

EuroProt+ Operating Manual with Troubleshooting Guide System version 2.10



DOCUMENT ID: PP-13-22720 VERSION: 1.3 2024-10-18, BUDAPEST

PROTECTION, AUTOMATION AND CONTROL FOR POWER INDUSTRY

VERSION INFORMATION

VERSION	DATE	MODIFICATION	COMPILED BY
1.0	2023-03-14	First published version	Saina, Zsarnai
1.1	2023-03-29	Minor corrections	Saina
1.2	2023-09-19	Events, disturbance recorder non-volatile info added	Erdős
1.3	2024-10-18	Minor corrections in chapter 4.1.2.1. Changes for firmware version 2.10.2.3013+ included in chapter 4.1.2.2 and chapter 4.2.3.	Saina

CONTENTS

1	Introd	uction		6
2	Startir	ng the de	evice	6
	2.1 T	he hard	ware modules of the device	6
	2.2 F	ast start	tup	6
3	Local	operatio	on on the front panel	7
	3.1 T	he struc	ture of the human-machine interface of the device	8
	3.2 U	Jsing the	e touch buttons	9
	3.3 U	Jsing the	HMI touchscreen buttons	11
	3.3.1	The	home screen	11
	3.3.2	The	parameters menu	12
	3.3.3	On-l	ine functions, Events, System settings	14
	3.3.4	Use	r-defined/Custom screens	14
4	Remo	ote opera	ation via web browser	16
	4.1 P	Propertie	s of the Ethernet communication	16
	4.1.1	The	Ethernet connection	16
	4.1	.1.1	Using the RJ-45 connection	16
	4.1	.1.2	Using the EOB connection	17
	4.1	.1.3	Using fiber optic connections	17
	4.1.2	Sett	ings needed for the Ethernet connection	17
	4.1	.2.1	Connection to the device with fix IP address $(2.10.2.3000 - 2.10.2.3012)$.	17
	4.1	.2.2	Connection to the device with fix IP address (2.10.2.3013+)	19
	4.1.3	Usin	g web browsers	20
	4.2 N	lenu iter	ns in the web browser	21
	4.2.1	Mair	n panel	21
	4.2.2	Para	ameters	22
	4.2	.2.1	Managing multiple parameter sets	24
	4.2.3	Syst	em settings	25
	4.2.4	Onli	ne data	26
	4.2.5	Evei	nts	27
	4.2.6	Dist	urbance recorder	28
	4.2.7	Corr	nmands	31
	4.2.8	Netw	vork protectionHood	32
	4.2.9	Doc	umentation	33
	4.2.10) Sec	urity	33
	4.2	.10.1	Security settings	33
	4.2	.10.2	User manager	34
	4.2	.10.3	Certificate handling	35
	4.2	.10.4	Alarms / Logging	36
	4.2	.10.5	Audit trails	37
	4.2.11	I Adva	anced	38
	4.2	.11.1	Maintenance	38

Ē









	4.2.1	1.2 I/O tester	
	4.2.1	1.3 Update manager	
5	Troubles	shooting	
	5.1 Wai	rning and Error Messages	
	5.1.1	Warning messages in the web browser	
	5.1.2	Error messages in the web browser	
	5.1.3	Error messages on the LCD screen	
	5.1.4	Operation of the IFR (Internal Fault Relay)	54
	5.2 Nec	cessary data before contacting Protecta Support	54
	5.2.1	Serial Number of the Device	54
	5.2.2	Information about firmware and configuration versions	55
	5.3 Qui	ck Troubleshooting	



USED SYMBOLS



Additional information



Useful information for settings.



Important part for proper usage.

1 Introduction

The **EuroProt+** type complex protection in respect of hardware and software is a modular device. The modules are assembled and configured according to the requirements, and then the software determines the functions. This manual describes the common properties of the numerous possibilities. It also provides technical guidance to operate the device locally with the LCD and remotely with a web browser. The individual characteristics of the specific applications are described in the manuals of the factory configurations.

2 Starting the device

In order to meet the device at the first time, this chapter provides information for new users to secure a safe first start-up of the device.

2.1 The hardware modules of the device

For technical details of the modules of the *EuroProt+* type complex protection please see the document *"Hardware description*". The applied modules for a certain application are listed in the corresponding *"Configuration description"* document. These documents are available online on the Protecta website by selecting the desired product.

