



**TOR 150 SERIES  
PROTECTION AND AUTOMATION  
INTELLIGENT ELECTRONIC DEVICES**

**Operation Manual. General technical requirements**

**AIPB.656122.029 OM1**



---

Relematika, LLC  
Yakovlev Ave. 1, 428020 Cheboksary, Russian Federation  
Tel.: +7 8352 240650, fax: +7 8352 240243  
Web-site: [www.relematika.com](http://www.relematika.com), [www.relematika.ru](http://www.relematika.ru)  
E-mail: [service@relematika.ru](mailto:service@relematika.ru), [info@relematika.ru](mailto:info@relematika.ru)

## **Copyright**

Copyright© Relematika, LLC, Cheboksary, Russian Federation, 2021. All rights reserved. Dissemination or reproduction of this document, or evaluation and communication of its contents is not authorized except where expressly permitted.

## **Purpose of this manual**

The manual describes the technical data, functionality, operation, installation and commissioning procedure for TOR 150 device of Relematika company.

## **Targeted audience**

Protection engineers, mechatronic engineers, commissioning engineers, personnel concerned with setting, monitoring and service of protection equipment, industrial automatic and control facilities within the electrical power systems.

## **Applicability**

This manual is valid for TOR 150 multifunctional IED.

## **Liability statement**

All responsible specialists have checked the contents of this document to ensure the description of both, hardware and software are as accurate as possible. However, deviations from the description cannot be completely ruled out, so that no liability can be accepted for any errors or failures contained in the given document, which content is reviewed regularly. Corrections will be included in following editions. Any suggested improvements are highly appreciated. Relematika, LLC reserves the right to make technical improvements without notice.

## Safety symbols and messages

The warnings and notes contained in this manual serve for your own safety as well as safety of people and property around you. Please observe them!

The following indicators and standard definitions are used:

### DANGER



Indicates an imminently hazardous situation which, if not avoided, will result in death, serious injury or property damage.

### CAUTION



Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury or property damage.

### WARNING



Indicates a potentially hazardous situation which, if not avoided, could result in death, serious injury or property damage.

### NOTE



Indicates information about the device or respective part of instruction manual which is essential to highlight.

## Warning

Only qualified personnel can work on this device. Certain parts of the device inevitably have dangerous voltage. Thorough familiarity with all warnings and safety notices of this manual along with applicable safety regulations is required. Failure to observe these precautions can result in fatality, personal injury or extensive material damage. The successful and safe operation of this device is dependent on proper handling, installation, operation and maintenance by qualified personnel.

### QUALIFIED PERSONNEL



For the purpose of this manual and product, a qualified person is one who is familiar with the installation, construction and operation of the equipment and hazards involved. Following qualifications are needed:

- knowledge to energize, de-energize, clear, ground and tag circuits and equipment in accordance with established safety practices;
- knowledge of proper care and use of protective equipment in accordance with established safety practices;
- proficiency in rendering first aid.

# Content

- 1. Application..... 7**
- 1.1 General technical specifications and characteristics ..... 8**
- 1.1.1 Basic parameters ..... 8
- 1.1.2 Auxiliary power supply ..... 8
- 1.1.3 Transformer energizing inputs ..... 8
- 1.1.4 Binary inputs ..... 9
- 1.1.5 Binary outputs..... 9
- 1.1.6 Electromagnetic compatibility..... 10
- 1.1.7 Insulation resistance..... 12
- 1.1.8 Acceptable operating conditions ..... 12
- 1.1.9 Data communication interfaces ..... 13
- 1.1.10 Reliability parameters..... 13
- 1.2 TOR 150 hardware design and operating characteristics ..... 14**
- 1.2.1 Power supply module ..... 15
- 1.2.2 Binary I/O modules..... 16
- 1.2.3 Input transformer module ..... 17
- 1.2.4 Main processor module ..... 18
- 1.2.5 Local HMI module..... 18
- 1.2.6 Information ports and communication interfaces ..... 20
- 1.2.7 Basic parameters of protection and measuring elements ..... 23
- 1.3 IED functionality ..... 25**
- 1.3.1 Processing of analog input values..... 25
- 1.3.2 Protection functions ..... 25
- 1.3.3 Disturbance recording ..... 26
- 1.3.4 Event recorder..... 28
- 1.3.5 Communication with APCS..... 28
- 1.3.6 Device Synchronization ..... 28
- 1.3.7 Circuit breaker control and diagnostic ..... 29
- 1.3.8 Application in digital substations using IEC 61850 standard..... 29
- 1.3.9 Service software ..... 31
- 1.4 Marking and sealing ..... 32**
- 1.5 Packaging ..... 32**
- 2. Operational guidelines..... 33**
- 2.1 Operating limitations..... 33**
- 2.2 Getting started and commissioning ..... 33**
- 2.2.1 Safety information..... 33
- 2.2.2 Visual inspection ..... 33
- 2.2.3 Installation and connection..... 33
- 2.2.4 Commissioning ..... 33
- 2.3 Access rights setup ..... 34**
- 2.3.1 Basic information ..... 34
- 2.3.2 Prohibiting configuration changes via Ethernet port ..... 35
- 2.3.3 Accounts ..... 35
- 2.3.4 Physical identity ..... 38
- 2.3.5 Connecting and configuring a smart card reader ..... 38
- 2.3.6 List of allowed MAC and IP addresses..... 39
- 2.3.7 Audit log ..... 40
- 2.4 Parameter setting..... 41**
- 2.5 User interface structure ..... 42**
- 2.5.1 User interface..... 42
- 2.5.2 Purpose of control buttons ..... 42
- 2.5.3 Assignment of function buttons ..... 42
- 2.5.4 Stand-by mode ..... 43

2.5.5	User interface menu .....	44
2.5.6	Current mode .....	44
2.5.7	Events .....	45
2.5.8	Disturbance recorder .....	46
2.5.9	Settings .....	47
2.5.10	Testing .....	48
2.5.11	Diagnostics .....	48
2.5.12	Parameters.....	48
2.5.13	IEC 61850 .....	51
2.6	Test Mode .....	52
2.6.1	Test mode for protection functions .....	52
2.6.2	Setting up test mode .....	53
2.6.3	Hardware Test mode .....	53
3.	Maintenance .....	57
3.1	General .....	57
3.1.1	Maintenance cycle.....	57
3.2	Safety precautions.....	57
3.3	Maintenance order and operability checks .....	57
3.3.1	Checking the resistance and insulation strength .....	58
3.3.2	Checking the applied setting parameters and configuration .....	59
3.3.3	Testing the validity of displayed analog values .....	59
3.3.4	Protection parameters (settings, protection functions, measuring elements) check....	59
3.3.5	Test of IEDs functionality when applying and removing auxiliary supply voltage .....	59
3.3.6	Test of IED functionality with external devices .....	59
3.3.7	Test of IED interaction with other low voltage equipment .....	60
3.3.8	Testing the IEDs under load (current and voltage) conditions.....	60
3.4	Failure list and troubleshooting.....	61
3.4.1	Introduction .....	61
3.4.2	Self-diagnostic.....	61
3.4.3	Error codes.....	62
3.4.4	Troubleshooting .....	64
3.5	Disposal .....	66
4.	Transportation and storage.....	67
5.	Manufacturer's warranty .....	68
	Appendix A Ordering structure .....	69
	Appendix B Layout, overall and mounting dimensions (mm).....	70
	Appendix C Inputs and Outputs of the blocks .....	72
	Appendix D Pin designation of communication ports.....	73
	Abbreviations.....	74

**PLEASE READ THIS MANUAL BEFORE ENERGIZING TOR 150 IED!**

This operation manual applies to microprocessor-based protection, automation, control and signalling devices of "TOR 150" type (hereinafter referred to as devices or IEDs) and contains the necessary information for studying the technical characteristics, establishes the rules for its operation, maintenance, storage and transportation.

This operation manual applies to IEDs with a base software version of at least 2.17.

The operation manual consists of two documents: AIPB.656122.029 OM1 and AIPB.656122.029-XXX OM2. The first one - OM1- contains information related to all types of IEDs, such as: technical data, existing IED design descriptions, structure and function of IED modules, operation and maintenance guidelines. The second document - OM2 - contains a description of the functional versions, composed by protection and automation functions and describes operating principles of different protection and automation functions.

The devices are made on a microprocessor element base and are equipped with unified blocks. The corresponding software is downloaded to the IED, which ensures the performance of the necessary functions. The IED has a freely configurable logic, which allows modifying typical functional logic diagrams, taking into account the specifics of the protected object.

Implementation of various communication protocols, such as IEC 61850-8-1 (MMS, GOOSE), ensures integration of the IEDs into substation/station control systems (in further text also SCS).

Reliability and lifetime of TOR 150 IEDs are provided with both the product quality and the compliance with operation conditions, transportation, storage, installation requirements. Therefore, meeting of all the requirements specified herein is obligatory.

Taking into account that Relematika, LLC (in further text Relematika) is continuously developing functionality and design of the IEDs, this operation manual cannot cover all the changes, improving parameters and quality of the product. The company reserves the right to make changes and IED improvements without prior notice to the customer.



## 1. Application

TOR 150 series IEDs are microprocessor-based devices intended for protection, control, automation and monitoring purposes in 6-35 kV power networks. The units are intended for installation in the relay protection switchgears, such as indoor and outdoor switchgears, on the relay protection panels, in the cubicles and on control boards of power plants and substations.

The IEDs can be applied in utilities with AC, rectified AC and DC auxiliary voltage.

The IEDs are freely programmable. Functional logical diagrams are developed by PCAP graphical programming tool, which enables the user to configure binary inputs and outputs, analog inputs, control buttons, LEDs, disturbance recorder, event recorder, user interface, etc. Freely programmable logic allows modifying and additionally developing typical functional logical diagrams, taking into account the special needs of the protected object.

The main application functionality of the IED is represented in the ordering code structure shown in Appendix B.

An example of forming a designation of protection and automation device of 6-35 kV busbar voltage transformer: with four voltage inputs of 100 V, two units of Input/Output circuits, RS-485 interface and Ethernet port 100 Base-T for a rated operating voltage of 220 V, with support of IEC 61850 protocol, alphanumeric display: "TOR 150 N 20 2102 P D1" device.

A number of optional functions, which are not covered by the present manual, can be implemented on special request. All deviations (concerning design and algorithm) from the standard version are described in the project (device) specific documentation.

Overall and mounting dimensions, weight of the device are presented in Appendix B.

## 1.1 General technical specifications and characteristics

### 1.1.1 Basic parameters

Table 1.1: Nominal parameters

Parameter	Value
Rated AC current $I_r$ , A: phase current circuits earth fault protection circuits	5 0,25 or 5
Rated AC voltage (phase-to phase) $U_r$ , V	100
Rated frequency $f_r$ , Hz	50
$U_{aux}$ nominal $U_n$ , V	110/220 DC 110/220 AC 110/220 rectified AC
$U_{aux}$ variation $U_n$ , V	from 88 to 242

### 1.1.2 Auxiliary power supply

Table 1.2: Auxiliary power supply – basic data

Parameter	Value
$U_{aux}$ nominal ( $U_n$ )	(110 – 220) V DC (100 – 220) V AC (100 – 220) V rectified AC
$U_{aux}$ variation	(80 – 110) % of specified range $U_n$ +20% $U_n$ - up to 0,3s
Current pulse at power up <sup>1)</sup>	10 A for 1 ms
Maximum load at DC/AC supply circuits	9 W / 11 VA (stand-by mode – 4 W/8VA)
Start-up time	max. 0,2 s
Interruption time (at $U_n$ , normal operation)	10 s without restarting the IED
$U_{aux}$ connection	No damage occurs to IED when power supply connected with reverse polarity

<sup>1)</sup> It is recommended to protect auxiliary power supply circuit with 15 A rated current automatic fuse.

### 1.1.3 Transformer energizing inputs

Table 1.3: AC current energizing inputs

Description	Value	
Rated AC current $I_r$	5 A <sup>1)</sup>	0.25 A <sup>2)</sup>
Burden at $I_r$ (per phase) <sup>3)</sup>	max. 0.5 VA	max. 0.1 VA
Burden at $I_r$ (per phase) <sup>4)</sup>	max. 13,5 VA typical 10,5 VA	- -
Thermal withstand capability		
At $I_r= 5$ A	4· $I_r$ continuously	100· $I_r$ for 1 s
At $I_r= 0.25$ A	4· $I_r$ continuously	100· $I_r$ for 1 s
Current operating range		
$I_r=5$ A	(0.01 – 40)· $I_r$	
$I_r=0.25$ A	(0.01 – 40)· $I_r$	
Measuring accuracy		
Measured current range	Relative error	

Description	Value
$(0.01 - 0.25) \cdot I_r$	$\pm 3 \%$
$(0.25 - 1.2) \cdot I_r$	$\pm 1 \%$
$(1.2 - 40) \cdot I_r$	$\pm 3 \%$
Additional relative error at:	
$U_{aux} = (80 - 110) \% \text{ of } U_r$	max. $\pm 1 \%$ of value measured at $U_r$
Ambient temperature between $(-40..55)^\circ\text{C}$	$\pm 5 \%$ of mean value measured at $(20 \pm 5)^\circ\text{C}$
Frequency range $(0.9 - 1.1) \cdot f_r$	$\pm 5 \%$ of mean value measured at $f_r$
<sup>1)</sup> Phase or residual currents. <sup>2)</sup> Residual current circuits. <sup>3)</sup> No built-in current/voltage source within IED <sup>4)</sup> Built-in current/voltage source within IED	

Table 1.4: AC voltage energizing inputs

Description	Value
Rated AC voltage $U_r$	100 V (110 V)
Burden at $U_r$ (per phase)	max. 0.5 VA
Thermal withstand capability	$2 \cdot U_r$ continuously $2.5 \cdot U_r$ for 10 s
Voltage operating range	$(0.01 - 2.0) \cdot U_r$
Measuring accuracy:	
Measured voltage range:	Relative error
$(5 - 120) \text{ V}$	$\pm 0.5 \%$
Additional relative error at:	
$U_{aux} = (80 - 110) \% \text{ of } U_r$	max. $\pm 1 \%$ of value measured at $U_r$
Ambient temperature between $(-40..+55)^\circ\text{C}$	$\pm 5 \%$ of mean value measured at $(20 \pm 5)^\circ\text{C}$
Frequency range $(0.9 - 1.1) \cdot f_r$	$\pm 5 \%$ of mean value measured at $f_r$

### 1.1.4 Binary inputs

Table 1.5: Binary inputs

Description	Value
Rated input voltage $U_{rBI}$	$(110 \text{ or } 220) \text{ V DC } ^{1)}$ $(110 \text{ or } 220) \text{ V AC } ^{1)}$
Contact oxide burning current	min. 30 mA for $(10 - 20) \text{ ms}$
Continuous binary input current	max. 3 - 4 mA      max. 3 - 4 mA rms
Continues permitted voltage	max. 300 V      max. 250 V
Reliable operate voltage	max. $0.77 \cdot U_{rBI}$ max. $0.77 \cdot U_{rBI}$
Reliable non-operate voltage	min. $0.6 \cdot U_{rBI}$ min. $0.6 \cdot U_{rBI}$
Setting ranges of operate/reset timers	$(0 - 60) \text{ s}$ , step 1 ms <sup>2)</sup> $(0 - 60) \text{ s}$ , step 1 ms <sup>3)</sup>
<sup>1)</sup> Rating and DC/AC type are to be specified at ordering. <sup>2)</sup> Default settings on each DC binary input are: operate time 10 ms, reset time-5 ms. <sup>3)</sup> Minimum operate time must be 25 ms, reset time - 40 ms	

### 1.1.5 Binary outputs

Table 1.6: Bistable output relays (K1.3)

Description	Value
Rated contact DC voltage $U_{rCON}$	220 V DC
Maximum commutated DC voltage	250 V
Maximum continuous current	2 A

Description	Value
Maximum making current	3 A
Breaking capacity	0.2 A (220 V DC, inductive load, time constant 7 ms)
Operate / Reset time	max. 20 ms
Commutation wear resistance	min. 50000 cycles at resistive load

Table 1.7: Output relays with increased inter-contact gap (relays K1.4, K1.5 on module P0503)

Description	Value
Rated contact DC voltage $U_{rCON}$	220 V DC
Maximum commutated DC voltage	250 V
Maximum continuous current	8 A
Maximum making current	10 A for 4 s at pulse ratio of 10 %
Breaking capacity	0.3 A (220 V DC, resistive load)
Operate / Reset time	max. 10/5 ms
Commutation wear resistance	min. 10000 cycles at resistive load

Table 1.8: Output signalling relays

Description	Value
Rated contact DC voltage $U_{rCON}$	220 V DC
Maximum commutated DC voltage	250 V
Maximum continuous current	8 A
Maximum making current	10 A
Breaking capacity	0.15 A (250 V DC, inductive load, time constant 20 ms)
Operate / Reset time	max. 10/5 ms
Commutation wear resistance	min. 10000 cycles at resistive load

### 1.1.6 Electromagnetic compatibility

TOR 150 remains operative and functional without performance derating under the influence of the following factors, presented in the following table. Abbreviations: SL corresponds to "Severity Level" and PC corresponds to "Performance Criteria".

Table 1.9: Electromagnetic compatibility

Type of test	Type test values	Related reference standards
Electrostatic discharge immunity test: - contact discharge - air discharge	6 kV, 150 pF 8 kV, 150 pF	IEC 61000-4-2:2008, SL=3, PC=B
Radio frequency electromagnetic field immunity test	10 V/m	IEC 61000-4-3:2010, SL=3, PC=A
Power frequency (50 Hz) magnetic field immunity test: - continuous - transient (for 3 s)	100 A/m 1000 A/m	IEC 61000-4-8:2009, SL=5, PC=A
Pulse magnetic field immunity test	1000 A/m	IEC 61000-4-9:2016, SL=5, PC=A
Damped oscillatory magnetic field immunity test	100 A/m	IEC 61000-4-10:2016, SL=5, PC=A

Type of test	Type test values	Related reference standards
Electrical fast transient/burst immunity test: - communication ports - other ports	4 kV pulse (5/50 ns) 4 kV pulse (5/50 ns)	IEC 61000-4-4:2012, SL=4, PC=A
Surge immunity test with 1/50 ns and 6.4/16 ns pulses: - power supply - communication - other ports	4 kV line-to-earth and 2 kV line-to-line 1 kV line-to-earth 4 kV line-to-earth and 2 kV line-to-line	IEC 61000-4-5:2014  SL=4, PC=A SL=3, PC=A SL=1, PC=A SL=4, PC=A SL=3, PC=A
Immunity to conducted disturbances, induced by radio-frequency fields	10 V, f = (0.15 – 80) MHz	IEC 61000-4-6:2013, SL=3, PC=A
Voltage dips, short interruptions and voltage variations:	$\leq 0,2 U_{aux}$ ( $t_{pf} = 5000$ ms); $\leq 0,3 U_{aux}$ ( $t_{pf} = 500$ ms); $\leq 0,6 U_{aux}$ ( $t_{pf} = 200$ ms); $\leq U_{aux}$ ( $t_{pf} = 20$ ms); min $t_{inter} = 500$ ms	IEC 61000-4-11:2004, PC=A
Ring wave immunity test: - single oscillations - repeating oscillations	4 kV line-to-earth; 2 kV line-to-line 2,5 kV line-to-earth; 1 kV line-to-line	IEC 61000-4-12:2006 IEC 61000-4-18:2006, SL=3, PC=A
Harmonics and interharmonics including mains signalling at AC power port, low frequency immunity tests	$\geq 15\%$	IEC 61000-4-13:2002
Voltage fluctuation immunity test for equipment with input current not exceeding 16 A per phase	$U_{aux} \pm 20\%$	IEC 61000-4-14:2009, SL=X, PC=A
Conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz: - continuously - for 1 s	30 V 100 V	IEC 61000-4-16:2009, SL=4, PC=A
Ripple on DC input power port immunity test	$U_{aux} \pm 15\%$	IEC 61000-4-17:2001, SL=3, PC=A
Immunity to variation of power frequency	$fr \pm 15\%$	IEC 61000-4-28:2001, SL=3, PC=A
Voltage dips, short interruptions and voltage variations on DC input power port immunity tests	$\leq 0,3 U_{aux}$ ( $t_{pf} = 1000$ ms); $\leq 0,6 U_{aux}$ ( $t_{pf} = 100$ ms); min $t_{inter} = 500$ ms	IEC 61000-4-29:2000, SL=3, PC=A
Radio-frequency disturbance characteristics	Class A	IEC CISPR 11:2004, IEC CISPR 22:2006

### 1.1.7 Insulation resistance

Unless otherwise specified, all the below values refer to following: ambient temperature within  $(20\pm 5)$  °C, relative humidity within (45 – 80) %, rated AC voltage frequency of 50 Hz.

