the working area. The **User** window will be opened:

3. In the opened window in the **Main**, **General rights**, **Individual rights** tabs perform the all necessary changes.
4. Using the **Cards** tab assign to the user an identifier. For this purpose:

Input of reader identifiers:

- Present the card to one of the readers included in the controller configuration. The **Input card** window will be opened.

To save the identifier, click the **Save** button. The **Input card** window will be closed, the identifier will be displayed in the working area.

Manual input of identifiers:

- In the working area click the **Manual input** button. The **Input card** will be opened.
- Enter the card identifier in the **Card number** box. Click the **Save** button. The **Input card** window will be closed, the card identifier will be displayed in the working area.

Add other cards similarly, if needed.

5. Using the **Fingerprints** tab assign to the user the fingerprints. For this purpose:
 - Click the **Activate complement** button and place the finger on the reader device.
 - To delete all the fingerprints, click the **Delete all fingerprints** button. All the fingerprints will be deleted from the controller.
 - To delete the fingerprints from the Mifare card, click **Clear Mifare** button and present the card to the reader. The fingerprints will be deleted from the card.
 - To enroll fingerprints to the Mifare card, click the **enroll to Mifare** button and present the card to the reader. The fingerprints from the controller will be enrolled to the card.
6. To save changes and send the parameters to the controller, click the **Save** button.

6. OPERATING DEVICE CONTROL

To control the operating device and change the operating mode in the direction with associated reader, make following:

1. Click **Operating device control** in the Web-interface menu. The page with working area will be opened:

<ul style="list-style-type: none"> Settings Configuration Access <li style="border: 1px solid blue; padding: 2px;">Operating device control Events Status Service 	Number	Operating device type
	1	Turnstile with operating device
	2	Turnstile with operating device

2. Click the OD bar in the page working area, to which it is necessary to issue the control command. The control window with selected OD will be opened:

Operating device control
✕

Unblocking time:

Direction:

Unblocking type:

Access control mode "Open"

Access control mode "Closed"

Access control mode "Control"

Access control mode "Security"

Block

Unlock

Raise the alarm

Reset the alarm

3. Using the buttons at the bottom part of the window, give the necessary command. The control window will be closed; the command will be passed to the controller. To close the window without submitting command is possible with the **Close** button .



Note:

- When arming, the direction of the OD associated with the reader is set, you select it in the dropdown **Direction** list.
- When you unlock the OD will be unlocked for the time chosen in the drop-down list **Unlock time**.

7. EVENTS

To view the event log of the controller:

1. Click **Events** in the Web-interface menu. The page with working area will be opened:

<ul style="list-style-type: none"> Settings Configuration Access Operating device control <li style="border: 1px solid blue; padding: 2px;">Events Status Service 	Clear	Filter
	Date	Event
	19.11.2019, 16:41:46 (GMT+3)	Passage denial: Identifier is not registered, Operating device 1, direction 1, card 8507436
	19.11.2019, 16:41:44 (GMT+3)	Operating device is locked, Operating device 1, direction 1
	19.11.2019, 16:41:44 (GMT+3)	Passing denial, Operating device 1, direction 1, UID 2019-11-13T11:24:48, card 21478005191
	19.11.2019, 16:41:37 (GMT+3)	Operating device is unlocked, Operating device 1, direction 1
19.11.2019, 16:41:36 (GMT+3)	Operating device is locked, Operating device 1, direction 1	
<< First < Next Previous >		

2. By default, all events stored in the controller memory are displayed, by 20 events on the page. To move through the pages of the event, use the buttons located in the lower part of the working area. The events in the page working area are displayed in reverse chronological order.

- There is possibility of selection in the report of events by categories and time. To do this, click the **Filter** button, the **Filter** window will be opened:

- In the drop-down **Selected categories** list tick the event categories boxes which should be reported. Following categories of events are available:
 - ID Card access;**
 - Access without ID Card;**
 - Security zone status change;**
 - Change input/output state change;**
 - Functioning;**
 - Service.**
- Use the **Range beginning point** and **Range end point** fields to set the period of the report.
- Click the **Apply** button to apply the filter, click the **Cancel** button to cancel any made changes. The **Filter** window closes, the events will be displayed in the report in accordance with the filter settings.
- To delete all events from the controller memory, click the **Clear** button at the bottom part of page working area.

8. STATUS

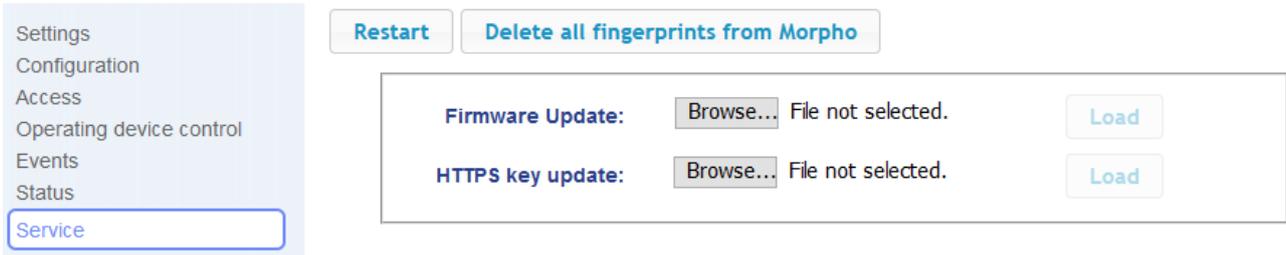
To view the controller status and status of all his resources click **Status** in the Web-interface menu. The page with working area will be opened:

	Object	Status
<ul style="list-style-type: none"> Settings Configuration Access Operating device control Events Status Service 	Device 1, direction 1	Sensor of passage normalized, Device is blocked, Access mode Control
	Device 1, direction 2	Sensor of passage normalized, Device is blocked, Access mode Control
	Device 2, direction 1	Sensor of passage activated, Device is break in, Access mode Control
	Device 2, direction 2	Sensor of passage activated, Device is break in, Access mode Control
	Input 1	normal
	Input 2	normal
	Fire alarm input 256	normal
	Output 1	normal
	Output 2	normal
	Output 3	normal
	Housing	opened
	Jumper IP Mode	removed
	Jumper IP Default	installed
	Using NAND	Yes
	Available on disk	466944kb
	External voltage	12.1, norm
Internal voltage	5.1, norm	

9. SERVICE

For maintenance of the controller:

1. Click **Service** in the Web-interface menu. The page with working area will be opened:



2. To restart the controller, click the **Restart** button.
3. To delete all fingerprints from Morpho, click the **Delete all fingerprints from Morpho** button.
4. To update the controller software (firmware), indicate the location of the software file using the **Browse** button and click the **Download** button.
5. To update the HTTPS key, select the location of the firmware file using the **Browse** and click the **Download** button. The file download progress will begin to be displayed, the controller can only be restarted after the download is completed.

PERCo

Polytechnicheskaya str., 4, block 2
194021, Saint Petersburg
Russia

Tel: +7 812 247 04 64

**E-mail: export@perco.com
support@perco.com**

www.perco.com



www.perco.com