2.2 Fast startup

The CPU module of the device is equipped with two processors: RDSP, for protection function processing, and CDSP, for communication function processing.

After powering up the device, the RDSP processor starts-up with the previously saved configuration and parameters. Generally, the power-up procedure for the RDSP and application functions takes approx. 4-5 sec. During this time the "Status LED" (see Figure 3-1) is red. If the protection functions are ready for operation the red LED turns to green, the fault relay NO contact closes (3-4 or 5-6) and the device is ready to trip after this short period. During the restart procedure after a new downloaded configuration, the LED is also red for a short time. Latched red LED however means general error. In this case the protection functions are not available.

The CDSP's start-up procedure is longer, because its operating system needs time to build its file system, initializing user applications such as HMI functions and IEC61850 software stack. The availability of the touch screen of the front panel after about 25-30 seconds indicates successful termination of the start-up procedure.



3 Local operation on the front panel



Figure 3-1 The front panel of the device

3.1 The structure of the human-machine interface of the device

The EuroProt+ device HMI on the front panel contains the following elements:

Table 3-1 The elements of the front par	ıel
---	-----

FUNCTION	DESCRIPTION		
User LEDs (16 pcs)	Three-colors, 3mm circular LEDs programmable by the user.		
COM LED (1 pc)	Yellow, 3mm circular LED indicating front panel communication link and activity		
Touch button LEDs (4 pcs)	Yellow, 3mm circular LEDs indicating touch button actions		
	Three-color, 3mm circular LED		
Status LED (1 pc)	Green: normal device operation		
	Yellow: device is in warning state		
	Red: device is in alarm state		
Touch buttons (4 pcs)	HMI touch buttons (On/Off Operation, Change Screen, LED acknowledgement), see Paragraph 3.2 for details.		
Buzzer	Audible touch button pressure feedback		
Changeable LED description label	Describes user LED functionality		
3.5" or optional 5.7" display	320*240 pixels TFT display with resistive touch screen interface		
Optical interface	This inteface is made for EOB connection, and/or serves as a service port for Protecta personnel only.		
RJ-45 connector	Supporting 10/100Base-T Ethernet connection		
	Ethernet Over Board: communication interface realizes isolated, non-galvanic Ethernet connection with the help of a magnetically attached EOB device. This is a proprietary and patented solution from Protecta Ltd.		
EOB connector (option)	EOB1 : Supporting 10Base-T Ethernet connection. Passive device with one RJ45 type connector. <u>Obsolete module.</u>		
	EOB2 : Supporting 10/100Base-Tx Ethernet connection. An active device that has a USB port in addition to the RJ45 connector for powering up. <u>All EOB topics in this manual are referring to EOB2.</u>		

3.2 Using the touch buttons

@\$**_**\$**_**\$ @\$**_**\$**_**\$

The home screen of the local LCD together with the red marked "Change screen button" and the "Operation buttons" is shown in the picture below.

0 0



Figure 3-2 The device face showing the home screen

Change screen button - This hardware button changes the currently displayed screen for the subsequent one. The available screens and the order in which they appear by default are: the home screen, parameters, online functions, events, system settings, security settings and the custom screens which can be added by the user with the help of the EuroCAP software. The order can be changed in the LCD editor of the EuroCAP configuration tool. When pressing the **"Change screen button"** – as an example – the windows shown in Figure 3-3 below can be seen and applied one-by-one, cyclically.

Parameter	function	າຣ			
User define Common VT4 module CT4 module CT4 module VT Supervis Distance pr	Onlin Binary Ir Binary Ou Common HMIButtor VI4 modul	e functions Eve Common Health of dev 2022-07-21 12 HV AutoReclos	nts System se System parame	ttings	
1Dir. commu Line Differ Teleprotect	CT4 modul CT4 modul VT Superv Distance 1Dir. com	Blocked:0n 2022-07-21 12 Common Health of dev 2022-07-22 06 HV AutoReclos Blocked:0n 2022-07-22 06	Station bus s Front etherne Ethernet comm Serial comm. Time synchron Timezone sett LCD backlight	Secure hand System serv Client whit	y settings Hling vices elist
			Set	Set	ţ. Save

Figure 3-3 Default menu screens (excluding the home screen) displayed on the LCD

Touch the navigation icons or the displayed text lines to perform any actions via the LCD screen.