Table 1.10: Insulation tests

Type of test	Type test values	Related reference standards
Insulation resistance: - between independent circuits - between circuits and earth	> 100 MΩ, 500 V DC > 100 MΩ, 500 V DC	IEC 60255-5:2000
Dielectric test <sup>1)</sup> : - communication circuits - all other circuits	0.5 kV, 50 Hz, 1 min 2 kV, 50 Hz, 1 min	IEC 60255-5:2000
Impulse voltage withstand test: - communication circuits - other circuits	Three positive and three negative impulses $(1.2\pm 0.36)/(50\pm 10)$ μs 1 kV, source energy 0.5 J 5 kV, source energy 0.5 J	IEC 60255-5:2000

<sup>1)</sup> At repeated tests a test voltage should not exceed 85 % of the specified value.

### 1.1.8 Acceptable operating conditions

TOR 150 IEDs are designed for operation in the environmental conditions accordance with IEC 60721-2-6:1990 and Table 1.11, Table 1.12

Place of installation should be protected against water, oil, emulsion splashes and direct solar radiation.

Table 1.11: Required environmental conditions

Parameter description	Value (range)
Maximum altitude above the sea level	up to 2000 m
Maximum permitted ambient temperature	+55 °C
Minimum permitted ambient temperature	-40 °C, (no frost and condensed moisture)
Maximum permitted relative humidity	98 % at 25 °C, non-condensing
Required environmental conditions	non-explosive, free from current-conducting dust, corrosive gases and fumes in concentrations, which could be disruptive for insulation and metals
Pollution degree	degree 1, i.e. no pollution, only dry, non-conductive pollution may occur

Table 1.12: Vibration, shock, bump and seismic tests

Type of test	Type test values	Related reference standards
Vibration response (sinusoidal)	Class 1	IEC 60255-21-1:1988
Vibration endurance	Class 1	IEC 60255-21-1:1988
Shocks response	Class 1	IEC 60255-21-2:1988

Type of test	Type test values	Related reference standards
Shocks withstand	Class 1	IEC 60255-21-2:1988
Bump	Class 1	IEC 60255-21-2:1988
Seismic	Class 1	IEC 60255-21-3:1993
IP code: front part other parts	IP40 IP20	IEC 60529:2013

### 1.1.9 Data communication interfaces

Table 1.13: Ethernet 100Base-TX port technical data

Parameter description	Value (range)
Connector type	RJ45
Maximum transmission segment distance	Up to 100 m

Table 1.14: RS-485 port technical data

Parameter description	Value
Connector type	Plug MSTB 2,5/4 (PHOENIX)
Insulation strength	500 V RMS (1 min)
The number of IEDs in the line	max. 32
Total length of a communication line	max. 1200 m

### 1.1.10 Reliability parameters

Specially implemented software and hardware back-up methods secure correct performance of implemented functionality. Self-supervision system continuously monitors software and hardware with available parameter checkout. In case a persistent failure is detected the IED generates a failure signal indicating the cause of a failure.

Table 1.15: Reliability parameters

Parameter description	Value (range)	Note
Mean time between failures (MTBF)	> 125.000 hours	-
Average unit repair time	0.5 h	Considering that all spare parts are available
Average service life time	At least 15 years	Considering that all operating conditions and maintenance procedures are followed
Average module service time	At least 10 years	-
Probability of failure to operate	$< 3 \cdot 10^{-4}/\text{year}$	-
Probability of false operation	$< 10^{-6}$ hour	-

## 1.2 TOR 150 hardware design and operating characteristics

TOR 150 IED is designed as a programmable logic controller with a central processing unit as a core, which provides interaction between all units included into the device.

TOR 150 IED is housed within a custom rack with different modules. Flush mounting rack is installed on the door of the relay compartment of the switchgear cubicle or on the panel of the protection cubicle with the rear connection of secondary conductors.

Overall, mounting dimensions, weight, layout and control elements arrangement on the front panel are shown in Appendix D.

Designations of contacts for connection to the blocks of binary inputs and output relays are presented in Appendix C. Designations of contacts of communication ports are shown in Appendix D.

TOR 150 IED includes the following modules:

- power supply module;
- input transformer module;
- main processor module;
- local human-machine interface module
- binary input/output modules;
- communication modules.

Electrical connection between modules is made using connectors and flexible conductors. TOR 150 has two versions:

- TOR 150 T – current protection IED;
- TOR 150 N – voltage protection IED.

End users can choose version of IED, quantity of BI modules and type of communication modules depending on the protected object and SCADA requirements.

The front panel contains:

- LED indicators;
- alphanumeric display;
- control buttons;
- USB Type B connectors.

The number and presence of LEDs and control buttons depends on the version of the used display unit.

The rear panel accommodates terminal blocks for connection to measuring, power supply, and signalling circuits as well as communication ports for connecting to different communication systems and a ground screw.

Terminal blocks enable connection of one or two cables of the same type:

- for screw connection with measuring current and voltage circuits: with minimum cross sectional area of 0,5 mm<sup>2</sup>. Maximum summary cross section area of conductors is 6 mm<sup>2</sup>;
- plug-in connectors provide screw connection for one rigid (flexible) cable with maximum 2.5 mm<sup>2</sup> cross section, or two identical cables with maximum cross section area of 1 mm<sup>2</sup> (rigid) or 1,5 mm<sup>2</sup> (flexible) each with a cross section of not less than 0.5 mm<sup>2</sup>.

IED design provides air gaps and insulation distance between the contact pins and the housing not is less than 3 mm over the air and 4 mm over the surface.

Protective earth circuit continuity is ensured in compliance with IEC 60439-1 Standard. Electrical resistance measured between the IED ground screw and any grounded metal part does not exceed 0.1 Ω.



### 1.2.1 Power supply module

Auxiliary AC or DC sources are connected to the IED through the contacts XA1:11, XA1:12. The power supply is galvanically separated from the sensitive electronic parts in a separate compartment, shielded from electromagnetic interference. The characteristics of the auxiliary power circuits are described in 1.1.2.

The IED is ready for operation (after the auxiliary supply source is energized) in 0.2 s.

The IED has a built-in energy storage which allows overcoming power outages up to 10 s without restarting the device. After power interruptions reliable operation of the device is ensured in accordance with the specified algorithms, and the following parameters are saved:

- Device settings and configuration;
- Oscillograms of emergency processes;
- Alarm parameters;
- Overaged circuit breaker;
- Alarm LED status.

The contacts of the output relays of the IED are not falsely closed when the auxiliary power source is energized and interrupted for any duration. The contacts of the output relays of the IED are not falsely closed, and the protection equipment is not damaged by applying reverse polarity DC operating voltage, or during commutations and ground faults in the auxiliary power system.

The IED has advanced power supply opportunities. The internal power circuits of IED can be energized from:

- external DC or AC auxiliary source 110/220 V connected to the power module;
- built-in source (current/voltage) from measuring current transformers. This feature is very useful in substations with AC auxiliary power system, since the AC auxiliary source is unreliable;
- USB port (type B). It can be used to design the IED when no auxiliary source is available. Power is supplied by a laptop and only individual electronic parts of IED are powered.

The built-in current/voltage source is powered by two current inputs of IEDs, connected in series to measuring current transformers (phases A and C). Thus, the power supply inside the IED is powered by the symmetrical load current of more than 2.5 A or from phase-to-phase fault current in the medium voltage network. The fault between phases A-C provides power to the built-in source via two input currents. The fault between A-B or B-C phases supplies energy to the source in only one of the faulty phase.

Reliable IED operation is provided with a total minimum current of 4.5 A only in two phases (auxiliary source de-energized). It means that IED (auxiliary source is de-energized). This means that the IED (no auxiliary voltage) turns on when the phase current or currents in two phases (sum of modules) are greater than 4.5 A. The IED operates normally and actuates the circuit breaker tripping if measured fault current exceeds the overcurrent protection settings.

**Note** - Energy for the tripping coil of CB must be supplied from an external power source (charged capacitor etc.)

It should be noted that the total load per phase is greatly increased in this case. Maximum load is up to 18 VA at rated current, when each of the output relays (10 pieces) is energized. Typical load is up to 12 VA (per phase) at rated current, when only one or two output relays are energized inside the IED.

### 1.2.2 Binary I/O modules

The IED contains one or two I/O modules. The quantity of binary Input/Output modules depends on the protected equipment and is specified in the order sheet.

Each I/O module contains five output relays and five binary input signals (Figure C.1 a, b). Binary inputs and outputs are routed to connectors X1-X4.

Characteristics of binary inputs are described in 1.1.4, output relays - in 1.1.5.

Input binary circuits are intended to operate on DC and AC. The type of operating current (DC or AC) is specified by the setting "Auxiliary power" in the "IED configuration/ Auxiliary power/ I/O board configuration" menu of the "RelayTool" service software (Figure 1.1). When using the device on facilities with a rectified operating current without smoothing, select the type of operating current "Alternating" by the setting.

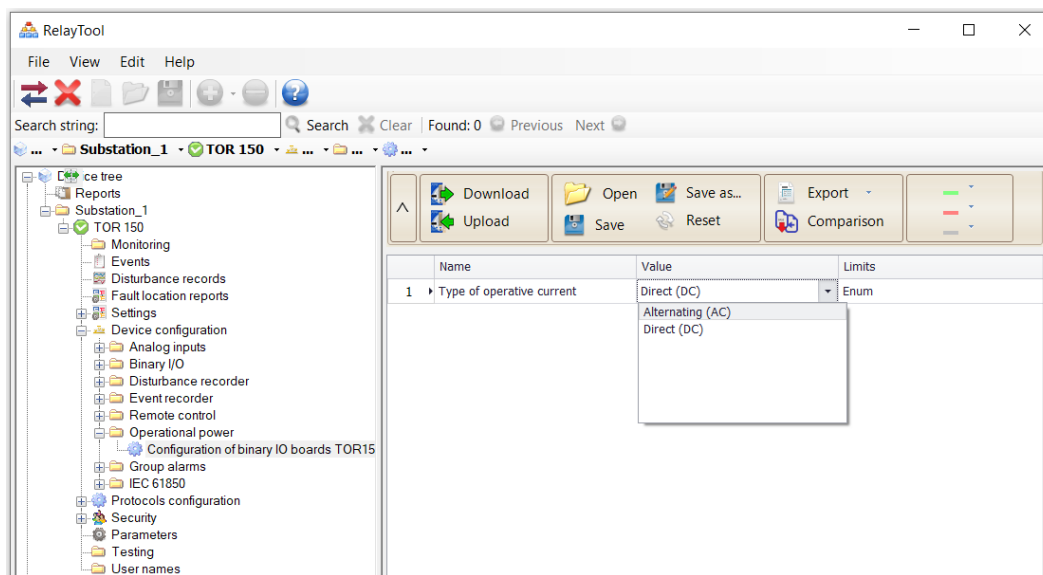


Figure 1.1: Setting the type of operating current

The operating and return times of each binary input circuit are adjustable in the range from 0 to 60 s with a step of 1 ms using the RelayTool service software in the IED configuration/ Digital Inputs/ Outputs/ I/ O boards configuration menu (Figure 1.2).

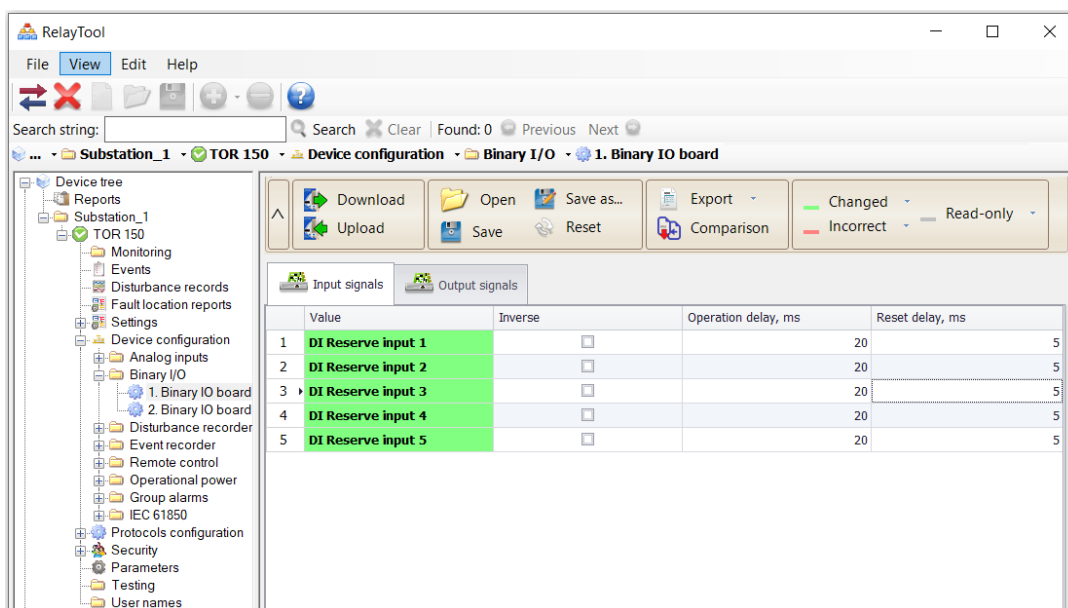


Figure 1.2: Configuring operating and returning of the binary inputs

Binary IO module P0503 includes 5 output relays:

- two output relays with increased inter-contact gap (relay K1.4, relay K1.5). This relay is used to close/open the circuit breakers.

- one bistable relay (relay K1.3). A command latching relay that captures the last control command sent to the circuit breaker (breaker position) and retains this information when no auxiliary power supply is available.

- two signalling relays (relay K1.1, K1.2). The relay K1.1 "Failure" has one normally closed contact. It is controlled by an internal signal from CP module. When the relay is energized and under normal operating conditions, it is in the switched-on state (contact open). The relay resets (contact closes) when a persistent failure detected by self-supervision system occurs or when auxiliary power supply to the IED is lost.

Binary IO module P0504 has five output signalling relays with normally open contact.

For switching currents exceeding the breaking capacity of the output relays, intermediate relays must be used. An intermediate relay is also used when it is necessary to simultaneously switch several independent circuits, i.e., to multiply contacts. The choice of the relay must be made basing on the common operating time. When using intermediate relays, it is recommended to use a spark suppression circuit, which consists of a resistor and a diode connected in parallel with a coil of an intermediate relay. An example of connection is shown in Figure 1.3.

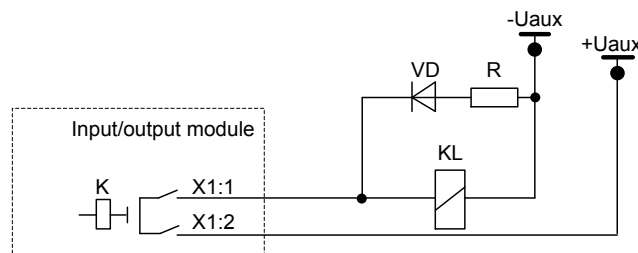


Figure 1.3: Example of connecting an intermediate relay

The resistance of the resistor in the spark suppression circuit is selected from the condition:

$$R=0,1 R_{KL},$$

where  $R_{KL}$  is active resistance of the intermediate relay coil, Ohm.

The power is selected under the condition of short-term current flow (not less than 2 W).

The diode must have parameters with a triple current and reverse voltage reserve:

$$I_{VD}=3 U_{aux}/R; U_{VD}=3 U_{aux},$$

where  $I_{VD}$  – direct current flowing through the diode in the forward direction, A;

$U_{VD}$  – DC voltage applied to the diode in the opposite direction, V.

### 1.2.3 Input transformer module

TOR 150 has one transformer module and up to four input current and/or voltage transformers. Analog circuits from the measuring CT, VT are routed to connectors XA1:1- XA1:10. The current transformer windings are intended for connection to measuring current circuits with a nominal value of  $I_{nom} = 5$  A (phase circuits) and  $I_{nom} = 5/0.25$  A (3I<sub>0</sub> current circuits). The voltage transformer windings are intended for connection to circuits with a nominal voltage value of  $U_{nom} = 100$  V.

The transformer module for current protection TOR 150 T IED contains three input CT and one VT. Two or three CTs can be used for overcurrent protection. For earth fault protection one zero sequence CT and one VT (connected to the open delta winding) can be used.

The transformer module for voltage protection TOR 150 N IED contains four VT inputs connected to the open delta end windings of the voltage measuring transformer.

The characteristics of the analog inputs are presented in section 1.1.3.

#### 1.2.4 Main processor module

The main processor module is the central module in TOR 150 IED and includes the following components:

- central microprocessor;
- random-access memory;
- non-volatile memory;
- real-time clock;
- analog-to-digital converter;
- additional communication module (installed on the rear panel of the IED via connector).

The main processor module is used for acquisition and final processing of analog and digital signals, delivery of control commands to output relays and other IEDs via digital communication channels. The module can also perform the following functions:

- real-time clock;
- time synchronization;
- disturbance and event recording and storage;
- human-machine interface;
- device self-supervision;
- communication with station control system.

The module is intended for collection and final processing of analog and binary signals, sending control commands to the output relays and other devices via digital communication channels.

Non-volatile internal memory stores functional programs, device settings and configuration, disturbance recordings and events. Data storage in non-volatile memory is carried out during the entire service life of the device, regardless of the presence of auxiliary voltage.

The real time clock is used to record the time of the registered events. The accuracy of the real time clock is better than one second (1 s) per day at temperatures from – 40C° to +55C°. In the event of de-energizing, a backup power supply unit is used to power the clock in the logical block.

#### 1.2.5 Local HMI module

The local HMI module contains LEDs, alphanumeric display, control buttons, which are located on the front panel of the IED (Appendix B).

The alphanumeric display consists of six lines of 21 characters.

To display the current state of the device on the front panel (Appendix B) there are:

- three LEDs **READY**, **TEST**, **ERROR** with fixed assignment;
- eight bicolor configurable general purpose LEDs;
- two bicolor LEDs for **I** and **O** buttons with fixed assignment;
- four bicolor LEDs for buttons **K1**, **K2**, **K3** and **K4**.

LED operating modes are described in the following table.

Table 1.16: LED operating modes

LED name	Lighting mode	Operating mode
<b>READY</b>	green	Auxiliary voltage applied, IED operates correctly
<b>TEST</b>	yellow	Test mode of IED
<b>ERROR</b>	red	Persistent internal fault detected by self-diagnosis system
<b>O</b>	red green	Circuit breaker is open (the required color is selected with the settings)
<b>I</b>	red green	Circuit breaker is close (the required color is selected with the settings)
<b>K1...K4</b>	red green	LED operating modes are set during configuration
General purpose	red green	LED operating modes are set during configuration

Using the graphical programming tool PCAP, you can customize the LEDs to indicate the position of the switching devices that are used when performing automatic control functions.

RelayTool service software allows to configure the LEDs for two modes of illumination for different logic signals. One logic signal can be connected to each LED operating mode (Figure 1.4).

Functional button LEDs are also configurable in the RelayTool software (Figure 2.1).

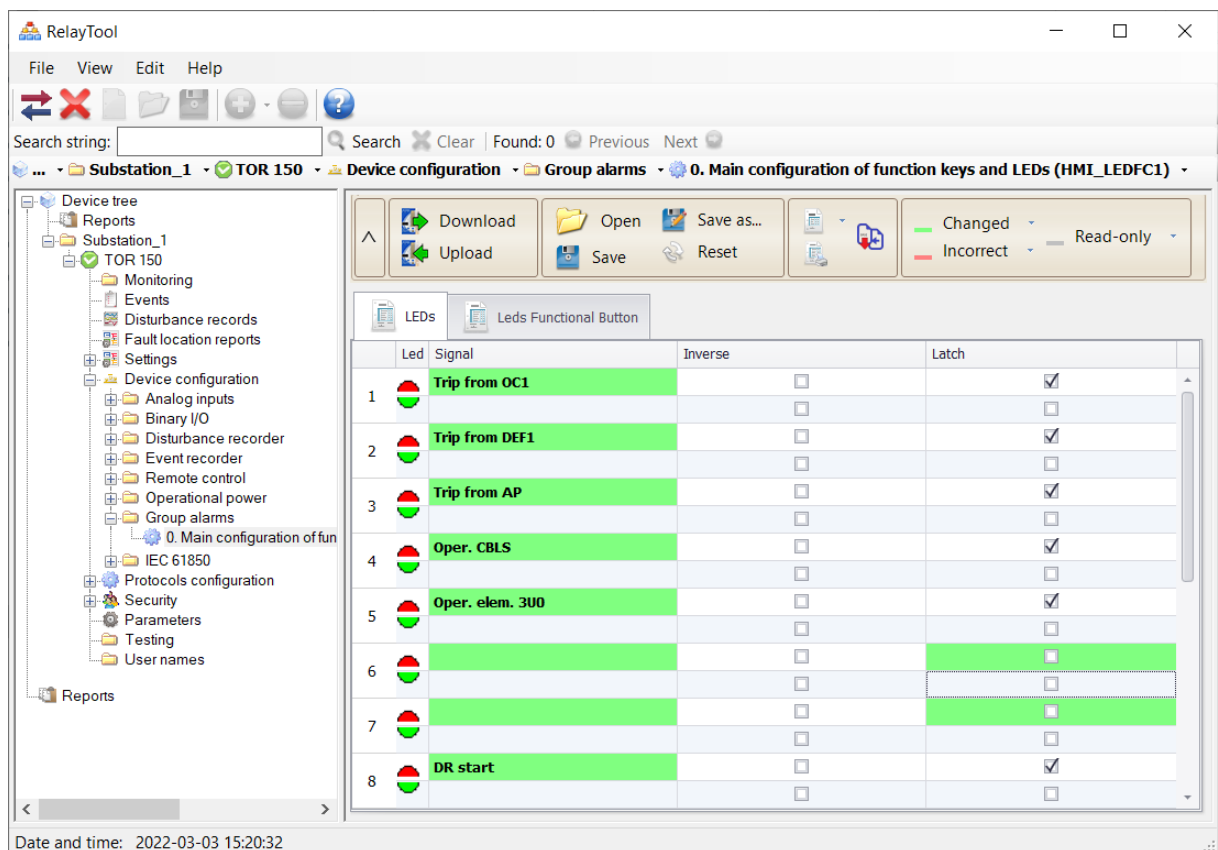


Figure 1.4: LED configuration

LED turns on in the mode of periodic illumination with alternating colors:

- in the presence of signal linked to two modes of illumination of one LED at the same time;
- in the presence of both signals linked to different modes of illumination of one LED.