Operation buttons - These buttons can be used to define certain functions on customer-defined windows. For example, the user can set up these buttons to turn on/off a circuit breaker or increment/decrement the position of the tap changer of a transformer. For more information, please refer to the User-defined/Custom screen section.

LED reset button – Pressing this button removes the latches from all active LEDs and resets them. Apart from an LED reset, this button can also perform other tasks depending on the relay configuration. Use of this button, as well as other HMI buttons can be changed using EuroCAP configuration tool by programming the outputs of the *HMI buttons* function block from the logic editor. For more details, see the respective manuals.







3.3 Using the HMI touchscreen buttons

The touchscreen is the main control area where the user will enable functions and input values by touching the screen. The touchscreen can be also remotely accessed and controlled through the web interface (for more information see the corresponding sections in the remote user interface).

3.3.1 The home screen

Lock icon – Touching this icon unlocks the device LCD interface, allowing a user to access various menu items in the device with specific privileges e.g. view settings, view data, manage settings, etc.



Figure 3-4 Unlocking the device LCD, notice the change in the "lock" icon

NOTE: The device is initially configured with the "Guest" user with all the privileges. As a result the user doesn't need to unlock the screen to access all the functions. However, if the "Guest" rights are limited, the user will need to unlock the screen by logging in in order to access some privileges.

The device is also initially configured with an "Admin" user with a default password **C1b3rS3c!**. Unlock the device with these credentials if the accessibility of the device is limited. See paragraph 4.2.10.2 for more details on user management.

Default/secondary languages (optional) - If available, the user can change the language of the device by pressing the corresponding flag. With this, the language will change (provided that the translations exist) on the following objects:

- remote web interface
- all menu points
- newly generated events
- newly created disturbance records
- device messages (e.g. command confirmation)



NOTE: if the language is changed by using the button on the web interface (see Paragraph 4.2.1), it will change on the web interface only; the other parts from the list above will remain as they were set here.

Information and LED buttons – By pressing the "i" button located on the top right corner of the home screen, additional information is displayed as shown in Figure 3-5. The LED icon on the top left corner starts the front panel LED test (see Paragraph 4.2.11.2).



Figure 3-5 Additional information on the home screen

3.3.2 The parameters menu

In this screen, the user can view, set and edit certain parameters within the device. The user can also choose which parameter set the device should use; this is done with the "Activate" button. The currently active parameter set has a red box around it (first set in the picture below).

In order to edit or activate a parameter set, touch its name first to select it: it will be highlighted in blue. Then touch the "Edit" or "Activate" button accordingly.

Parameter sets
Default_set_1
Default_set_2
Û
Edit Activate

Figure 3-6 Parameter sets

Activate button - Activates the selected parameter set so the device will use those values. The activated parameter set will have a red box around it. Only devices configured with multiple parameter sets have an activate button.

NOTE: if the parameterset change has a condition configured to it, the activation button will disappear. In this case, activation of the parameter sets is defined in the device configuration (e.g. binary input or software switch).

Edit button - This button takes the user to another screen listing the available function blocks (FBs).

The screen in Figure 3-6 will only appear if there are more than one parameter sets. Otherwise, the user is immediately taken to the function blocks. Normally, the various function blocks appear in blue. In case someone has changed a certain value within a given function block, the name of the function block in this menu item will turn red to notify the user. Within function blocks, the values of the parameters are normally green, but if they have been modified, they will also turn red. As an example, change the VT4 voltage type from 200V to 100V as follows:



Figure 3-7 Changing VT4 module Type



IMPORTANT! In order to finalize all changes, the user has to go back to the screen where all the function blocks are listed and save the changes as shown above.

Also, make sure that while someone is modifying the parameters in the LCD touchscreen, no one else is doing so on the web interface since this could lead to confusion as to what the values of a parameter set are.

Other parameters can be modified similarly to the previously described VT4 voltage type. The following parameter types are available in the function blocks:

Integer or timer - This is a whole number, and it can be entered with the help of the number pad.

Floating-point number - This is a number that has a decimal point. This can also be input through the number pad.

List item - A list is displayed with all the possible choices. In this case the user simply needs to select the desired one (e.g. VT4 voltage type).

Checkbox - The user has the option of enabling or disabling the parameter.

3.3.3 On-line functions, Events, System settings

These menu items have the same content as described in chapter 4. System settings can be modified similarly to the parameters in paragraph 3.3.2.

3.3.4 User-defined/Custom screens

It is possible to add screens based on the user's needs with the help of the EuroCAP software. The operation buttons can also be set up to perform certain functions. An example can be seen using a Single Line Diagram on the following page.

Consider a network represented by the SLD below and we have set up the required operational buttons to function as "on"/"off". To switch "on" the busbar disconnector Q1:

- 1. Touch the disconnector "Q1" icon on the touchscreen.
- 2. The selected object is highlighted and starts blinking. Some action must be performed with the chosen object; otherwise the selection times out after a short period.
- 3. So, while blinking, press the "I" button, which has been configured to be the "on" button when the Q1 object is highlighted.
- 4. A dialogue box pops up for confirmation of this operation. Again, a limited time is available for confirmation, otherwise the requested operation is canceled. Press "Ok" to confirm.
- 5. Another dialogue box pops up stating that the operation was successful. Press "Ok".
- 6. The scheme is updated accordingly, with the Q1 line disconnector in the "on" position.

Note again that this behavior was only an example; it may vary according to the configuration of the actual device.





Figure 3-8 Closing Q1 disconnector

This screen is updated in real time. A change in any sort of state or any parameter that is set up to be measured, will be shown and updated accordingly.

If there is an error with the operation (e.g. block by interlocking), the device will notify the user with another another dialogue box popping up with the reason for the error.

4 Remote operation via web browser

A web browser and an Ethernet connection are needed in order to access the device interface. HTML5 compatible web browser is recommended. To properly display the data on the screen, it is recommended to have a screen resolution of at least 1024x768. The latest version of the following web browsers can be used:

- Mozilla Firefox
- Apple Safari
- Google Chrome
- Microsoft Edge

JavaScript must also be enabled in your browser. For security reasons, the device allows only limited number of connections over the network (a maximum of 10 is guaranteed).

4.1 Properties of the Ethernet communication

The built-in 5-port Ethernet switch allows EuroProt+ to be connected to IP/Ethernet based networks. The following Ethernet ports are available in general:

On the front panel of the device:

• RJ-45 Ethernet or EOB (Ethernet over Board) user interface

On the rear side of the CPU unit:

- Station Bus (100Base-FX Ethernet)
- Redundant Station Bus which can be:
 - o 100Base-FX Ethernet, or
 - 10/100Base-T port via RJ-45 (only one can be active of these two)
- Process bus (100Base-FX Ethernet)

The different HMI and CPU types are utilizing different ports. Further information about the available ports and the applied interfaces on various HMI and CPU types can be found in the **"Hardware description"** document.

The embedded web-server supports the following actions:

- Modifying user parameters
- Managing the event list and disturbance records
- Managing passwords
- Online displaying measured data and generated binary information
- Performing commands
- Firmware update
- Performing other administrative tasks
- User management and security settings

4.1.1 The Ethernet connection

There are several ways to be connected to an Ethernet network. The availability of the below listed connection types depends on the device hardware configuration.

4.1.1.1 Using the RJ-45 connection

RJ-45 connector is available on the front panel if no EOB is selected for the configuration. In addition, many CPU types also utilize an RJ-45 connector, which is located on the rear side of the device on the CPU card. Using an UTP cable with RJ-45 connector at both ends, the device can be connected directly to a computer or an ethernet switch.







4.1.1.2 Using the EOB connection

EOB connection is available on the front panel if no RJ-45 connector is selected for the configuration. Attach the magnetic EOB connector to the front panel of the device (see Figure 3-1). The magnets assure the correct position of the adapter. Connect the other two ends of the cable to the RJ-45 connector and to the USB port of a computer. The special cable with magnetic connector on one end and RJ-45+USB connectors on the other end shall be ordered from Protecta.