It is possible to invert the logic signals of the LEDs and fix the state of the LED in the non-volatile internal memory. When the supply voltage is applied, the latching LEDs restore the memorized state.

Latching LEDs can be reset by the **RESET** button on the front panel of the IED, by a signal to the IED binary input, or via communication channels by a command from the automated control system.

The front panel includes also buttons for CB control, signalling as well as programmable keys for automation and protection functions:

- four buttons for navigating through the menu;
- one confirmation button and one command cancel button;
- one button **RESET** to reset the alarm;
- buttons **K1 ... K4** for programmable keys;
- one button **I** to close the CB;
- one button **O** to open the CB;
- one button **🔒** to activate the buttons **I, O, K1... K4**.

The purpose of the user interface buttons is described in 2.5.

## 1.2.6 Information ports and communication interfaces

### 1.2.6.1 General

Communication with APCS and the substation monitoring system is carried out in accordance with the following standards:

- IEC 60870-5-103-2005 "Telecontrol equipment and systems. Part 5. Transmission protocols. Section 103. Companion standard for the informative interface of protection equipment";
- IEC 60870-5-104-2004 "Telecontrol equipment and systems. Part 5. Transmission protocols. Section 104. Network access for IEC 870-5-101 using standard transport profiles";
- MODBUS is a set of standards: Modbus Application Protocol, containing the specification of the application layer and Modbus over serial line, containing the specification of the channels and physical layers;
- IEC 61850 is a set of standards that include peer-to-peer and client-server communication standard, substation design and configuration standard, test methodology standard, environmental requirements standard, design standard. This standard defines object-oriented programming (approach to analysis) of data and services. The standard allows intelligent devices (IEDs) from different vendors to exchange information with each other, bypassing the automated control system, and simplifies its design. Provides GOOSE performance not worse than class P2 according to IEC 61850-5 (13.6.1) and IEC 61850-10.

There is a USB communication port on the front panel, which is intended for connecting a computer via a standard USB 2.0 A-B cable. This port is used to configure and parameterize the device, as well as update the device software. In addition, it is possible to power the device from USB. When the device is powered from USB, the output relays operation may be limited.

**Note** - To connect the IED via the front port, the CP210x USB to UART Bridge Controller driver is required.

There are communication ports (RS-485, Ethernet) on the rear panel of the IED, intended for connecting the device to APCS. These communication ports can also be used to configure

and parameterize the device. Physical interfaces of communication ports, their quantity, and type are determined in the Order Sheet.

Integration of protection devices into substation monitoring system (substation bus) and APCS is provided:

- according to the standard IEC 60870-5-103-2005 or Modbus-RTU, Modbus-ASCII using a serial port (RS-485) brought out to the **XT1** connector;
- according to the IEC 61850-8-1 standard (MMS, GOOSE), IEC 60870-5-104-2004, Modbus-TCP using Ethernet ports (100 Base-T) brought out to the **XT3** and **XT4** connectors. When operated using the IEC 61850-8-1 standard, the data structure complies with IEC 61850-7.

Ethernet ports **XT3** and **XT4** support IEC 62439-3 redundancy (PRP).

Table 1.17 presents options for the interface of communication ports.

Table 1.17: Communication port options

Rear connector designation	Interface type
XT1	RS-485 (ACS)
XT2	Reserve
XT3	Ethernet 100 Base-T
XT4	Ethernet 100 Base-T

Baud rate for the ports with different interfaces is:

- up to 100 Mbps for 100 Base-T Ethernet;
- up to 0,2 Mbps for RS-485;

Communication port connector designations are shown in Appendix D.

#### 1.2.6.2 Assignment and technical data of communication ports

##### 1.2.6.2.1 Port with Ethernet interface 100 Base-T

The version of the port with Ethernet 100 Base-T interface is used to connect the IED to a local area network of an enterprise via a twisted pair communication line. The technical data of the port are given in Table 1.18, the purpose of the connector contacts presented is presented in Table 1.19.

Table 1.18: Port technical data

Parameter	Value
Connector type	RJ45
Maximum transmission distance	Up to 100 m

Table 1.19 : Connector pin assignment

Pin	Signal	Assignment
1	Transmission + (TX+)	Transmitting a positive signal by the IED
2	Transmission – (TX-)	Transmitting a negative signal by the IED
3	Receive + (RX+)	Receiving a positive signal by the IED
6	Receive – (RX-)	Receiving a negative signal by the IED

Recommended:

- to connect an intermediate protection device of RG5 or RG6 type to protect against electromagnetic interference via communication ports of the Ethernet IED (twisted pair);
- to install ZCAT 2035-0930 filter on the RG5 or RG6 cable directly in front of the IED port for additional protection against electromagnetic interference;
- to carry out laying of communication cables in boxes or shielding covers;

- to use a shielded twisted pair cable with a shielded RJ45 connector.

**Note** - RG5, RG6 devices, and ZCAT 2035-0930 filter are not included in the IED delivery kit and are ordered separately.

**Attention!** When connecting PC to the IED via Ethernet ports, you must specify all subnet parameters in the communication settings, including "Gateway" parameter to provide correct operation (0).

#### 1.2.6.2.2 Port with RS-485 interface

This version of the port with RS-485 interface is used to organize a half-duplex exchange of information with the IEDs via a two-wire communication line based on a twisted pair. This communication method is recommended for use with a relatively small number of devices at simple facilities. The purpose of RS-485 port connector contacts is shown in Table 1.20. The technical data of the port are presented in Table 1.21.

A typical connection scheme provides for parallel connection of IEDs to a communication line of a voluntary topology, taking into account the restrictions presented in Table 1.21.

The port operation is provided by a two-wire connection scheme of the same-named contacts; to ensure the potential equalization of the signal ground, it is recommended to use a third conductor (for example, the conductor of an unoccupied cable pair). In addition, to reduce signal reflections and increase noise immunity, terminating resistors should be installed at the ends of the communication line. The value of the terminating resistor should be equal to the characteristic impedance of the cable being used. A typical value for a twisted pair RS-485 is 120 Ohm. The RS-485 port of the IED has a terminating resistor (with resistance of 120 Ohm). To connect the terminating resistor to the communication line, a jumper should be installed in accordance with Figure D.1 Appendix D. The cable shield must be grounded on both sides from the IED side by the ground screw located on the rear panel next to the RS-485 port.

Table 1.20: Connector pin assignment

Pin	Signal	Assignment
1	Common	Signal ground
2	DATA B (D+)	Positive data input/output
3	DATA A (D-)	Negative data input/output
4	R	Terminating resistor pin

Table 1.21: Port technical data

Parameter	Value
Connector type	Male MSTB 2,5 (PHOENIX)
Insulation strength	1500 V RMS (1 min)
Number of devices in line	Up to 32
Total length of communication line	Up to 1200 m



## 1.2.7 Basic parameters of protection and measuring elements

### 1.2.7.1 Reset factors of measuring elements

The values of the basic reset factors of the measuring elements are given in Table 1.22 .

Table 1.22: Measuring element reset factors

Parameter	Value
Reset factor of overcurrent and overvoltage measuring elements, at least	0,9
Reset factor of undercurrent and undervoltage measuring elements, does not exceed	1,1

### 1.2.7.2 Operating and reset times

Operating (reset) time of over- (under-) current and voltage measuring elements does not exceed 30 ms during the supply of corresponding  $3 I_{oper}$  or  $3 U_{oper}$  and does not exceed 40 ms during the supply of  $1,2 I_{oper}$ .

Reset (operating) time of over- (under-) current and voltage measuring elements does not exceed 35 ms during the reset of the input current from  $10 I_{oper}$  to zero or voltage from  $3 U_{oper}$  to zero.

Operating time of the CBFP measuring elements does not exceed 25 ms when applying  $2 I_{oper}$ , reset time during the reset of the input current from  $30 I_n$  to zero – 20 ms.

Operating (reset) time of maximum (minimum) measuring elements reacting to the change in frequency does not exceed 120 ms.

Reset (operating) time of all measuring elements reacting to the rate of frequency change does not exceed 150 ms.

Reference mean relative error at the protection time delay does not exceed:

- $\pm 30$  ms with a time delay of less than 5 s;
- $\pm 1\%$  of the setting with a time delay of more than 5 s.

**Important!** Time delays are pure times that do not include the operating times of the measuring element, protection start, logic diagram operation, and operation of the output relay.

### 1.2.7.3 Accuracy of measuring elements

#### 1.2.7.3.1 Current and voltage measuring elements

Reference mean error of operating current (voltage) of current measuring elements (voltage, except for the third harmonic voltage) does not exceed  $\pm 3\%$  of the setting.

Reference mean error of the third harmonic voltage measuring elements does not exceed  $\pm 5\%$  of the setting.

Additional error of operating current (voltage) of current (voltage) measuring elements at temperature difference in operating temperature range does not exceed  $\pm 5\%$  of mean value, defined at temperature of  $(20 \pm 5) ^\circ\text{C}$ .

Additional error of operating current (voltage) of current (voltage) measuring elements at frequency difference in the range from 0.9 to 1.1  $f_{nom}$  does not exceed  $\pm 5\%$  of mean value, defined at nominal frequency.

#### 1.2.7.3.2 Frequency measuring element

Reference mean error of operation threshold of frequency measuring element does not exceed  $\pm 0.02$  Hz.

Additional error of operating threshold of frequency measuring element at temperature difference in operating temperature range does not exceed  $\pm 0.02$  Hz of mean value, defined at temperature of  $(20 \pm 5) ^\circ\text{C}$ .

#### 1.2.7.3.3 Frequency rate of change measuring element

Reference mean error of operation threshold of all frequency rate of change measuring elements does not exceed  $\pm 0.15$  Hz/s.

Additional error of operating threshold of all frequency rate of change measuring elements at temperature difference in operating temperature range does not exceed  $\pm 0.15$  Hz/s of mean value, defined at temperature of  $(20\pm 5)$  °C.

### 1.3 IED functionality

The IED performs built-in functionality for relay protection, automation, signalling, and control of power facilities, as well as measurement, registration, disturbance recording and communication in accordance with provided software and hardware. Basic software together with library functions allows communication between the application software and the IED hardware platform. The application software ensures execution of the protection scheme, which is designed using a graphical programming tool.

The default logic diagram is set at the manufacturing plant and has a flexible algorithm that can be changed for a specific project during commissioning. The functional logic diagram of the device is described in the following document AIPB.656122.029-XXX OM2.

#### 1.3.1 Processing of analog input values

Analog signal processing algorithm ensures communication with ADC unit, calibration, filtering, calculation and delivery of various measured analog values. During calibration process, it is possible to adjust input CT and VT signal values by their amplitude and phase angle. In general, TOR 150 enables measurement and calculation of current, voltage, network frequency values as well as corresponding amplitude and RMS values, phase angles, symmetrical and transient signal components with possibility to display and transfer them via communication channels. A graphical programming tool PCAP comprises a sufficient set of mathematical elements for calculation of all the required parameters, while the hardware platform makes it possible to connect current, AC and DC voltage power sources, depending on TOR 150 version and functionality.

#### 1.3.2 Protection functions

Depending on the version, various relay protection functions can be implemented in the device, the description of which is presented in the document for a specific version of the device AIPB.656122.029-XXX OM2.

IEDs includes a list of basic and additional functions of relay protection and automation, monitoring and control of different power system elements such as overhead or cable lines, small distribution transformers, small asynchronous motors and other power system elements within the voltage range from 6 to 35 kV on the basis of the following protection functions:

- over/under current protection;
- over/under voltage protections;
- over/under frequency protections;
- circuit breaker control functionality.

Current protection IED TOR 150 T has a set of non-directional overcurrent protection and earth fault protection.

TOR 150 N IED contains a set of over/undervoltage and frequency protections.

### 1.3.3 Disturbance recording

TOR 150 IED includes disturbance recording functionality intended for recording of disturbances with a view of their further analysis. Disturbance recordings are stored in COMTRADE® format (IEC 60255-24:2013). PC based RelayTool software enables selection of disturbance recorder parameters as given below in Table 1.23. Up to 29 starting conditions can be set by proper selection of starting signals. Four types of starting modes for each of the starting signal are provided (see Table 1.24). Starting conditions for each separate disturbance recording can be viewed both via local HMI and via RelayTool software.

Table 1.23: Disturbance recorder parameters

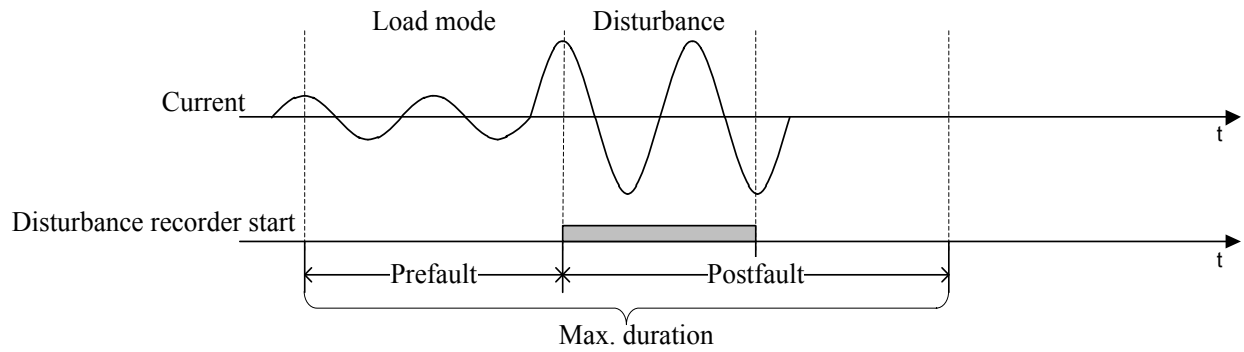
Parameter (display on HMI)	Range	Description
Pre-fault recording time (Prefault)	(100-1000) ms step 100 ms	Pre-fault recording time (before the first starting condition occurred)
Post-fault recording time (Postfault)	(100-5000) ms step 100 ms	Post-fault recording time (after starting condition disappeared)
Maximum allowed recording time (Max.duration)	(1000-10000) ms	Maximum disturbance recording time, Should be more, than a sum of parameters <b>Prefault</b> and <b>Postfault</b>
Sampling rate	1000, 2000 Hz	Signal sampling rate

Table 1.24: Disturbance recorder starting conditions

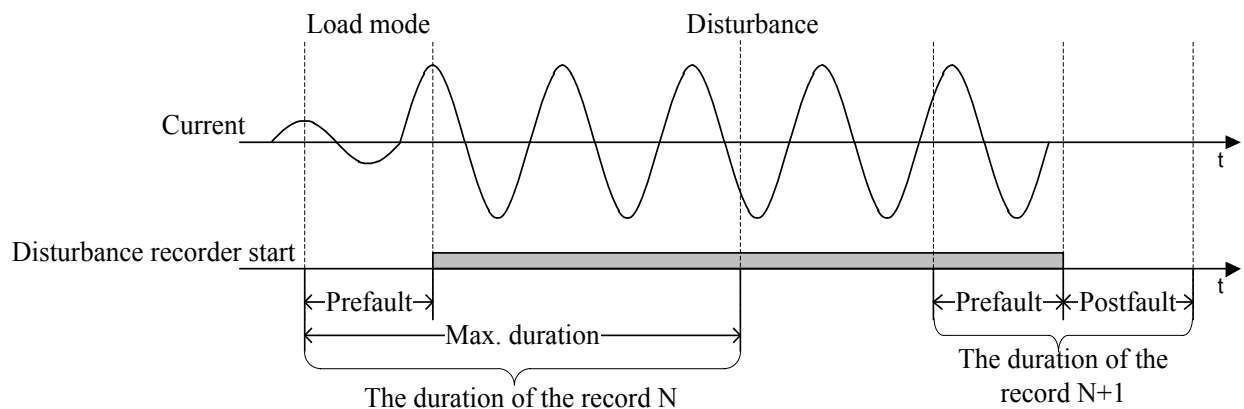
Start signal type	Description
DR start at signal change	Disturbance recording duration is set by recording parameter values <b>Prefault</b> and <b>Postfault</b> (Figure 1.5a)
DR start at signal appearance	
DR start at signal loss	
Continuous DR starting	Disturbance recording duration is determined by the duration of starting signal with addition of <b>Prefault</b> and <b>Postfault</b> values. Maximum duration is limited by the value of parameter <b>Max.duration</b> . If disturbance recording duration exceeds <b>Max.duration</b> , then disturbance recording terminates. After that, when starting conditions disappear, an additional disturbance recording is made, duration of which is determined by the value of recording parameters <b>Prefault</b> and <b>Postfault</b> (Figure 1.5b)

The capacity of disturbance recorder depends on the number of recorded signals. Each of the disturbance recordings can have the duration and sampling rate presented in Table 1.23. The disturbance recorder has an automatic archiving function. The number of stored disturbance recordings is at least 30 with maximum duration up to 10 s. The maximum number of stored disturbance recordings is no more than 200. The recording of oscillograms is organized in such a way that when an overflow occurs, the oldest disturbance recording is erased and a new one is written in its place. When the starting conditions are met, all binary input and output signals and starting conditions are automatically recorded. It also provides a record of all measured and selected calculated values and up to 256 additional logical signals, the composition of which is set when configuring the logical part. Input binary signals are recorded after expiration of operating and return time of the corresponding binary inputs. Signals that give commands to operate the corresponding output relays of the IED are recorded as binary output signals.

The disturbance recorder operating algorithm for different trigger modes is schematically presented in the Figure 1.5.



a) Recorder start upon signal change, rise, reset



b) Continuous start of the disturbance recorder

Figure 1.5: Disturbance recorder operating algorithm

When a start signal changes on the fact of change, occurrence, or disappearance of the signal, the previous mode is written into the memory, the duration of which is set by the "**Pre-mode**" parameter. After the end of starting the disturbance recorder, the recording of the mode continues for the time specified by the "**Post-mode**" parameter. The duration of one disturbance recording is determined by the value of the recording parameters "Pre-mode" and "Post-mode".

When a long start signal appears, the disturbance recording is written in the memory, equal in duration to the sum of the start signal duration and the values of the recording parameters "**Pre-mode**" and "**Post-mode**". When the duration of the oscillogram exceeds the parameter "**Max. duration**", its recording ends. After that, when the start signal disappears, an additional oscillogram is recorded, equal in duration to the sum of the "**Pre-mode**" and "**Post-mode**" parameters (Figure 1.5 b).

To prevent cyclic overwriting of the non-volatile internal memory in the event of bounce of any start cause, an additional interlock is provided. If in total for more than 1 hour any start cause was in the triggered state for more than 20% of the time, then blocking is performed. The lock is returned with a subsequent decrease in the total duration to 10%.

Uploading of disturbance recordings is carried out with the help of ACS or specialized software, as well as according to the IEC 61850-8-1 MMS protocol. It is also possible to read disturbance recordings via FTP. For preliminary and subsequent analysis of disturbance recordings, the function of obtaining a report on the recorded waveform can be used using the Quick View menu item, which contains brief information about the start time, the duration of the disturbance recordings, the reasons for the start, the settings used, etc.

At the end of the name of the signal that triggered the disturbance recorder, information about its value at the moment of start is added in brackets: "(1)" - the start occurred when a single logical value appeared, "(0)" - when the value was zero.

### 1.3.4 Event recorder

IEDs include an event recorder, intended for time tagging of binary signals triggering from 0 to 1 and vice versa, which are used for further analysis of protection, measuring elements, logic, etc. during different system events. Time tagging accuracy is 1 ms.

Maximum capacity of event recorder is 1500 events, which are stored in ROM. Event storage is performed according to the FIFO principle. Up to 256 different logical signals can be recorded; the event list is defined by RelayTool.

All events with their time-tags can be viewed via local HMI, all events can be sent to APCS or SMS system. Specified software is used for uploading the event log.

### 1.3.5 Communication with APCS

Integration of protection devices into the automated process control system is shown in Table 1.25.

Table 1.25: Integration of protection devices

Standard	Port type	Connector designation
IEC 60870-5-101-2006	RS-485	XT1
IEC 60870-5-103-2005		
Modbus-RTU, Modbus-ASCII		
SPA-Bus		
Modbus-TCP	Ethernet	XT3 and XT4
IEC 60870-5-104-2004		
IEC 61850-8-1 MMS		
IEC 61850-8-1 GOOSE		

The procedure for configuring communication interfaces is presented in the document AIPB.05.15.015 34 "Parameterization and monitoring program for relay protection and automation devices RelayTool. User manual".

The service software is used to configure the remote control commands. The maximum number of control commands is 32.

The list of parameters and events for transferring data to the APCS depends on the implementation of a specific project (functional logic diagram) and the functional blocks used. The choice of parameters and settings transferred to the APCS is carried out at the stage of project implementation in terms of APCS. For a non-typical functional logic diagram or a diagram that has undergone changes during commissioning, a list of parameters is set directly during commissioning.

### 1.3.6 Device Synchronization

Synchronization of the real time clock of the IEDs is carried out by means of IEC 60870-5-103-2005, IEC 60870-5-104-2004, IEC 60870-5-101-2006, Modbus, SPA-Bus, NTP/SNTP, NMEA0183.

**Note** - The IED has the ability to adjust the time through HMI, synchronization from the internal real-time clock and through the BDUBus protocol.

Synchronization parameters are configured in the IED menu **Synchronization** (2.5.12.3).

Synchronization via NTP / SNTP is carried out via Ethernet ports **XT3** and **XT4**, NMEA0183 - via serial port **XT1**.

### 1.3.7 Circuit breaker control and diagnostic

TOR 150 has advanced CB control opportunities. End user can close/open of CB via:

- push buttons on the front plate of IED. There is the separate button prevented some spontaneous "Close/Open" operation;
- command generated by APCS;
- command from external close/open switch connected to the binary input module P0503.

Auxilliary control circuits of CB (trip coil, close coil) are monitored by two inputs of P0503 module. Circuit breaker control system monitors different malfunctions in this circuits (breaking and short circuits) and generates a signal for IRF output relay. Diagnostic algorithm monitors the values of operating current as well as close/open times of the CB and stores them in the memory of the IED. In addition, the algorithm calculates residual mechanical life and commutation life of the circuit breaker (for each phase).

### 1.3.8 Application in digital substations using IEC 61850 standard

Device integration in digital substations is ensured with the help of IEC 61850 standards.

#### 1.3.8.1 Communication interfaces for IEC 61850 support

IED support for IEC 61850 is defined in the IED Order Sheet. For the description of characteristics of the Ethernet ports, see 1.2.6.2.

The station bus ports are configured via the menu item **Ethernet 1** (2.5.12.1.2).

The station bus ports support the IEC 62439-3 PRP redundancy protocol to ensure reliable data transmission and reception. The PRP mode is selected via the **Mode** menu.

Additionally, the station bus ports support virtual network (VLAN) mode for traffic management in the digital substation. Up to sixteen VLAN numbers are allowed. Enabling and disabling VLANs, as well as configuring ports to belong to VLAN is carried out in the corresponding Ethernet menu item.

#### 1.3.8.2 IEC 61850-8-1 MMS protocol support

The IEC 61850-8-1 MMS protocol is supported over the station bus ports. The IED supports up to six simultaneous connections to the IED using the IEC 61850-8-1 MMS protocol.

The IED supports IEC 61850 standard services using the following main functions:

- getting device structure and reading data;
- working with datasets;
- working with reports;
- control;
- reading oscillograms.

The IED handles the quality attributes of each of the signals using internal diagnostics.

##### 1.3.8.2.1 Device structure retrieving and data reading

IED provides services for obtaining the structure of logical devices and logical nodes implemented in the IED, objects and data attributes, types and classes of logical nodes and data, parameters of control blocks.

##### 1.3.8.2.2 Working with datasets

The device supports services for working with datasets. Static and dynamic data sets, created in the process, are implemented within the framework of the standard.

The dataset can include any elements of the device structure.

#### 1.3.8.2.3 Working with reports

The device supports reporting services. Buffered and unbuffered report types are implemented.

Report parameters can be configured via the service software or directly by the client application.

#### 1.3.8.2.4 Control functions

The device supports all control models provided by the standard:

- status-only (status only);
- direct-with-normal-security (direct control with normal security);
- sbo-with-normal-security (SBO control with normal security);
- direct-with-enhanced-security
- sbo-with-enhanced-security (SBO management with enhanced security).

The control model can be changed using the service software in the IEC 61850 IED configuration. By default, all controllable elements are set to the "direct-with-normal-security" control model.

#### 1.3.8.2.5 Reading the disturbance recordings

The device supports a service for working with files, which provides reading of disturbance recordings from the device via MMS protocol. Operations of deleting and writing the files are not provided by the device software.

Disturbance recording files can be transferred either as separate files in COMTRADE format, or as a zip-archive, depending on the archiving settings.

#### 1.3.8.2.6 IEC 61850-8-1 GOOSE protocol support

The IED provides support for IEC 61850-8-1 GOOSE protocol via the station bus ports.

The IED provides receiving and sending of up to 16 GOOSE messages with the size of up to 100 signals each via the station bus ports.

Using GOOSE messages, the IED is able to receive and send logical signals (one-point and two-point states) in an arbitrary data structure (determined by the configuration).

Reception of signals using GOOSE messages is performed with a quality control of the signals themselves and control of the test flag.

The time between receiving a signal and sending it in a GOOSE message is no more than 10 ms via the station bus.

**Note** - GOOSE messages contain a mandatory VLAN number, which is set in the service software. When VLAN is enabled on the station bus ports, it is necessary to configure the supported VLAN numbers on the Ethernet ports, otherwise GOOSE messages with VLAN number that does not set in the port parameters will not be transmitted or received.



### 1.3.9 Service software

#### 1.3.9.1 RelayTool software for monitoring and basic configuration

RelayTool software is a PC based software tool, which has been designed to:

- monitor Intelligent Electronic Devices on the site;
- view and edit settings, fix their changes and compare different setting files;
- download and analyze disturbance recordings via BSCOPE software, manual trigger of disturbance recording, change disturbance recorder parameters;
- monitor signals (view their current values), diagnose communication channels with IEDs;
- download and view event logs;
- configure different signals towards binary inputs, outputs, LEDs, disturbance recorder, event recorder, APCS communication protocols and etc.;
- authorize users.

For details, refer to RelayTool User manual.

#### 1.3.9.2 PCAP software for flexible logic programming

PCAP software is a PC based software tool, which is designed to:

- create functional logic diagrams using graphical elements;
- analyze, validate and convert schemes to IED files;
- create new measuring modules and functional blocks;
- program analog processing of measured values;
- configure of analog inputs, binary inputs and outputs, LED indication for disturbance and event recorders, signals for APCS communication and etc.;
- determine the appearance of user-defined HMI;
- edit parameter structure;
- upload/download diagrams to/from IED;
- authorize users.

For details, refer to PCAP User manual.

#### 1.3.9.3 BSCOPE software for disturbance record analysis

BSCOPE software is a PC based software tool, which is designed to:

- read recordings stored in COMTRADE<sup>®</sup> format (IEC 60255-24:2013);
- display stored recordings of analog and binary signals;
- calculate and display analog signals, phases and modules;
- calculate and display power frequency, symmetrical components;
- calculate and display user defined signals;
- plot phasor diagrams and hodographs;
- print recordings.

For description refer to BSCOPE User manual.

## **1.4 Marking and sealing**

TOR 150 has labelling in accordance with design documentation and IEC 60255-27:2005, which is done in a way providing its clarity and preservation during the life time.

Each IED has a label on the rear panel, which shows:

- manufacturer trademark;
- name and notation of the device;
- rated auxiliary supply voltage;
- binary inputs rated voltage;
- manufacturing date (month, year);
- serial number of the device;
- “Made in Russia” mark;
- sign of product conformity.

Shipping container is labelled with handling signs “Fragile”, “Keep dry”, “Top”.

Labelling of transportation box, when the IED is shipped separately (not within the relay cubicle), contains also:

- recipient name;
- shipping address;
- device notation;
- device serial number;
- additional information specified by the ordering documentation.

Device design does not provide sealing.

## **1.5 Packaging**

TOR 150 packaging is done in accordance with Relematika design documentation and IEC 60255-27 for storage and transportation conditions. Allowed storage time presented in Sec.4.

## 2. Operational guidelines

### 2.1 Operating limitations

Device operation and maintenance should be performed according to these instructions. Operating conditions concerning the influence of climatic and mechanical factors shall comply with the requirements as to 1.1.7.

IED possibility to operate under the conditions, which differ from the specified ones should be coordinated with Relematika company.

## 2.2 Getting started and commissioning

### 2.2.1 Safety information



When getting started and commissioning one should be guided by all applicable instructions and directives as well as present operation manual instructions.

Only specially trained personnel should be admitted for installation, maintenance and operation of devices.

Removing/inserting of modules from/to the IED and working on its connectors should be performed only on a de-energized device.

Before power-on and during operation, the IED should be reliably earthed by the ground screw, placed on the IEDs rear panel, to the earthing loop (bay, cubicle case) with the shortest earthing path by a copper wire of at least 4 mm<sup>2</sup> section area.

### 2.2.2 Visual inspection

Put the packed IED on a horizontal surface, guided by the manipulation sign "Top!". Remove the transport package and assure that its content corresponds to the packaging list.

Examine the delivered IED to ensure that it has no mechanical, package damages, occurred during transportation. Check that marking is available and not damaged.

In a case of any deviations or damages of the device, Relematika or its official representative should be informed immediately.

### 2.2.3 Installation and connection

Overall and installation dimensions are specified in Appendix B. Install the IED accordingly to its location.

Connect ground wire as to 2.2.1.

Connect the IED according to approved project and present operating instructions. Connection should be carried out with the wires as it is described in 2.2.1.

### 2.2.4 Commissioning

At delivery, each IED has default factory settings. During its commissioning all the settings should be checked and, if required, changed according to 2.4.

In order to put the unit into commissioning, all the required operations, specified in Table 2.3 for testing at initial power-on should be performed.

When shipping the IED as a part of relay protection cubicle, all the required tests for the cubicle at initial power-on should be performed in accordance with the attached operating documentation.

## 2.3 Access rights setup

### 2.3.1 Basic information

Authorized access to IED functions is implemented via user groups with different access rights, as presented in the Table 2.1.

Table 2.1: User groups

Group name	Group description	Group user by default	Default password
<b>Relematika</b>	Group intended for manufacturer's specialists during service works and etc. Contains only one user	Relematika	*
<b>Admin</b>	Group used for adding and deleting users in groups <b>Relay specialists, Operating personnel, Guests</b>	Admin	admin
<b>Relay specialists</b>	Group, allowing functions for relay protection operating and commissioning staff	Specialist	1
<b>Operating personnel</b>	Group, allowing functions for operating staff. Contains at least one user	Operator	1
<b>Guests</b>	Group, allowing basic (reading) functions. Contains only one user	Guest	–
* Accessible only to Relematika specialists.			

Basic access rights to IED functionality via local HMI are presented in the following Table 2.2.

Table 2.2: Access rights to IED functionality

HMI function	RM	A	R	O	G
LED indication reset via <b>RESET</b> button	+	–	+	+	+
<b>I, O</b> and <b>K1, K2, K3, K4</b> buttons usage	+	–	+	+	–
Event list clearing	+	–	–	–	–
Disturbance records clearing	+	–	–	–	–
Disturbance recorder manual start	+	–	+	–	–
Settings group editing/activation/creation/deleting	+	–	+	–	–
Test output signal selection	+	–	+	–	–
<b>Test/Operation</b> mode selection, test mode parameters changing	+	–	+	–	–
LED test	+	–	+	–	–
Hardware test	+	–	+	–	–
Communication port adjustment	+	–	+	–	–
<b>Date/Time</b> adjustment	+	+	+	+	+
Synchronization methods adjustment	+	–	+	–	–
User and password editing	–	+	–	–	–



In Table 2.2 the following abbreviations of groups are used: RM – “Relematika”, A – “Admin”, R – “Relay specialists”, O – “Operative personnel”, G – “Guests”.

The access right named "Relematika" can only be used by the developer's specialists when performing maintenance work on the IED. As part of the group performing this role, there is one built-in account "Relematika", which has full access to all functions and data of the IED. The user cannot add accounts to the "Relematika" group and use or delete the built-in "Relematika" account. However, the

user has the possibility of disabling this role, making it impossible to perform any actions on behalf of the "Relematika" user. This action is available to the users of Administrator group. In order to minimize the user rights, it is not recommended to enable the "Relematika" role before the start of IED maintenance.

The access right named "Administrator" allows to configure security functions and obtain information about their operation. Only users of this group can manage other accounts. If it is impossible to get access to a user of the "Administrator" group (for example, if the corresponding password has been lost), you should contact the developer's technical support service. To prevent the described situation, it is recommended to use a set of organizational and technical measures, including, for example, the following:

- appointment of employees responsible for using the "Administrator" role;
- appropriate training and knowledge testing of designated employees;
- adding additional (backup) accounts to the "Administrator" group;
- backing up account passwords in sealed envelopes and keeping records of the use/ opening of these envelopes in the appropriate journal;
- ensuring the storage of reserved passwords in a separate lockable vault and securing responsibility for access to it.

The access right named "PAC" provides the ability to access all production functions of the PAC IED, their parameters and corresponding data, excluding the capabilities of the "Administrator" group.

The access right named "Operational personnel" provides access to the basic production functions of the PAC IED, excluding the capabilities of the "Administrator" group.

The access right named "Guest" allows to receive data about the IED's operation and perform functions not related to information security capabilities. The built-in Guest account does not have a password, since the functions and data available on its behalf are publicly available.

When operating power is supplied to the IED, the "Guest" user is installed in the system. The user can be selected through the Settings/Access menu (2.5.12.4) or through the dialog box that appears when trying to control a function for which there is no access right. Adding and deleting users in groups and changing their passwords can be done using the RelayTool service software. The session of the current user is terminated when the user is changed via the HMI or after the inactivity timeout or reboot.

### **2.3.2 Prohibiting configuration changes via Ethernet port**

This function allows you to enable or disable the remote update of settings. This function can only be controlled from the HMI OSD menu.

The mode of changing the settings over the network is controlled through the **Settings/Security** menu items by setting the "Disable Eth conf" parameter ("On" - enable, "Off" - disable). After exiting the menu, a confirmation message appears on the screen to confirm the change in settings, allowing you to save the changes.

### **2.3.3 Accounts**

#### **2.3.3.1 Account management**

During the initial configuration of the IED, each of the roles contains one built-in account of the same name. For the groups "Administrator", "Relay protection and automation" and "Operational personnel" the user can add up to 15 accounts in total, as well as edit or delete existing accounts. Built-in accounts have passwords shown in the previous Table 2.1, it is recommended to replace them with those that meet the security requirements at this protected object during the initial configuration of the IED.

**Note** - In order to ensure the confidentiality of authentication data, when entering passwords, the entered characters are not displayed and are replaced by the "\*".

To manage accounts, select the **Security/User Editor** items in the RelayTool software, then click the Unload button in the right part of the window.

To add a new account, left-click the "mouse" to select the group to which the new account will be added, and click on the "Add user" button, then in the window that appears, enter the name of the new user, his password and click on the "Apply" button. If the entered data is correct, the account is added to the selected group, if it is incorrect, an error message is displayed.

It is allowed to change the password of accounts. To edit the password for accounts, left-click the "mouse" to select the group that contains the edited account and double-click the left mouse button to click on the user password value field, then enter a new value and press the Enter button, after which it is necessary to re-enter password in a new window and click the "Apply" button.

Any account, including a built-in one, can be deleted. To do this, select the group containing the deleted account by clicking the left mouse button, then click on the line with the data of the deleted account and click the Delete user button. In this case, a window for confirming the deletion is displayed, in which you must click on the "Yes" button to delete the account or "No" to refuse deletion. It is impossible to transfer an account from one group to another (change the role). To do this, you must first delete an account in one group and then create the same account in another group.

#### 2.3.3.2 Username

Username may consist of a combination of uppercase and/or lowercase letters of the Russian and/or English alphabets and numbers. Other characters are not allowed when entering usernames. The username cannot be longer than 15 characters. If you try to add a user with a longer name, only the first 15 characters will be saved.

#### 2.3.3.3 Managing security settings

The control of the safety parameters with the HMI is carried out via the menu items **Settings/Security** by setting the corresponding parameter. After exiting the menu, a confirmation message appears on the screen to confirm the change in settings, allowing you to save the changes.

To manage security parameters using the RelayTool service software, select the **IED Properties** item in the menu tree and then click the "Unload" button. In the list of parameters that appears, you must go sequentially to the **Settings/Security** items and after double-clicking the left mouse button in the cell of the corresponding parameter, enter the value. The changes made are saved by clicking the "Download" button. If the entered parameter value is incorrect, the changes will not be loaded, and the screen will display an error message about changing the IED properties.

Setting parameters can also be performed using the RelayTool software by going to the **Security/User** editor items in the menu tree and pressing the "Settings" button. In the window that appears, select the field of the corresponding parameter, enter the required value and click on the "Apply" button.

#### 2.3.3.4 Service mode

"Service mode" refers to the functions and data available to the "Relematika" role, which are used only for servicing, updating the IED software or when providing assistance to users by the manufacturer's specialists. If there is no need for the services of the manufacturer's specialists, then the "Service mode" should always be disabled.

Management of the "Service mode" is possible using the display menu of the HMI and the service software "RelayTool".

The "Service mode" is controlled by setting the "Service mode" parameter ("On" - enable, "Off" - disable).

#### 2.3.3.5 Password length

In order to increase brute-force resistance, it is recommended to use user passwords of the maximum length, consisting of upper and lower case letters of the English alphabet and numbers (the maximum possible number of characters is eight).

**Note** - The parameter is controlled only when the parameter "Password complexity" is enabled (2.3.3.7).

The value of the minimum number of password characters can be set using the HMI display menu and the RelayTool service software.

Setting the minimum password length is carried out by setting the value of the parameter "Min. length".

#### 2.3.3.6 Password expiration

Limiting the password validity period increases its resistance to brute force attempts due to forced rotation. The password expiration value can be set from 1 to 999 days. It is recommended to set the value of this parameter in accordance with the requirements for this protected object. The set value will be valid for all accounts.

**Attention!** Password expiration can occur after IED synchronization is complete.

**Note** - The password expiration counter is reset when the IED is restarted.

The value of the password validity period can be set using the HMI display menu and the RelayTool service software.

When attempting to IED access via the HMI if the password expires, the user is automatically prompted to enter a new password twice. The new password is saved only if the twice entered new values match. Otherwise, an "Error" message is displayed and access is denied. Using the RelayTool service software, you can enter a new password by going to the **Security/User Editor** items in the menu tree, selecting a group, a user and double-clicking the left mouse button in the Password field.

Setting the password validity period by setting the value of the parameter "Validity period".

#### 2.3.3.7 Password Complexity

Inclusion the requirement of password complexity specifies the minimum allowed list of characters that the password should consist of. It is recommended to enable this requirement to increase the strength of user passwords against guessing attempts. The set value will be valid only for created accounts and when changing passwords of existing accounts.

**Note** - When enabling the requirement, you must set the minimum password length according to 2.3.3.5.

This requirement can be set using the HMI display menu and the RelayTool service software.

Setting the password complexity requirement is carried out by setting the value of the "Complexity" parameter ("Yes" - enabled, "No" - disabled).

#### 2.3.3.8 Number of attempts to enter an invalid password

To limit the number of attempts to guess a password, it is recommended to set the value of the counter of the maximum allowed number of entering an incorrect password in the range from 1 to 999. The entered value will be valid for all accounts and will be monitored for each user session. When the counter reaches the assigned maximum value, the account is locked. It is recommended to set the value of this parameter in accordance with the requirements for this protected object.

#### Notes

1 The number of attempts to enter incorrect password is controlled for each user session (for example, through HMI or RelayTool software).

- 2 Counting of the number of attempts to enter incorrect password using the RelayTool software and HMI is carried out separately.
- 3 The counter of the number of attempts to enter the wrong password is reset when the IED is restarted.
- 4 If the number of attempts to enter incorrect password for one account is exceeded, all accounts of this type of connection are blocked.