4.1.1.3 Using fiber optic connections

The different types of fiber optic interfaces for 100Base-FX Ethernet provides connection to an Ethernet switch with identical fiber optic inputs. Using this connections all IED-s on the network with client functionalities, e.g. a computer, has access to the device. For more details about the fiber optic connector types see the CPU and COM module sections in the *"Hardware description*".

4.1.2 Settings needed for the Ethernet connection

The web interface of the EuroProt+ devices can be accessed over Ethernet based protocols only. Therefore, it is extremely important to set up the network before accessing the device.

Typically, the rear ports are connected to the substation network. The front port is ideal for management or troubleshooting. Station bus settings and front ethernet settings can be defined separately.

To connect the device to a station or corporate network, contact the system administrator for available IP address, gateway address, net-mask, DNS and NTP server addresses.

The user can also connect directly to the device via Ethernet protocol. In the following guidance, we assume that the user connects directly to the device via computer without the presence of any active network component (e.g.: switch, router).

4.1.2.1 Connection to the device with fix IP address (2.10.2.3000 – 2.10.2.3012)

The device uses fix IPv4 address range and the user is allowed to modify the address. User's computer must be set with fix IP address and netmask according to the used IP address range and netmask in the device.

Settings of the device:

The initial IP addresses of the device can be read from the home page of the LCD. If connected via the rear ports, use the displayed station bus "IP address". By default the device uses the station bus IP address in all ports including the front. The default netmask is 255.255.0.0. If the front ethernet IP is different, in any case it can be read from the same LCD screen, "FE IP address". The default FE netmask in that case is 255.255.0.0.

After the initial setup, the IP address settings can be changed from the **System settings** \rightarrow **Station bus settings** menu for the rear ports and **System settings** \rightarrow **Front ethernet settings** for the front port.

The screenshot below shows sample **Station bus settings**:





[-] STATION BUS SETTINGS			
		Device value	New value
IP address		192.168.80.11	192.168.80.11
Netmask		255.255.0.0	255.255.0.0
Default gateway		192.168.1.1	192.168.1.1
IP address mode	0	Static IP	Static IP
DNS1 address		192.168.1.1	192.168.1.1
DNS2 address		0.0.0.0	0.0.00
Redundancy mode	0	PRP	PRP



Sample **Front ethernet settings** in "separate" mode are shown below:

		Device value	New value		
Mode	?	Separate	Separate	~	
VLAN Id	?	4094	4094		(1 - 4094 /
IP address		10.200.200.1	10.200.200.1		
Netmask		255.255.255.0	255.255.255.0	~	
Internal network access	?				
DHCP server		V			

Figure 4-2 Sample front ethernet settings in the device (separate mode)

Settings of the user's computer (with fix IP address):

• Connection to the station bus

The possible IP settings of the user's computer according to the sample device settings above: *IP address:* in range from 192.168.0.1 to 192.168.254.254*

Netmask: 255.255.0.0 Default gateway:192.168.0.1

*Note: the IP address must differ from that of the device

Internet Protocol Version 4 (TCP/IPv4) Properties					
General					
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator				
Obtain an IP address automatical	у				
Use the following IP address:					
IP address:	192 . 168 . 10 . 12				
Subnet mask:	255.255.0.0				
Default gateway:	192.168.0.1				
Obtain DNS server address autom	atically				
• Use the following DNS server add	resses:				
Preferred DNS server:					
Alternative DNS server:					
Validate settings upon exit	Advanced				
	OK Cance	el			

Figure 4-3 An example of settings in the user's computer with fix IP address

• Connection to the front ethernet (separated mode)

The front ethernet port has an embedded DHCP server. To connect the PC, enable DHCP by checking the "DHCP server" box under the **Front ethernet settings** tab as shown in Figure 4-2**Error! Reference source not found.** above. Secondly, use automatic IP settings in the PC network settings. See Figure 4-4 below.

Internet Protocol Version 4 (TCP/IPv4) Properties	×
General Alternative Configuration		
You can get IP settings assigned auto this capability. Otherwise, you need t for the appropriate IP settings.	omatically if your network suppo to ask your network administrat	orts or
Obtain an IP address automatica	ally	
O Use the following IP address:		
IP address:		
Subnet mask:		
Default gateway:		
Obtain DNS server address auto	matically	
OUse the following DNS server ad	dresses:	
Preferred DNS server:		
Alternative DNS server:		
Validate settings upon exit	Advanced	ł
	OK Ca	ancel

Figure 4-4 Possible settings in the user's computer with DHCP server

IMPORTANT: Caution shoud be taken if the front ethernet port has to be connected to the corporate network. In these cases, as a safe practice, uncheck the "DHCP server" box in the **Front ethernet settings** tab, otherwise the device could act as a new DHCP server in the network.