The value of the maximum number of attempts to enter incorrect password can be set using the HMI display menu and the RelayTool service software.

Setting the maximum number of attempts to enter incorrect password is carried out by setting the value of the parameter "No. of attempts".

#### 2.3.3.9 Password blocking time

This parameter allows you to set the time (from 1 to 999 minutes) for which the user account will be temporarily blocked when it reaches the maximum number of password attempts within one session. The set value will be valid for all accounts. It is recommended to set the value of this parameter in accordance with the requirements of the protected object.

The password lock time can be set using the HMI display menu and the RelayTool service software. Setting the blocking time is carried out by setting the parameter "Block time".

### 2.3.4 Physical identity

The possibility of identification using physical devices is realized by connecting additional smart card readers to the IED and a PC with installed RelayTool service software, configuring them and performing work on managing smart cards.

The function of using physical identification devices can be enabled or disabled using the HMI display menu or the RelayTool service software.

After enabling this function and restarting the IED, any action using the HMI or the RelayTool service software will be accompanied by the requirement to present the user's smart card (except for publicly available functions and data). Access becomes impossible without presenting a smart card. To gain access, it is necessary to attach a smart card associated with this user to the reader. Smart card association must be performed during the initial setup of the IED and immediately after creating new accounts.

**Note** - If no smart card has been associated with this user, it is allowed to temporarily use any smart card.

Physical identification management by setting the "Physical identification" parameter ("On" - enable, "Off" - disable).

### 2.3.5 Connecting and configuring a smart card reader

#### 2.3.5.1 Readers

Readers are connected to the RS-485 port of the IED and the USB port of the PC, respectively. The reader connected to the IED is used for local user identification. The reader connected to a PC is used for remote user identification using the RelayTool service software and for assigning smart cards to user accounts.

After connecting the reader to the IED, it is necessary to configure it using the HMI display menu or the RelayTool service software. This function is available only to users of the "relay specialist" group.

#### 2.3.5.2 The card-reader is configured:

- using the HMI via the menu items: Configuration/Communication ports/RS-485;



- using the RelayTool service software through the Settings /RS485 menu items.
- It is necessary in the cell of the "Protocol" parameter value to select the "RFID" protocol, "Baud rate - 9600", "Parity" - "None", "Stop bits" - "1".

### 2.3.5.3 Configuring "Physical identification" on PC

The reader is connected to one of the standard USB ports of the PC. For the reader to work correctly, you need to install the `ftdi32_certified.msi` and `ftdi64_certified.msi` drivers for 32-bit and 64-bit Microsoft Windows, respectively. The installation files are located on the optical disc supplied with the device. Driver installation is performed using the authority of the local OS administrator. Additional configuration of the driver or the RelayTool service software is not required.

### 2.3.5.4 Associating a smart card with a user account

This function is performed only with the RelayTool service software and is available only to users with the "Administrator" role. One smart card can be associated with multiple accounts. In order to ensure control over the use of smart cards, it is recommended to organize accounting of issued identifiers, their correspondence to their accounts, and use smart card labeling. In case of loss of a smart card, to prevent unauthorized access, it is necessary to associate another smart card with this account as soon as possible. When deleting an account, the previously associated smart card can be used for another account without additional steps.

To associate a smart card with a user account, go to the menu tree under the Security / User editor items, select a group and user account and click on the "Link card" button. When the waiting window appears with the message "Attach the key to be linked to the reader", you must attach the associated smart card to the reader. The smart card time-out is 60 seconds and when it expires, the error message "Error. Reader timeout expired".

## 2.3.6 List of allowed MAC and IP addresses

To ensure the possibility of limiting the remote control of the IED, as well as for identifying the IED by the ICS servers, it is possible to filter traffic by maintaining a list of allowed MAC and IP addresses. The operations of creating, modifying and deleting list entries, as well as reading it, are possible only with the RelayTool service software.

If incorrect or erroneous entries are added to the list of allowed MAC and IP addresses, remote access to the IED may not be possible.

In this situation, it is necessary to connect to the IED via a virtual USB port and correct the erroneous entries in the list.

To get a list of allowed MAC and IP addresses, go to Security/List of allowed IP addresses in the menu tree and click on the "Upload" button. During the initial setup of the IED, the list is empty. It is recommended to include in this list only the MAC and IP addresses of the PC with the RelayTool service software installed, as well as the APCS servers.

To add an entry to the list, click on the "Add" button, and the address 127.0.0.1 is automatically added to the "IP" field, which must be replaced with the required address and the corresponding MAC address. In addition, you can add the addresses of the PC with the installed service software RelayTool by clicking on the "Add your IP + MAC" button. In this case, a window with a list of local addresses is displayed, from which you can select the required address and click on the "Select" button, while the value of the MAC address is added automatically. To delete an entry from the list, just select it with the "mouse" and click on the "Delete" button.

To apply the list of allowed MAC and IP addresses, click on the "Load" button, and a window for confirming changes is displayed with a message about the need to restart the IED. The IED must be rebooted manually.

### **2.3.7 Audit log**

During the operation of the IED, events generated during the execution of security functions are stored in the security audit log. This log is implemented in the form of a table, which displays the following data:

- date and time of the event;
- the name of the user from whose session the event was registered;
- the source of the event (for example, the IP address of the PC and the communication protocol);
- text of the message about the event;
- event status (for example, "Successful" or "No access").

The audit log does not have any parameters and settings and cannot be modified, deleted or disabled. The audit log is designed to accumulate information about events, data about which can be used in the investigation of information security incidents.

Viewing the audit log is only possible with the RelayTool service software. To do this, go to the Security/Audit log items in the menu tree and click on the "Upload" button. Audit log data is presented in the form of a table, the rows of which can be colored: green for a successful event, red for an error event, no color for access denied.

The entire audit log is displayed automatically. The user can specify filtering options to display only the required data. To do this, you must specify the values of the fields at the top of the log table, by which the data will be sampled.

When the volume of the audit log is full, new data is recorded automatically, while the old data is erased. To ensure the continuity of saving data on security events, it is recommended to save the audit log to files at a sufficient frequency for the given securable object. To save the audit log, you must click on the "Export" button, select one of the saving formats (PDF, DOCX, XSLX) and specify the file name.

## 2.4 Parameter setting

IED is freely configurable and has adjustable parameters. Table 2.3 shows IED settings, which can be entered via HMI user interface or using the service software.

Table 2.3: IED parameters configurable via HMI

Setting	Editable parameters
Bay connection parameters (2.5.6)	Rated values of currents, voltages, other measurable values; measuring transformer parameters
Protection function settings (2.5.9)	Activation/deactivation and operating mode (setting position selection), entering setting values
Communication parameters (2.5.12.1)	Selection of a communication protocol and its parameters
Time and date parameters, synchronization method (2.5.12.2, 2.5.12.3)	Date, time and UTC
Disturbance recording (2.5.8.4)	Archiving
Test (2.5.10)	Disturbance recorder enabling, check signal definition

RelayTool software should be used for configuration of the parameters presented in the following Table 2.4.

Table 2.4: Configurable parameters

Object	Editable parameters
Protection function settings	Activation/deactivation and operating mode (setting position selection), entering setting values
Analog inputs	Selection of CT and VT ratings
Binary inputs	Configuration of corresponding hardware input and connection to logical signal
Binary outputs	Configuration of corresponding hardware output and connection to logical signal
LEDs	Configuration of corresponding LED and connection to logical signal
Disturbance recording	Disturbance recorder parameters, definition of starting and operating conditions, setting of analog and binary signals
Event recording	Logical signals configuration
Test	Disturbance recorder parameters, check signal definition

## 2.5 User interface structure

### 2.5.1 User interface

HMI is divided into two functional parts: user interface module and LED module.

The user interface module is a bi-directional communication medium (if equipped with a display). It means that:

- an event may occur, which is reflected in the menu items to inform the operator about the fact that took place and requiring his intervention;
- the operator can display certain data of interest to him.

The user interface module consists of a display and control buttons. The display (if available) shows information about the current state of the control object and the IED itself. The IED interface is based on a menu with a tree structure, navigated by control buttons. The buttons can have different purposes depending on the position in the menu structure at the time of use.

The LED display module has eight bicolor (red and green) general purpose LEDs. Each LED is named on the front panel in accordance with its internal purpose. LED illumination modes are presented in 1.2.5.

### 2.5.2 Purpose of control buttons

The **C** (Cancel) button has two main functions:

- **cancellation** of any operation in the dialog box;
- **exit** from the current mode or move to a higher level of the menu tree.
- The **E** (Enter) button has the following functions:
  - **entry** into the menu of a lower level indicated by the cursor;
  - **execution**, the button confirms the execution of the action indicated on the display;
  - **confirmation** of input of numerical values and selection of a list item;
  - **transition** to the mode of quick editing of parameters.
- **Left (◀)** and **Right (▶)** buttons perform:
  - fast movement of the cursor (through four items or to the end of the page) through the menu items on the same level;
  - moving the cursor in the horizontal direction in the parameter editing mode to change the active familiarity.

Simultaneous pressing of the **Left (◀)** and **Right (▶)** buttons is used in the **Current mode** menu item to call the menu for setting the reference analog signal.

**Note** - An analog signal is taken as a reference signal, the angle of which is used as a basis for comparison with the angles of the similar analog signals.



The **Up (▲)** and **Down (▼)** buttons have four functions:

- moving the cursor up, down through the items of the current menu at the same level;
- selection of confirmation options in the dialog box;
- changing the parameter value in edit mode;
- switching between information windows of the standby mode.


The **RESET** button is used, as a rule, to reset the IED alarm.

**Note** - The functions of the buttons are given for one-time pressing.

Button **I** is designed to turn on the circuit breakers, **O** - to turn off the circuit breakers.

Button  is intended to enable the action of commands from the **I** and **O** buttons. Press and hold the button , and press one of the **I** or **O** buttons to execute the corresponding control command.

### 2.5.3 Assignment of function buttons

Functional buttons **K1, K2, K3, K4** are intended for operational management of the software keys. They are controlled only when the button  is pressed together ahead of time.

The buttons are configured using the RelayTool software (Figure 2.1). Each button can be enabled or disabled (column "Use").

The signal read from the function button is specified in the "Function key \Signal" column. The button can be configured either as an operational button or as a toggle (column "Mode"). In the first case, each time you press, for example,  $\text{K1}$ , the signal from the button enables the logic circuit in the form of a short pulse. In the second case, each time you press, for example  $\text{K2}$ , the state of the software key is changed, the signal from which is sent to the circuit. Information about the state of the software key configured in the switch mode is stored in the non-volatile internal memory of the device.

The state of the software key, i.e. the signal specified in the "Function key \Signal" column is recommended to be displayed on one of the two LED colors of the function button (usually green) in the "FC LED \ Signal" column, without inversion and pickup.

If the function button is not used, then its LED can be used as a general-purpose LED, with storing the state in the non-volatile memory ("Pickup" column) and inversion ("Inversion" column). The LEDs of the latching function button are reset by pressing the RESET button.

It is possible to control the states of the buttons (switch mode) through the signals specified in the columns "Setting signal" and "Reset signal" ("Remote control of the FC") in the RelayTool software, to which pulse remote control commands can be entered via communication protocols, including number according to IEC 61850- 8- 1 MMS. In button mode, the remote command signal can be set in the "Set signal" column ("FC remote control").

There is a field "Remote control signal", which determines the source of control of the states of the function buttons. When the logic signal is zero, the state is controlled from the function buttons themselves, and the signals "Set signal" and "Reset signal" are blocked. With a single logical signal, control is carried out from the signals "Installation signal" and "Reset signal", and the actions from the function buttons are blocked. Thus, using the "Remote control signal" field, it is possible to implement the remote control mode using an external switch connected to the binary input of the IED. There is no other possibility of transferring to the remote control mode in the "TOR 150".

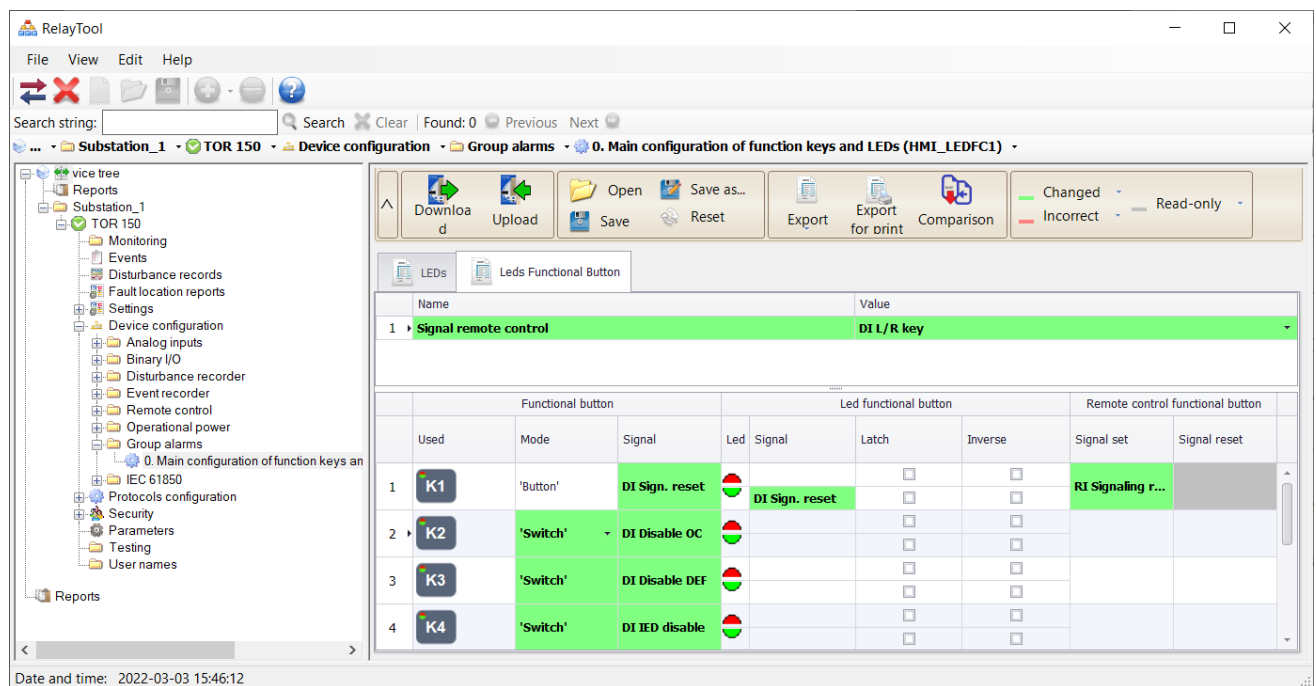


Figure 2.1: Button configuration window in RelayTool software

### 2.5.4 Stand-by mode

As soon as the IED is turned on, the local HMI enters the standby mode. In this mode the IED screens switch sequentially, displaying the following information:

data on disturbance recordings: number, date and time of the latest recording, cause of triggering;  
information on the latest events: signal abbreviation, status (0 or 1), date and time of the event;

information on failures detected by built-in self supervision: WARNING!!! ERROR!, description of the failure;

information on the current measured values;

Screens are displayed only when records, events, failures or selected values are available. The screen displaying a failure has the highest priority: when a failure is detected, only this screen is displayed.

Every screen displays date, time and active setting group number "Active group" at the top.

Display turns off when inactive for 2.5 minutes. Press any button to activate the display screen.

The HMI display switches to standby mode screen after 60 minutes if no button is activated. In this case, the "Guest" user is installed in the system.

### 2.5.5 User interface menu

User interface menu is the main tool for controlling IED operation and receiving information about its state.

Pressing the **E** button will switch the device from standby mode to the main menu.

The main menu (depending on IED version) includes the following items:

- Current mode (2.5.6);
- Events (2.5.7);
- Disturbance recorder (2.5.8);
- Settings (2.5.9);
- Testing (2.5.10);
- Diagnostics (2.5.11);
- Setup (2.5.12);
- Information (2.5.12.6);
- IEC 61850 (2.5.13).

The lower-level menu content depends on the device current state and therefore some of the items could be not available. An active state is indicated at the top screen line (for example, Settings).

Several types of screens are distinguished in the menu:

- **selection list** (most of the menu): current selection is underlined with a cursor in the left part of the screen; jumping to the sub-menu is possible;
- **list without selection** (indication of read-only parameters): there is no cursor on the screen;
- **dialog window** (request for an action execution): no cursor, functions of the buttons are shown on the screen.

If the number of menu items exceeds the number of the screen rows, symbols ↑, ⇅ or ↓ are shown on the left top of the scrollbar.

### 2.5.6 Current mode

In the **Current mode** menu, the user can view the current values of analog and logic signals. This menu is configurable. The composition of the items of this menu in the factory setting depends on the type of the IED and, as a rule, contains the following items.

### 2.5.6.1 Input Signals

The **Input Signals** menu contains binary input signals for each of the binary I/O blocks, into which the values from the binary inputs of this block are written. Each input signal is described by its number on the block, name and current value (logical "1" or logical "0").

### 2.5.6.2 Output signals

The **Output Signals** menu contains binary output signals for each of the binary I/O blocks that affect the output relays of this block. Each output signal is described by its number on the block, the name and current value (logical "1" or logical "0").

### 2.5.6.3 Current values

The menu **Analog signals** represents measured analog values:

- primary and secondary phase currents,
- primary and secondary phase/phase-to-phase voltages and residual voltage;
- frequency, etc.

The displayed information about the current values is determined by the device configuration and is not common for all IEDs.

AC currents and voltages are displayed in polar form (RMS value and its phase relative to the phase of the reference signal).

Reference signal information is displayed by simultaneously pressing the Left (◀) and Right (▶) buttons in the analog value menu.

### 2.5.6.4 Circuit breaker diagnostics

The menu **Breaker Diagnostic** is designed to display information about the monitored circuit breaker and is displayed when using the corresponding function in the device.

The **Opening time** menu contains information on the duration of the last trip time of the circuit breaker for each phase (in ms).

The **Closing time** menu contains information about the duration of the last switch-on time (in ms).

The **Tripping currents** menu contains information on the currents of the last breaker trip for each phase (kA).

The Breaker Status menu contains the following information:

- **BML,%** - remaining mechanical life of the circuit breaker (in percent);
- **BML** - the number of remaining "on-off" cycles;
- **Ntrip** - the number of "on-off" cycles performed;
- **BCL ph.A,%** - remaining switching resource of CB phase A (percentage);
- **BCL ph.B,%** - remaining switching resource of CB phase B (percentage);
- **BCL ph.C,%** - remaining switching resource of CB phase C (percentage).

## 2.5.7 Events

This menu is used to display information on events registered by the IED. All events registered by the IED are stored in non-volatile internal memory.

**Events** menu contains the following items:

- **List** - display information about events;
- **Clear All** - deletes all events from the memory.

### 2.5.7.1 View

In the **List** menu, the user is prompted to select an event to view. The screens that open sequentially when you press the **E** button display the date, time (in the format \*DD.MM.YYYY \*> YY: XX: CC.ZZZ, where YY - hours, XX - minutes, SS - seconds, ZZZ - milliseconds), a list events. When the desired event is selected, the date and time, the active setting group, the oscillogram number (if the event was recorded in the oscillogram) are displayed.

### 2.5.7.2 Deleting all events

The **Clear All** menu (requires authorization and confirmation) allows you to clear the internal memory, for example, when carrying out commissioning or setting up the IED, when the information is not important to personnel after short-term use.

The **Clear All** function should be used with caution as it results in irreversible loss of data on all previous disturbances in the power system.

**Note** - This menu is available only for the manufacturer's specialists.

### 2.5.8 Disturbance recorder

The **Disturbance recorder** menu is used to display information recorded by the device during the latest disturbance situation. All disturbance recordings are stored in an internal non-volatile memory. They can be accessed via a process control system or RelayTool software.

The menu Disturbance recorder contains the following items:

- **Records list** – contains information about saved disturbance recordings and their quantity;
- **Clear all** – clears all disturbance recordings from the memory;
- **Manual trigger** – manual start of a disturbance recorder (requires confirmation);
- **Parameters** – viewing of disturbance recorder parameters.

#### 2.5.8.1 View

The User is offered to select a disturbance recording to be viewed. In the **Records list** menu the current, previous and next disturbance recording are displayed with the time stamp (in the format DD.MM.SS.XXX, where XXX are milliseconds), disturbance duration, short name of a signal, which has initiated triggering of the current disturbance recording. Scrolling through the list of recordings is made by means of **Left** and **Right** control buttons.

After selecting of a desired disturbance recording with **E** button, the user jumps to the next menu level, containing the following information about the recording:

**Triggering** – List of signals, which initiated the disturbance recording;

**Note** - At the end of the name of the disturbance recorder start signal, "(1)" is added, which means start on the appearance of "(1)" logical value of the signal, or "(0)", which means start on its disappearance.

**Events** – List of events recorded by the IED;

**Clear** – Erasing the current recording from the internal memory (requires confirmation).

**Note** - This menu is available only for the manufacturer's specialists.

#### 2.5.8.2 Clearing all disturbance recordings

The **Clear all** menu (with confirmation) makes possible to clear the internal memory, for example, during device commissioning or configuration, when the previous information is not actual.

The **Clear all** function should be used with care as it leads to permanent loss of data about all the previous disturbance conditions recorded by the IED.



This menu can be used only by Relematika specialists.

#### 2.5.8.3 Manual triggering

The **Manual trigger** menu is used for manual triggering of disturbance recorder. Use this function to get a snapshot of the controlled object status.



#### 2.5.8.4 Parameters

The **Parameters** menu contains information about the parameters of disturbance recorder function:

- **Max.duration** – Maximum disturbance recording length, in ms;
- **Postfault** – postfault disturbance recording length (after triggering conditions disappear), in ms;
- **Prefault** – prefault disturbance recording length (before triggering conditions appear), in ms;
- **Sample rate** – sampling frequency;
- **Archiving** – permission for automatic compression of the records in separate \*.zip archive;
- **Signal names** – choosing a signal name to be displayed with the recording: Eng – internal tag, Ru1251 – user short name.

The parameters of the duration and sampling rate of the disturbance recorder function can be edited in the disturbance recorder configuration in the RelayTool software.

Changing the archiving mode and signal names is done via the HMI of the IED.

### 2.5.9 Settings

Use the **Settings** menu to view and edit different parameters for protection functions included in the IED and to set their operating modes. The IED can have up to sixteen setting groups, one of which is set as active. An active group number is displayed in a standby mode and in the main menu. Reference information is displayed by pressing **F1** in the setting menu row.

#### 2.5.9.1 View

Use the **View** menu to view the current setting values, timers' characteristics, state (positions) of programming switches.

#### 2.5.9.2 Edit

In order to edit parameters enter the **Edit** menu, select an active group, enter a password and select a setting. By pressing **E** button the user will be get the possibility to change the parameter. Confirm entry by **E** button. In order to enter the extended settings editing mode press **F2**.

When the setting is changed, exit the menu, then you will be offered to save the changes.

Parameters can be also edited with the RelayTool software.

#### 2.5.9.3 Activate

Enter the **Activate** menu in order to select (change) an active setting group from the list. The user will be offered to enter a required password so that the changes would come into effect.

**Note** - It is possible to activate a group of settings through binary inputs or by remote control commands.

#### 2.5.9.4 Create

The **Create** menu is used to create a new setting group. The number of the setting group being created is assigned automatically and is equal to the smallest free number. When creating a group, the user chooses which setting values are copied into it - either the default settings or the settings of an existing group.

When creating a setting group, the user will be prompted to log in and then confirm the creation.

#### 2.5.9.5 Delete

The **Delete** menu is used to delete the setting groups. The user must select the group to be deleted from the list. Next, the user will be prompted to log in, and then confirm the deletion.

**Note** - It is highly discouraged to delete the last or active setting group.

### 2.5.10 Testing

There are functions, which are impossible to test without participation of qualified maintenance personnel. In order to test functionality of measuring elements, the device is set into the test mode. For detailed description of the test mode refer to 2.6.

Use the **Testing** menu to verify the IED operation capability:

- **Test output** – setting the operating test output relay. A submenu includes the **Reset** function which, if selected, de-energizes the relay, which then cannot be controlled until the next signal assignment;
- **Test mode** – test mode enabling/disabling;
- **Enable recording** – enable/disabling of disturbance and event recording during the active test mode;
- **Number of trig.** – number of disturbance recorder triggering in a test mode (resets on test mode exit).
- **SCADA test** – displayed in a test mode, used for automatic testing of communication protocols (IEC 103, IEC 104, IEC 61850, Modbus). The testing cycle is performed by sending events when the logical signals are sequentially changed to the value "1" and then to "0". The user can select the communication protocol (IEC-103, IEC-104/101, IEC-61850, Modbus), the number of test cycles, the interval between successive signal changes and start testing (in ms). This menu will be useful when setting up communication with APCS - to check configuration of the signals for the selected communication protocol, their reception and displaying in APCS.

### 2.5.11 Diagnostics

TOR 300 has built-in internal failure detection functions, which enable detecting and alarming (output signal, LED indication) the internal faults in operating mode. Use the **Diagnostics** menu to check the IED status according to self-supervision tests:

- **Status** – shows general and current status of the hardware (central and signal processor, peripheral units). When a failure is detected, it contains error codes, see 3.4.3;
- **LEDs** – contains three tests of LEDs on the front panel of the IED. The first test is used to check the red light glowing of the general purpose bicolor LEDs, functional buttons, **I** and **O** buttons and yellow **Test** LED. The second test is to check the green status of the general purpose LEDs, the functional and **I / O** buttons, and the green **Operation** LED. In the third test, all bicolor LEDs for general purpose, functional buttons, and **I / O** buttons cyclically change red and green light, and the single color "READY" and "TEST" LEDs flash. When selecting the "LEDs" function, the user controls their state visually;
- **Hardware** – changing to extended testing mode. In this mode, all external circuits are disabled, the protections are disabled. A detailed description of the test mode is given in 2.6.3;
- **Information** – contains information about the number of IED starts, about the last start (date in the format HH.MM.YYYY and time in the format YY: XX: CC.ZZZ, where YY is hours, XX is minutes, SS is seconds, ZZZ is milliseconds), reset function of information about all starts (requires authorization and confirmation), detailed information on software versions.

### 2.5.12 Parameters

The **Parameters** menu is intended for editing the displayed date and time, setting the parameters of communication with APCS for each of the communication ports, setting the time synchronization parameters, changing the user and setting up information security functions.

**Attention!** The accuracy of the IED's internal clock is important for joint analysis of disturbance recordings from multiple IEDs.

### 2.5.12.1 Communication ports

The **Comm. ports** menu contains items **RS-485** (XT1 connector), **Ethernet 1** (XT3, XT4 connectors), which include editable settings for joint operation of several IEDs in a common network and remote access to this IED.

2.5.12.1.1 RS-485 menu (Port 1) is used to view and set (select and configure) communication port parameters and contains:

- **Protocol** – selection of communication protocol: IEC103, Modbus, IEC101, RFID, SPA-Bus, NMEA0183, BDUBus (specialized internal protocol for communication with service software);
- **Comm. parameters** – used for setting the following parameters:
  - a) **Baudrate** – selection of data transfer rate. Baud rate options in bit/s are: 2400, 9600, 19200, 38400, 57600, 115200, 230400;
  - b) **Data bits** – number of data bits;
  - c) **Parity** – check bit is usually set to zero or one so that the total number of digits in a byte is always either even or odd. Used for data transfer check;
  - d) **Stop-bits** – bits denoting the end of the byte transferred;
- **Prot. params** – specific parameters of the protocol used for certain communication port.

For **IEC103** and **IEC101** protocols:

- a) **Address** – device address in the network according to the standard IEC 60870-5-103-2005 and IEC 60870-5-101-2006, respectively;
  - b) **Timeout** – maximum allowable time to form a response, ms;
  - c) **Latency** – communication channel delay,  $\mu$ s;
- **Disturbance records** – defines the procedure for working with oscillograms according to the standard IEC 60870-5-103-2005 or IEC 60870-5-101-2006, respectively, and contains:
    - a) **List** – determines the number of disturbance recordings transmitted by the device (last eight (standard), last 16, 24, or all);
    - b) **Clear** – whether it is necessary to erase disturbance recordings after unloading;
    - c) **Report** – whether it is necessary to generate a spontaneous message with a list of new disturbance recordings.

For **MODBUS** protocol:

- a) **Address** – device address in the Modbus network;
- b) **Timeout** – maximum allowable time for formation of a response, ms;
- c) **Mode** – selection of ASCII or RTU mode.

For **BDUBus** protocol:

- a) **Address** – device address in the BDUBus network.

For other communication protocols (**NMEA0183**, **SPA-Bus**, **RFID**) there are no parameters.

2.5.12.1.2 Menu Ethernet 1 (connectors XT3, XT4) is used to view and set parameters of communication ports and contains:

- **MAC** – unique MAC address of the device. This number is used to identify the sender and recipient of the frame;
- **IP** – unique network address of a device in a computer network built on the base of IP protocol;
- **Mask** – IP network mask;
- **Gateway** – IP gateway address must be set taking into account the device's IP address and netmask.
- **Protocols** – allows you to configure the connection parameters of the device according to the standard IEC 60870-5-104-2004; in the menu, the depth of issuing (in days) by the IED information from the event log is set, as well as the timeouts of the setpoint and commands;
- **Mode** – selection of communication ports operation mode:
  - a) **PRP** – used when applying PRP network topology. The mode should be enabled only after confirmation of the presence of PRP by the APCS service technicians. **If the network does not**

**support PRP, then this mode must be disabled**, otherwise communication problems may occur;

b) **Switch** – used when there is no PRP on the site;

c) **Hot-standby** – used when there is no PRP at the site and the need to provide redundancy. The mode provides simultaneous connection of the IED to the facility network via two ports, while one port is always used for receiving and transmitting data, the other is in reserve. If communication is lost on the active port, the switch to the backup port occurs.

- **VLAN** – enable/disable VLAN mode and configure its parameters:

a) **Mode** – enable/disable VLAN mode;

b) **VLAN number** – sets this VLAN tag in outgoing untagged traffic when VLAN mode is enabled. Incoming traffic with this tag will be received in the IED;

c) **VLAN GOOSE** – allows you to set a "white list" of 16 VLAN numbers for incoming and outgoing packets, i.e. list of allowed VLANs. The VLAN number participates in this list. Packet filtering using this list is performed in hardware and allows you to reduce the load on the communication port and provide more reliable packet reception in a busy network. Typically used to filter GOOSE packets. At the same time, other packets with VLAN numbers from this list will also be accepted in the IED, and also that outgoing GOOSE with VLAN numbers that are not in this list will be blocked. Packets without a VLAN tag or with a null VLAN tag are not blocked;

- **PRP settings** - setting of PRP Supervision parameters:

a) **SVF period** – period of sending PRP Supervision packets, s;

b) **MAC** – destination address of PRP Supervision packets.

**Note** - The settings in the Gateway item and the mode selection in the Mode item of the Ethernet 1 menu are applied only after confirmation of the request to restart the IED.

#### 2.5.12.2 Menu Date/Time

Menu Date/Time - editing the local date, time, time zone of the UTC and setting the format of the time displayed in the APCS.

The local date and time are set in the format DD.MM.YY, HH: MM and are stored in the non-volatile clock. Changing the date and time via the HMI is possible if it is allowed in the menu "Settings\Synchronization\Methods\HMI".

The local time zone relative to the UTS is specified in the format  $\pm$  HH: MM.

In the **APCS** item, the time format issued in the APCS is set: local time for a specified time zone (**Local**) or time for a UTC time zone (**UTC**).

#### 2.5.12.3 The **Time sync. methods** menu contains:

**Methods** - selection of a method (source) of time synchronization and its state (Ok, Error or Disabled): **HMI** (possibility of adjusting the time via HMI), **Techn.int.** (from RelayTool software via BDUBus technology interface), **Internal RTC** (real time clock), **IEC103**, **NTP/SNTP**, **IEC104/101**, **MODBUS**, **NMEA0183**, **SPA-Bus**. For each method, it is possible to enable it (one synchronization source is possible), display its status (normal operation or error), the number of synchronizations. Additional parameters are provided for NTP/SNTP sync method: **IP** – primary and secondary SNTP server addresses; **Period** - server polling period (in seconds);

- **Parameters** - synchronization parameters common for all methods: **Threshold** - the minimum difference between the time of the IED and the SNTP server, if exceeded, the time from the server will be applied (in ms).

2.5.12.4 The Access menu is intended for authorization - selecting a user and entering a password (2.3). This item is useful, first of all, to install the "Guest" user in order to prevent the execution of actions with extended access rights of the current user (Table 2.2).

2.5.12.5 The Security menu is intended for entering parameters of access to the IED functions and contains:

- **Min. length** - the minimum number of password characters required to set it (2.3.3.5). It is recommended to use user passwords of maximum length (eight characters), consisting of uppercase and lowercase letters and numbers. The set value will be valid only for created accounts and when changing passwords of existing accounts;
  - **Expiration date** - password expiration date (2.3.3.6);
  - **Complexity** – selection of the minimum acceptable character set (2.3.3.7. When the requirement is enabled - the simultaneous presence of uppercase and lowercase letters of the English alphabet and numbers, with the requirement disabled - any letters of the English alphabet or numbers;
  - **Num. of attempts** – the number of incorrect input attempts in each user session, upon reaching which the account is blocked (2.3.3.8);
  - **Block. time** – account blocking time (2.3.3.9);
  - **Service mode** – service mode enable/disable (2.3.3.4);
  - **Eth conf.prohib.** – selection of the setting change mode (2.3.2);
  - **Phys. identification** – identification using smart cards (2.3.4).
- Changing the settings in the Security menu is available only to users of the "Administrator" role.

#### 2.5.12.6 Information

The **Information** menu is used to display information about:

- the name of the manufacturer of the device (Relematika LLC);
- the name of the power facility (station, substation) where this device is installed (set in the RelayTool software);
- the name of the protected connection (set in the RelayTool software);
- device model name;
- a brief description of the logic diagram (for example, a typical project);
- **Serial N** - serial number of the IED;
- **HW** – general hardware version of the device;
- **SW** – general software version of the device;
- **FS** – device function set version;
- **LV** – version of the device functioning algorithm (logic scheme);
- **Fnom** – device system frequency.

#### 2.5.13 IEC 61850

The **IEC 61850** menu is intended for displaying the current state and checking the operability of the IEC 61850 server in the IED (substation bus, which uses the MMS and GOOSE protocols (**Substation bus**). It is also possible to enable the simulation mode (**Simulation**).

**Note** - The simulation mode is used when setting up the IED. In this mode, signals are received/sent from the test setup.

The substation bus item line displays:

- «Ok» – with correct operation and correct configuration of all IEC 61850 protocols used on the bus;
- «Err» – if an incorrect configuration of at least one of the protocols used on this bus is detected.

**Substation bus** menu item contains sub-items: **Inp. GOOSE** - states of received GOOSE messages, **Out. GOOSE** - the states of the transmitted GOOSE messages and the **MMS server** - the health state of the MMS server.

Incoming GOOSE messages configured in the IED are displayed in the **Inp. GOOSE** menu item. as a list. The following parameters are displayed for each of the configuration messages:

- MAC – MAC address of the incoming GOOSE message to which the IED is subscribed;
- ID – GOOSE message identifier;
- ConfRev – GOOSE configuration revision number;
- StNum – number of signal state change in GOOSE message;

- SqNum – message relay number;
- Error – diagnostics error code (Table 2.5).

Outgoing GOOSE messages configured in the IED are displayed in the **Out. GOOSE** menu item. as a list. For each of the messages, the following parameters are displayed to check the correctness of the configuration:

- MAC – Outgoing GOOSE MAC address;
- StNum – number of signal state change in GOOSE message;
- SqNum – message relay number.

The **MMS server** menu item contains the following information:

- Analog - the number of configured analog signals;
- Discrete - the number of configured binary signals;
- Control - the number of configured control signals;
- Settings - number of configured setpoints;
- Clients - the number of clients connected to the IED.

Table 2.5: Diagnostic error codes at failure detection when receiving GOOSE messages

Error code	Description
0x0000	No errors
0x0001	AppID comparison error (app id)
0x0002	Simulation bit comparison error
0x0004	Control block reference comparison error
0x0008	Dataset reference comparison error
0x0010	Message ID comparison error
0x0020	"Test" field comparison error
0x0040	Configuration revision error
0x0080	Number of elements in the dataset comparison error
0x0100	Error in counting the number of elements in the dataset
0x0200	Data type comparison error in dataset
0x1000	Variable size comparison error
0x8000	Error waiting for GOOSE message reception

## 2.6 Test Mode

The IEDs have implemented testing modes: protection functions and IED hardware.

### 2.6.1 Test mode for protection functions

#### 2.7.1.1 Purpose and operation.

The mode is designed to test the operation of the ME and generate logical signals. Test mode allows you to check the protection both in the withdrawn state and under load.

The transmission of signals to the APCS in the testing mode is regulated by the communication protocols (1.2.6).

When switching to the test mode, the recording of oscillograms and event registration are automatically disabled. This ensures the operation of protection functions, various background tasks, configuration and setpoint functions and registration of system events.

The test mode is carried out by applying the **IED test** signal to the binary input of the IED or through the Testing menu (the **Test mode** item). You can also enter the test mode using the service software. This inhibits the output relays of the IED and turns on the **TEST** LED (yellow).

When testing mode is enabled, the quality of data sent via IEC 61850 protocols (MMS, GOOSE) is marked as "test". This should be taken into account when interacting with external equipment using the IEC 61850 standard.

## 2.6.2 Setting up test mode

In the Testing menu, item Control. output, assignment of logical signals to the output relay "Control output" is carried out. In the submenu, the user is offered a complete list of logical signals, which are presented in the form of a structured list of short signal names. The menu heading displays the designation of the function to which the tested ME belongs.

The service software is used to select the output relays that are blocked in the test mode to prevent unnecessary activation of the output relays.

It is possible to enable registration of the mode in the **Test** menu:

- in the item **Perm. osc./reg.**, this turns on the disturbance recorder and event recorder. Disturbance recording is performed according to standard trigger conditions, triggering on the control output is disabled and configurable separately;
- in the item **Number of starts**, while the disturbance recorder is started at the control output, other start conditions are blocked.

**Note** - Menu items **Perm. osc./reg.**, **Number of starts** are active only in test mode.

After removing the "Test IED" signal, the IED cancels the test mode and returns to normal operation.

## 2.6.3 Hardware Test mode

### 2.6.3.1 Purpose and operation

The hardware test mode is designed to check the operation of hardware nodes during periodic checks or during checks before commissioning to identify a malfunction of the tested nodes.

When entering the test mode, the functions of protection, disturbance recording, logging, and self-testing are automatically terminated.

If an error (inconsistency) is detected, it is necessary to record the error in the fault log; therefore, it is possible to record the result of passing the test (successfully or not).

### 2.6.3.2 Preparation for testing

Disconnect from the circuit IED before testing:

- c) binary input signals;
- d) input analog signals;
- e) output binary signals.

When entering the test mode through the Diagnostics / Hardware menu, you must log in and confirm the transition to the hardware test mode. In this case, you will go to the service menu.

Further, when you press the **E** button, you go to the main menu. To carry out diagnostics, select the **Diagnostics** item and confirm the fulfillment of this requirement (Figure 2.2).

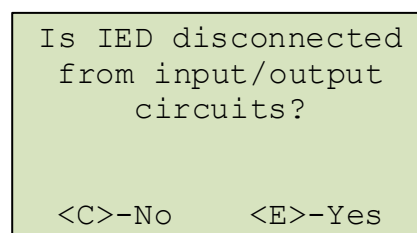


Figure 2.2: Circuit disconnection confirmation

After making sure that the circuits of the input and output signals are disconnected, select the option "Yes" by pressing the button **E**. After that, the test mode will be entered, while the operation of the output relays is allowed.

If "No" is selected, the operation of the output relays is automatically blocked and a message about this is displayed on the screen (Figure 2.3). Next, you enter the test mode, in which the binary outputs are not checked (item **IN/OUT PCB Test**).

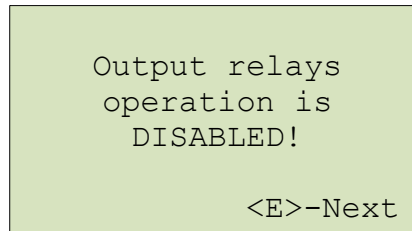


Figure 2.3: Relay blocking confirmation

### 2.6.3.3 Test start

The list of tests of the Diagnostics menu item is displayed:

- Screen test;
- Keyboard test;
- LED test;
- MP board test;
- Test "Failure";
- Test of IN/OUT PC-boards;
- Analog channels.

The test is started by selecting the corresponding menu item on the screen of the HMI device. It is possible to stop the execution of tests by pressing the C button, except for the keyboard test.

Upon completion of each test, it is necessary to confirm the result of the test ("Was the test successful? <C> –No <E> –Yes").

The result of passing the test is fixed on the screen opposite the menu item of the corresponding test ("ok" or "er").

### 2.6.3.4 Screen test

When the test is run, the functionality of the screen indicator is checked.

During the test:

- all segments of the indicator light up simultaneously, then the screen is cleared;
- segments are lighting and blinking off sequentially.

### 2.6.3.5 Button test

This test checks the performance of the control buttons and function buttons.

#### 2.6.3.5.1 Control buttons

The test is carried out by short-term pressing on the button, while the name of the tested button should be displayed in the button Test line on the screen. With this test, you can check the function of all buttons on the device (Figure 2.4).

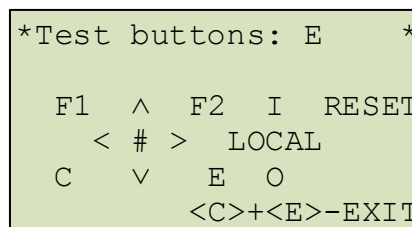


Figure 2.4: Button test

Exit from the mode is performed at simultaneous short-term pressing of buttons **E** and **C** or after receiving the corresponding command through the diagnostic port.

#### 2.6.3.5.2 Functional buttons

The test is carried out by short-term pressing the button, while the button name (**K1**, **K2**, **K3**, **K4**) should be displayed on the screen in the **Button Test** line. No button press required to the test functional buttons.

When the button  is pressed, the name **Key** should be displayed in the **Button Test** line.



### 2.6.3.6 LED test

After starting the test, the indication of all LEDs is checked.

When testing LEDs, the following conditions are checked:

- all LEDs are off;
- LEDs are on in the "red" and "yellow" mode;
- LEDs are on in the "green" mode;
- sequential switching on and off of single-color LEDs once, and bicolor LEDs twice (first they turn on in the "red" light mode, and then "green").

### 2.6.3.7 Logic block test (MP board test)

To check the correct operation of the real-time clock microcircuit installed in the logic block, the IED displays a message about the set date and time on the screen (Figure 2.5). It is necessary to confirm the correctness of the displayed information.

```
* Test CP module *
Date 29.05.2021
Time hh:mm:ss

Displayed correctly?
<C>-No <E>-Yes
```

Figure 2.5: Checking the real time clock

To check the correctness of file systems, information about all devices and partitions of the system is displayed on the screen (Figure 2.6):

- device name (ram, boot, oscil, log);
- total / free memory, kB;
- the status of checking file operations.

```
* Test CP module *
Device: oscil
Memory: 7796/3195 kB
File ops.: Done

<C>-Exit <E>-Next
```

Figure 2.6: Checking the correctness of file systems

If file operations fail, one of the messages is displayed in the line **F. operations** (Figure 2.7):

- on file creation error – **er crt f**;
- on writing into a file error – **er wr f**;
- on file closing error – **er cls f**;
- on file opening error – **er opn f**;
- on file reading error – **er rd f**;
- on file deleting error – **er del f**.

If all operations are performed correctly, the line displays the inscription "passed". Press **E** to continue the logic block check test.

```
* Test CP module *
Device: log
Memory: 6358/495 kB
File ops.: Done

<C>-Exit <E>-Next
```

Figure 2.7: Checking the correctness of file operations

You need to make sure that the data is displayed correctly and to continue the test of the logic block check press **E**.

When checking for the presence of required protection files, messages with the names of the missing files are displayed.

If it is found that the necessary protection files are missing, the test is considered **unsuccessful** and it is necessary to record the information displayed on the screen and inform the manufacturer.

#### 2.6.3.8 Relay "Failure" Test (Test "Failure")

The test is intended to check the correctness of the operation of the relay "Failure" and LED **ERROR**. The entrance to the mode of changing the state of the relay is carried out using the button **E**. The relay is closed or opened in the mode of changing the state using the buttons "**Up**" or "**Down**". Together with the closing / opening of the relay, the LED **ERROR** must be switched on / off accordingly.

At the end of the test, the relay opens and the LED turns off, respectively.

#### 2.6.3.9 Test of power supply and / or digital I/O units (Test of I/O boards)

This test checks blocks containing binary inputs and outputs. Depending on the IED configuration, this menu item contains the corresponding number of items equal to the number of blocks (slots).

When entering the test block, depending on the type of the IED, the screen is displayed line by line from top to bottom (Figure 2.8):

- slot number of the tested block;
- the type of the tested block;
- the number of inputs and outputs;
- information about the status of binary input channels;
- information about the status of digital output channels;
- number of the checked output, if the outputs are checked.

**Note** - In the lines **Inputs** and **Outputs** the symbol "-" means no input signal or contacts are open, "digit" means the presence of a signal or relay contacts are closed. The digit corresponds to the least significant digit of the binary input and / or output number (for example, for input 1.2, digit "2" is displayed, for input 2.4 - digit "4").

```
*Test Slot01-P0503*
5in/5out
Inputs: | 1-3--
>Outputs:| -2---
Input No. 02
```

Figure 2.8: Checking binary inputs and outputs

The binary inputs are checked by applying the auxiliary power voltage to the binary inputs of the IED.

Checking the binary outputs (output relays) of the unit under test is carried out by changing their state using the button **E**. Button **C** is used to exit the mode of changing the state of the output relays. The change of the state is carried out with the help of "**Up**" or "**Down**" buttons.

Outside of the mode of changing the state of the relay, it is possible to select the next or previous board in the list using the "**Right**" or "**Left**" buttons, respectively.

When you select another block for testing or stop testing the block, the states of the output relays are reset.

### 3. Maintenance

#### 3.1 General

##### 3.1.1 Maintenance cycle

The tests are carried out at the appropriate time and to the extent agreed with the customer. The scope of testing can be reduced during the operation and testing procedures can be changed in accordance with the Customer's internal maintenance rules for microprocessor based (protection) equipment. ***In any case, first of all, the necessary internal rules of the owner of the company must be observed.***

Relematika's recommendation for IEDs maintenance cycle is eight years.

Maintenance and repair of IEDs should be performed by specially trained, certified personnel, representatives of Relematika.

#### 3.2 Safety precautions

The IEDs are designed as fire-proof and safe in accordance with IEC 60255-27:2005.

When operating and maintaining IEDs, follow the relevant standards and regulations applicable to microprocessor-based relay protection devices.

The requirements for personnel and operator's instructions necessary for the operation and maintenance of the device are specified in 2.2.1 of this Operation Manual.

The IED poses no environmental hazard when operated and stored in accordance with the requirements.

#### 3.3 Maintenance order and operability checks



**Only specially trained personnel should be admitted to maintenance of the above mentioned equipment.**



**Relematika should be immediately informed in case of any defects being detected within tested TOR 150 IED or PC communication device.**

Table 1.1: Types of activities during IED maintenance

Checking activities
a) visual inspection: check for marks of shocks, leakage including dried-up spots, oxidized spots on metal surfaces, dust content, visual inspection of input and output signal terminals, contact surface condition of communication interface terminals
b) internal inspection: dust removal; visual inspection of circuit components for overheating marks, loosening of soldered connections due to cracks, check for oxidation; supervision of connector joint and mechanical component fastening, screw connection tightening
c) insulation resistance test of independent circuits (except for communication interface circuits) towards the rack and between each other
d) dielectric strength test of independent circuits (except for communication interface circuits) towards the rack and between each other
e) operability check of binary inputs, output relays and LEDs
f) setting (or check) of required IED configuration according to accepted design solutions and technical characteristics (functions)
g) setting (or check) of relay settings according to the defined configuration
h) checking the validity of displayed quantities and phase angles of currents (voltages) from an external source

Checking activities
i) testing of operating parameters (settings) and reset ratios of each measuring element when applying current (voltage) from an external source; monitoring of LED status during operation
j) testing of protection operating time for compliance with set time delays
k) test for absence of maloperation during connection and disconnection of auxiliary supply voltage with repeated energizing after 0.5 s at the minimum value of the setting range with current (voltage) set for 0.8 of the operating current (voltage)
l) test of IED operation with the set values and measurement of the operating value change at auxiliary supply voltage equal to 0.8 and 1.1 $U_{rated}$
m) test of measuring elements and logic circuit interaction with supervision of all the output relay contacts status and visual inspection of LEDs and signalling lamps status. The test is performed with auxiliary supply voltage equal to 0.8 $U_{rated}$ and provided that corresponding operation of each measuring element and presence of required signals to binary protection inputs is ensured
n) test of protection and control functions with output relay contact action towards the circuit breaker or other switching devices control circuits
o) test of event recording, disturbance recording, protection parameter displaying functions
p) test of bay breaker or other switching devices control (close/open)
q) test of common control and signalling operation with other devices, with required actions to the breaker or other switching devices
r) test under load conditions

### 3.3.1 Checking the resistance and insulation strength

Insulation test is performed in a cold state according to IEC 60255-27:2005 requirements.

#### 3.3.1.1 Before the tests

Before starting the test the following actions should be obligatory taken:

- de-energize the relay and disconnect all external AC (be sure to short-circuit the incoming current circuits before their disconnection) and DC circuits;
- connect circuits inside the independent groups by temporary jumpers. Depending on a version of TOR 150 the following independent groups of circuits can be differentiated:
  - a) AC current;
  - b) AC voltage;
  - c) binary inputs;
  - d) power supply;
  - e) alarm (signalling) circuits;
  - f) output circuits for close/open coils;
  - g) output relays.

#### 3.3.1.2 Insulation resistance measurement

Insulation resistance measurement between the circuits connected to each other and the housing, also between each circuit and the rest of circuits connected to each other is performed by megohmmeter with 1000 V for the circuits with rated voltage of more than 60 V according to the rules of technical maintenance. Measured insulation resistance should be at least 100 MOhm for all specified cases.

### 3.3.1.3 Insulation strength test

Insulation strength between the mentioned circuits towards the housing and between themselves should be tested with the test voltage of 1000 V and frequency of 50 Hz for 1 min. After the test, the IED insulation resistance should be measured once again. Insulation resistance test is considered to be successful if the insulation resistance value remains within at least 100 MOhm.

Insulation tests are carried out in a cold state in accordance with the requirements of IEC 60255-27.

### 3.3.2 Checking the applied setting parameters and configuration

Checking of the applied setting parameters and configuration is performed according to the detailed project design documentation. A local HMI is used for an active setting group selection and setting adjustment.

IED is shipped with default factory configuration. Using the PCAP or RelayTool software a customer can change the default configuration.

For a list of parameters to be configured see 2.4.

### 3.3.3 Testing the validity of displayed analog values

External output circuits should be disconnected from the IED's output terminals.

The test is carried out by applying current and voltage from an external source to corresponding IED connectors. Current and voltage values and phase angles are monitored on local HMI display and/or by RelayTool software. Additionally, current and voltage values can be viewed via web-interface.



Here and further, a specialized protection test system is used as an external source.

### 3.3.4 Protection parameters (settings, protection functions, measuring elements) check

External output circuits should be disconnected from the IED's output terminals. Test procedure for the protection functions is performed according to their description and applicable standards.

During the tests as per paragraphs 0 and 0 the corresponding LEDs are also supervised.

#### 3.3.4.1 Testing of protection functions measuring elements

Testing of measuring elements is carried out by supplying from an protection test system currents and/or voltages, corresponding to the setting values of the tested functions (simulation of fault conditions). Measuring element operation is supervised by the operation of the corresponding check output relay with operation and reset parameters being recorded.

#### 3.3.4.2 Testing of complete protection functions

Testing of complete protection functions (measuring elements, time delay and related logic circuits interaction) is carried out by simultaneous activating of the logical signals and currents and/or voltages, corresponding to the tripping state. Supervision is performed by detecting the operation of check output relay or others.

### 3.3.5 Test of IEDs functionality when applying and removing auxiliary supply voltage

External output circuits should be disconnected from the IED's output terminals. When operating currents of 90 % of operating values are applied to the IED, auxiliary supply voltage is de-energized and energized once again. During the test no protection operation should occur.

### 3.3.6 Test of IED functionality with external devices

Test of IED operation towards the central signalling system and interaction with external devices is carried out by commissioning personnel according to the established procedures.

### **3.3.7 Test of IED interaction with other low voltage equipment**

Possibility of operation on primary equipment control circuits should be eliminated. Test of interoperation with another low-voltage electrical equipment available on the site is carried out by simulating corresponding conditions and supervision of output signalling .

### **3.3.8 Testing the IEDs under load (current and voltage) conditions**

Depending on IED version, operating current and voltage test includes the following:

- test of current circuits by measuring secondary load currents in phases;
- test of serviceability and connection correctness of voltage circuits;
- current circuit connection check for each current transformer group using vector diagram and checking it against the actual power direction in a primary circuits;
- test for correct connection of fuse failure blocking.

### 3.4 Failure list and troubleshooting

#### 3.4.1 Introduction

Failures can occur due to improper transportation, storage and maintenance, component wear. Self-supervision (diagnosis) system tests for failures at power-on and during operation of the IED.

#### 3.4.2 Self-diagnostic

Self-diagnostic is divided to the following two stages: initial (at power on/restart of IED) and continuous (during IED operation).

Self-diagnostic comprises supervision of the following important IED components: CP module, power supply module, binary input/output modules and HMI module. Binary input/output units include current-based supervision of output relays coils. Self diagnostic information is collected from all controllers within the device and is analyzed in central and signal processors.



IED self-diagnostic does not supervise output relay contacts (for example, “stuck” state), binary input operability and winding integrity of input current and voltage transformers.

When a persistent failure is detected within any of the supervised elements, and **ERROR LED** is lit on IED front panel and control of output relays is blocked.

When a failure is detected during the operation, two error code sets are generated, current and general. Current error code represents the self-diagnostic state at the present moment, general code displays all detected failures, including fleeting and then disappeared faults.

Information about detected failures is available under the **Diagnostics/Status** menu item presented bellow.

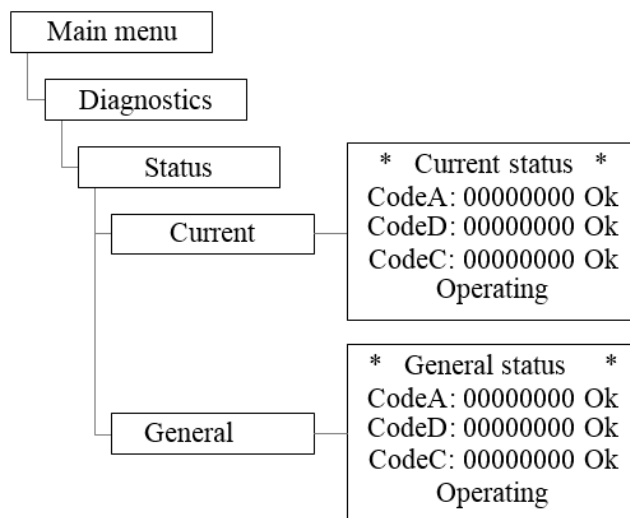


Figure 3.1: Example of Diagnostic / Status menu

The following three code types are displayed in menu items **Current** and **General**:

- **Code A** means the failures detected by central processor (CP);
- **Code D** displays the failures detected by signal processor (DSP);
- **Code C** (auxiliary) means total amount of failures detected in peripheral units (power supply, binary input/output). Entering the menu item and pressing **E** button initiate failure codes per each module, second right digit indicates the number of the module starting from the power supply unit.

The displayed codes make possible identification of every detected failure. The list of codes is presented in Table 3.2 and Table 3.3. Text descriptions of failures are available by entering the menu item (except for C codes).

### 3.4.3 Error codes

Failures, which are detected during continuous self-diagnostic are presented in a hexadecimal notation according to the rules stated below.

**Error code** consists of eight digits and comprises information about the type of failure. Every digit is a hexadecimal number of four binary-code bits (Table 3.3). Every bit corresponds to a certain event (failure), the list of which is presented in Table 3.2 and 3.2. Zero self-diagnostic codes mean no faults detected. A failure code provides information about one or several faults detected simultaneously. For example, code A is 00000001 means: "CP module fail 1" (serial bit number is 1, digit is 1); 00000200 denotes "CP module fail 6" (serial bit number is 2, digit is 3); 00000800 stands for "Scheme error 1" (serial bit number is 4, digit is 3), 00000A01=00000800+00000200+00000001 indicates "CP module fail 1", "CP module fail 6", "Scheme error 1". Other codes are generated in the same way.



Table 3.2: Error code A

HMI message		Description
Error code	text	
0x00000001	CPU board error	Analog block ADC error
0x00000002	CPU board error	Reserve
0x00000004	Software failure1	SW failure
0x00000008	Front PB error1	Front panel board error
0x00000010	CPU3 board error	CPU board error
0x00000020	Settings reset	CPU board error
0x00000040	CPU4 board error	CPU board error
0x00000080	Osc. error	CPU board error
0x00000100	CPU5 board error	CPU board error
0x00000200	CPU6 board error	CPU board error
0x00000400	Clock reset	Resetting data in the clock memory
0x00000800	Scheme error	CPU board error
0x00001000	Reserve	Reserve
0x00002000	App. error	Error from functional diagram
0x00004000	App.error&disable	Error from functional diagram with IED disable
0x00008000	ADC failure	ADC diagnostic error from functional diagram
0x00010000	BI conf. failure	Binary I/O block configuration error: Block missing, Type mismatch, Reuse, Missing configuration, Maximum board number exceeded
0x00020000	–	Ethernet module error
0x00040000	Reserve	Reserve
0x00080000	Reserve	Reserve
0x00100000	CPU1 board error	CPU board error
0x00200000	Reserve	Reserve
0x00400000	ADC1 conf. error	Analog inputs configuration error
0x00800000	ADC2 conf. error	Analog inputs configuration error
0x01000000	No setting group	No group of settings
0x02000000	No calibration	IED not calibrated
0x04000000	Sticky button	Sticky button
0x08000000	HMI exchange failure	HMI exchange failure
0x10000000	SW5 failure	SW failure
0x20000000	Scheme5 error	Error from functional diagram
0x40000000	SW6 failure	Short-term CPU overload, temporary lack of time to execute an operational task
0x80000000	Critical overload	Critical CPU overload, long-term lack of time to execute an operational task

Table 3.3: Correspondence of hexadecimal code to binary

Error code bit value (in hexadecimal)	Active bit numbers (binary code)
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

### 3.4.4 Troubleshooting

If a **persistent** malfunction is detected, which can lead to a false operation or a failure in the operation of the device, the IED actuation on the output circuits is disabled, while the **ERROR** LED on the front panel of the IED turns on. Alarm actuation is provided by the NC contact of the IED.

#### Attention!

If any malfunction of the IED is detected, it is necessary to write the error codes, a textual description of the error, information about the last restart and configuration of the device and report them to the manufacturer.

Troubleshooting work can only be carried out by personnel who have passed specialized training and have necessary equipment.

After eliminating the malfunction and before putting the device into operation, it is necessary to check the correctness of the setting parameters of the device (settings, disturbance recorder parameters, etc.) and make sure that its operation is correct.

In case a **persistent** failure is detected, which can cause a possible maloperation or failure to operate, the output circuits of the IED are set out of operation; in this case **ERROR** LED is lit. Signalling is provided by a normally-closed contact.

The main IED malfunctions and troubleshooting are shown in Table 3.4.



If failure is detected, report registered error codes, text description of a failure, information about latest device restart and configuration to Relematika or its representative.

Only specially trained personnel with dedicated equipment and tools is admitted to perform troubleshooting service.

After the failure is repaired and before the IED is put again into operation, the corresponding parameters (settings, disturbance recorder parameters, etc.) should be checked. Assure that IED operates properly.



Upon detection of the failure, it is necessary **first** to write down the error codes, which are displayed on the HMI, than report it to Relematika or its representative. In some cases (for short-term failures) it can be sufficient to interrupt power supply to remove the failure.

Table 4.4: Malfunctions and Troubleshooting

Feature	Possible reason	Error code	Troubleshooting
When turned on, the IED does not start, while the <b>READY</b> LED is off	Power supply failure	–	Replace / repair the IED
When turned on, the IED does not start, but the <b>READY</b> LED is on, the HMI has the inscription "Relamatika"	Defective logic block (processor)	–	Replace / repair the IED
There is no logic signal in protection when voltage is applied to a binary input	The node of inputs of one of the blocks of binary Input/Output is faulty	C:0x00002000*	Replace / repair the IED
Permanent open / closed state of the output relay inappropriate to the applied action	The node of outputs of one of the blocks of binary Input/Output is faulty	C:0x00004000*	Replace / repair the IED
A message about a malfunction of the IED hardware blocks during loading or during operation of the IED	One of the binary Input/Output units, power supply unit is faulty	C:0x00002000	Determine the faulty IED block by error codes. Restart the IED by removing the power supply, wait until the <b>READY</b> LED turns off. If the error persists after restarting the IED, repair/replace the IED
Software failure message	One-time software crash. Possible CPU board failure	A:0x00000002 A:0x00000004	If an error occurs repeatedly, update the protection circuit using the service software and restart the IED by removing the power supply until the <b>READY</b> LED turns off. If the problem persists, repair/replace the IED block
Reset message	Single failure of non-volatile memory of registrars and settings	A:0x00000020	Check and set configuration parameters. If the error persists, replace/repair the IED
DR memory failure message, possible loss of previous disturbance recordings	Single failure of non-volatile memory of disturbance recordings	A:0x00000080	The function is automatically restored. If the error persists, repair/replace the logic block, and there is no need to urgently take the device out of service

<b>Feature</b>	<b>Possible reason</b>	<b>Error code</b>	<b>Troubleshooting</b>
Clock failure message	One time reset	A:0x00000400	Check and, if necessary, set the IED time parameters. If the error repeats, replace/repair the IED, and there is no need for urgent withdrawal of the device from operation.
Fault message caused by configuration or protection scheme	The IED operates with an incorrect or inappropriate protection scheme	A:0x00000800 A:0x00010000 A:0x00020000 A:0x00400000 A:0x00800000 A:0x20000000	Check the compliance of the scheme with the protection IED, update the protection scheme using the service software
Other malfunctions			Troubleshoot IED replacement/repair
* Does not detect a malfunction of the output relay contacts (for example, sticking), as well as the operability of binary inputs, the integrity of the windings of intermediate current and voltage transformers.			

### 3.5 Disposal

On expiry of specified service life IED should be dismantled and disposed. No special safety measures should be taken while dismantling and disposing of a device nor special tools and accessories are required.

#### **4. Transportation and storage**

Transportation and storage conditions correspond to 1.1.8. Permissible shelf life period before commissioning is two years.

Transportation of a packed IED should be carried out by means of any closed-type transport. Transport packaging must be rigidly fixed.

Loading, fixing and transportation of the device should be carried out according to valid regulations for carriage of goods by corresponding means of transportation.

## **5. Manufacturer's warranty**

Relematika ensures compliance of IEDs with the standard specifications subject to operating, transportation and storage conditions by the customer.

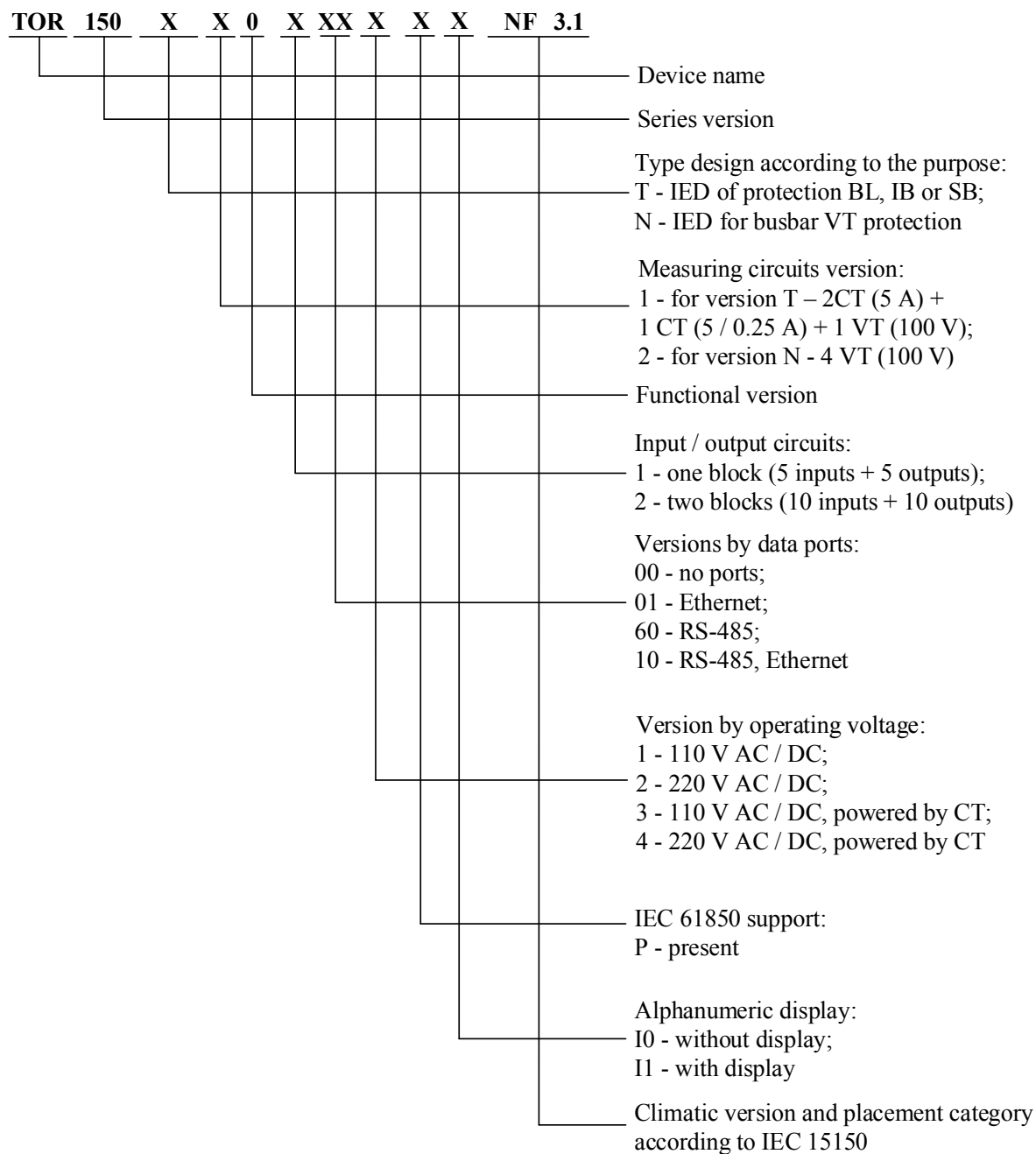
The warranty period is 5 years from the date of manufacturing. Extended warranty is provided upon additional agreement with Relematika.

Manufacturer warranty does not cover IEDs with mechanical damages and are not valid in the case of breach of operating conditions (influence of increased values of voltage, current, disturbance level, ingress of moisture and foreign current-conductive materials or objects inside the rack, etc.).

If device is supposed to be returned to Relematika, it should be packed in a package ensuring safety during storage and transportation.

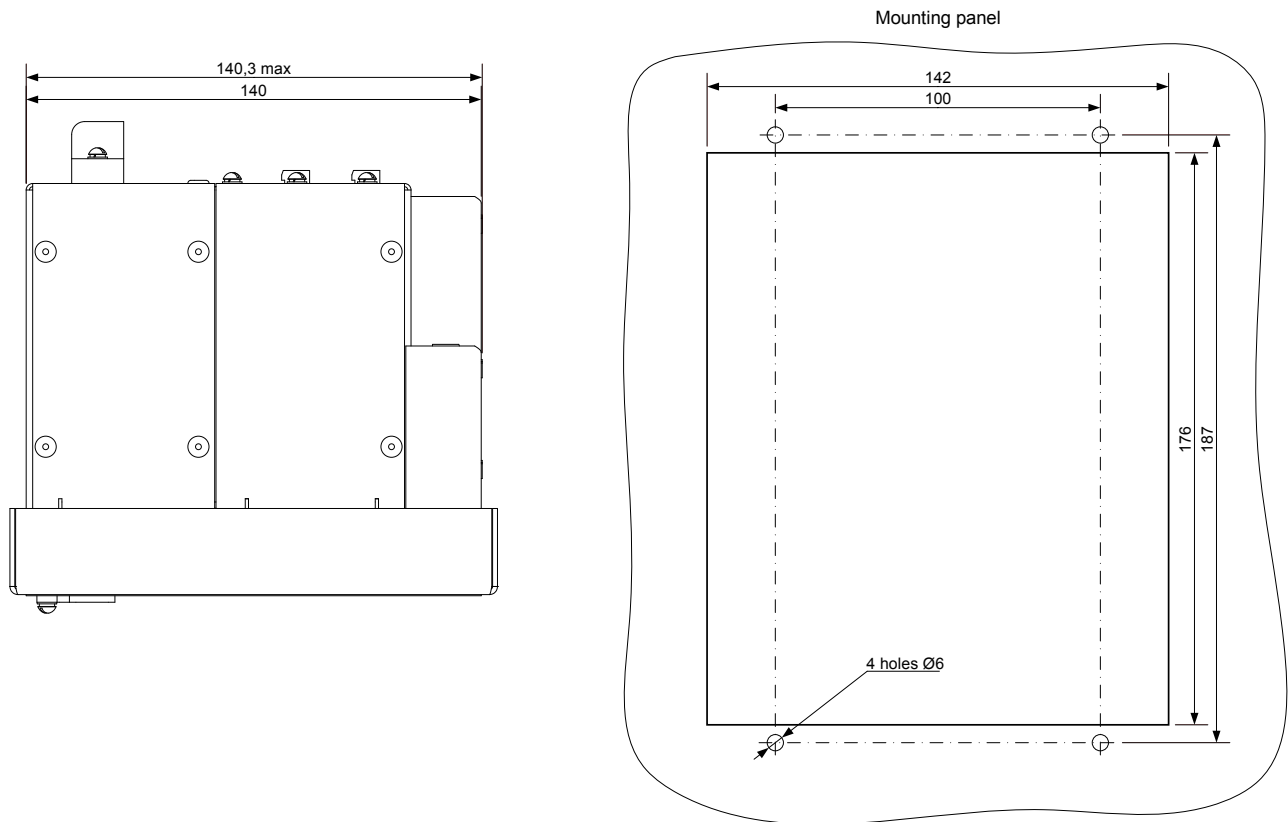
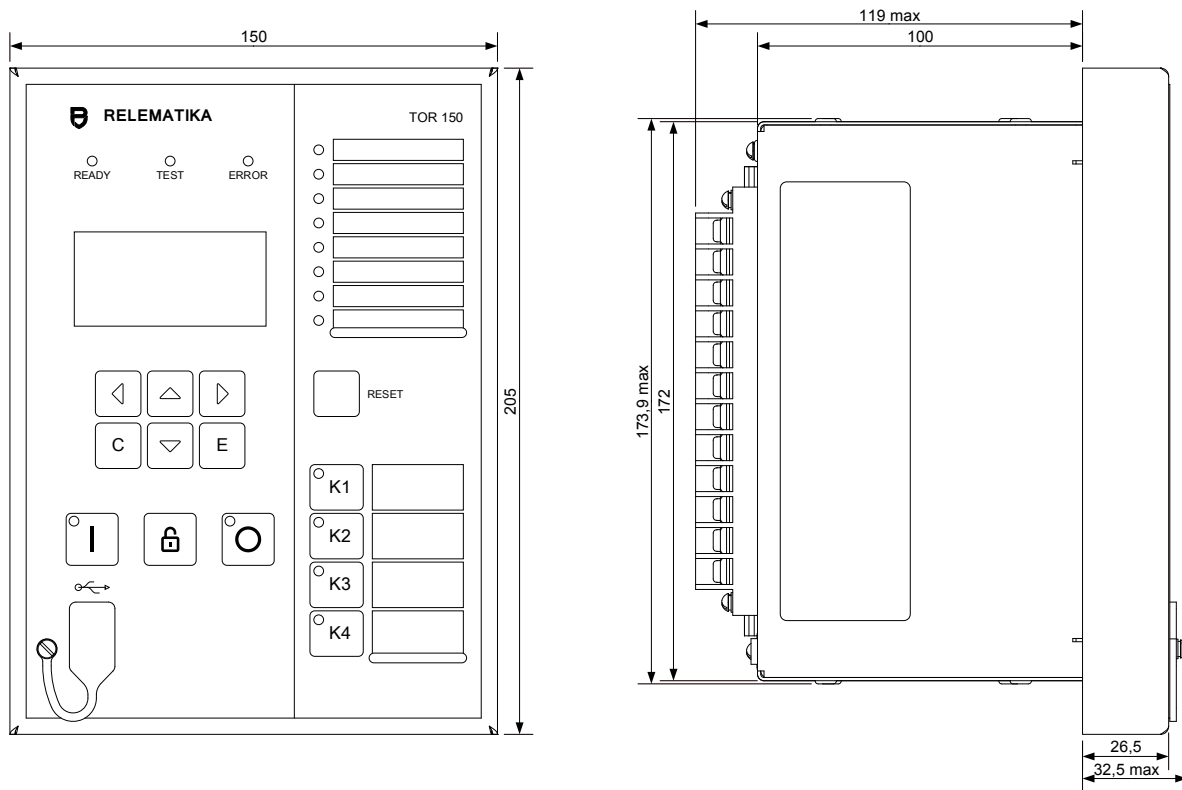
The Manufacturer should guarantee repair or replacement of the device during its lifetime. Shipment term of spare parts from Relematika warehouse should not exceed three months from the moment of signing the contract for purchasing of these spare parts.

## Appendix A Ordering structure



**Note** - The hardware design is selected at the manufacturing plant in accordance with the program execution and the number and type of analog inputs and binary Inputs/Outputs indicated in the Order Sheet.

## Appendix B Layout, overall and mounting dimensions (mm)



Weight : max. 2.5 kg for the version without power supply from CT;  
max. 3 kg for version powered from CT.

Figure B.6: Overall and installation dimensions of the TOR 150 device



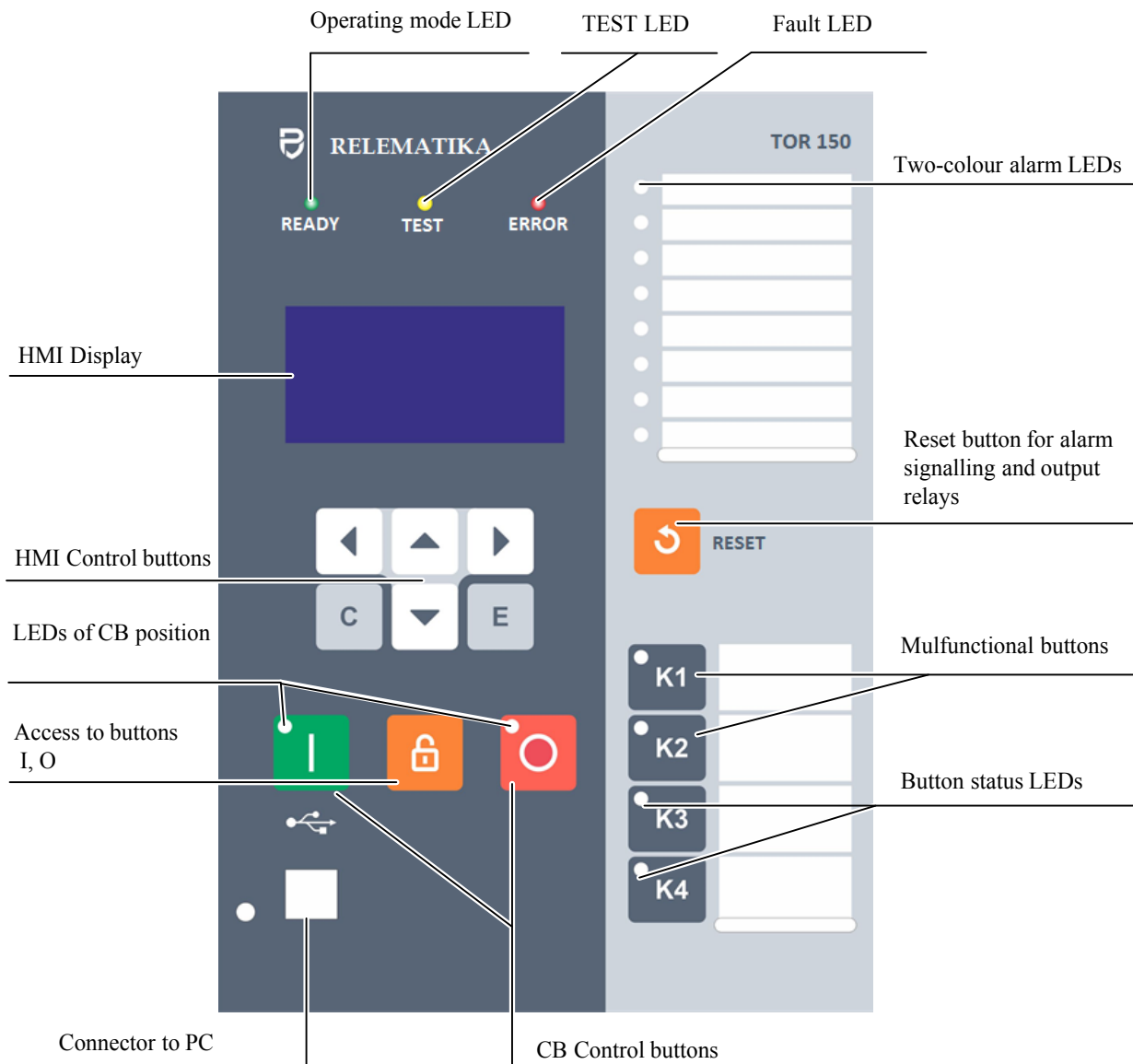
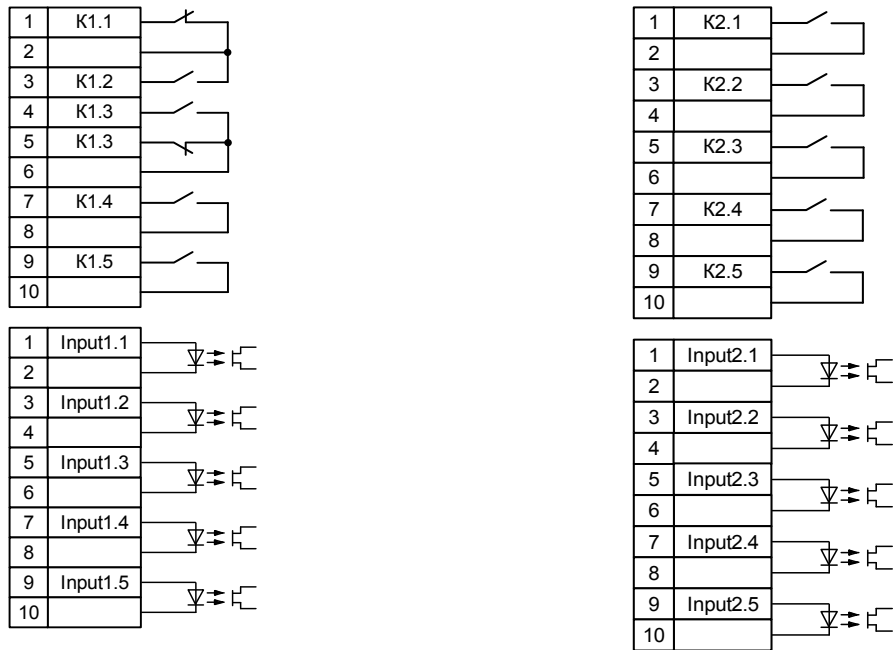


Figure B.7: HMI elements of TOR 150 IED

### Appendix C Inputs and Outputs of the blocks



a) Block P0503 (110/220 V AC/DC)

b) Block P0504 (110/220 V AC/DC)

Figure C.1: Input and output circuits of BI/BO blocks

## Appendix D

### Pin designation of communication ports

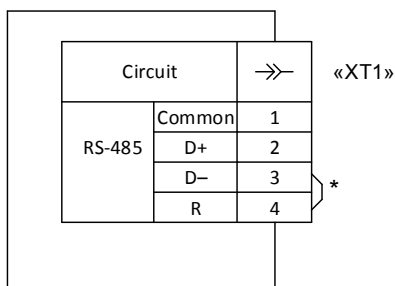


Figure D.1: Communication port RS-485

\* The jumpers are placed if the IED is installed at the end of the communication line. The number of resistors should not be more than two.

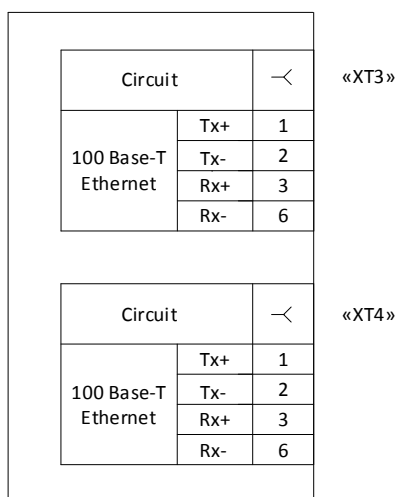


Figure D.2: Ethernet communication ports

Description of communication ports is shown in the following Table D.1.

Table D.1: Description of communication ports

Rear connector designation	Figure	Communication port
«XT1»	D.1	RS-485 (APCS)
«XT3», «XT4»	D.2	Ethernet 100 Base-T

## Abbreviations

APCS	Automatic Process Control System
ADC	Analog-to-Digital Converter
BDUBus	Proprietary Technological Protocol
CT	Current Transformer
EMC	Electromagnetic compatibility
Eth	Ethernet
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
GOOSE	Generic Object-Oriented Substation Event
HMI	Human-Machine Interface
MMS	Manufacturing Message Specification
NTP/SNTP	Protocol of time synchronization over a computer network
OM	Operator's Manual
PAC	Protection, Automation and Control
PC	Personal Computer
PRP	Parallel Redundancy Protocol
RTC	Real Time Clock
ROM	Read Only Memory (non-volatile memory)
SW	Software
VT	Voltage Transformer