4.1.2.2 Connection to the device with fix IP address (2.10.2.3013+)

Settings of the device:

• Switch mode "On", Front Ethernet "integrated"

This is the default mode of the device and it is expected that when the device is first shipped, these will be the applied settings. To connect to any port of the device in this mode, the IP address can be read from the LCD homepage. Since only the IP address is displayed, the user will need to know the default netmask, which, like in earlier firmware versions, is 255.255.0.0.

• Front ethernet separated

At the first changing of the front ethernet setting mode to 'separate', the default network mask is 255.255.255.0. So, if the LCD displays a different "FE IP address" from the switch "IP address", the user can use the default netmask. Otherwise, to get the exact settings, refer to IP Network settings tab under device system settings (to see how to access system settings, see chapter 3.2).

• Switch mode "Off"

If the switch mode is OFF, to check the settings of the specific port through which the user is connected, refer to IP Network settings.

Settings of the user's computer:

0 0 0

The settings of the users computer remains the same as in chapter 4.1.2.1. To connect to the station bus, use manually assigned IP address as in Figure 4-3. To connect to the separated front ethernet, use automatically assigned IP as in Figure 4-4.

For more details on connection to the device via ethernet, refer to **Cybersecurity and Connectivity Guide for firmware versions 2.10.2.3013+** available in the Protecta website.

4.1.3 Using web browsers

First the user must check if the browser is accessing the device via proxy-server. If there is a proxy-server in the network, the system administrator shall be contacted in order to get access.

If this is clarified, the user can type the IP address of the device into the browser's address bar. (The IP address can be read from the home screen of the local LCD). After that the usual procedures of web browsing shall be followed.



4.2 Menu items in the web browser

4.2.1 Main panel

	[-] FRONT PANEL					
Main						
Parameters		•	E2-Line E	1		
System settings		Concerned Train	<u>-</u> -		urrent time:	
Online data		General Imp	oc mp	15 Aug	g, 2022 14:03:39	
Events		 Z1 Trip 	Res OC Trip	• s	tation name:	
Disturbance recorder		Z2 Trip	Voltage Trip	•	Protecta	
Commands		Z3 Trip	Frequ Trip	•	Class	
Network protectionHood Documentation		• Z4 Trip	NVRS	• 19	IP address: 02.168.80.11	
Security		Z5 Trip	AutoReclose	•	IP address:	
Advanced		Dis Start	LDiff Trip	• 19	92.168.80.11	
Login		AR Blocked	LD CommFail			
** =			×			
Active Security Alarm 🖄					PROTECTA	
						_
	IDENTIFICATION					
	Station name		Protecta			
	Device name		Class	Rename	1	
	Serial number		100766			
	Scharhamber		130700			
	INFORMATION					
	Device uptime		0 hour(s), 1 minute(s)			
			134 day(s), 15 nour(s)			
					פת	

Figure 4-5 Main menu

The front panel of the device can be controlled from here (Figure 4-5). The image in the center of the screen acts/responds in the same way as the touch screen and the LEDs, except the on (1) and the off (0) buttons. These two buttons are inactive for security reasons.

The X button on the bottom of the front panel picture initiates a LED reset. LED description text is determined by the configuration and may be different than the actual label inserted in the device front panel.

Identification - User can change the station and device names from this panel by typing in the new values and clicking on the Rename button. IEC61850 IED name is only for display here but can be edited in the EuroCAP tool if needed.

Information part - There are two fields for measuring device operating time. Uptime field displays the time elapsed from the last power on of the device. Device lifetime field value equals the number of days of the device's energized state. In case of a CDSP update, the device uptime disappears and RDSP/CDSP uptime appear.

The language button (if present) under the menus changes the displayed language on the webpage only. This means that the menus (parameters, settings etc.) will be shown in the chosen language, but the events and disturbance records will still be generated on the language set on the main local LCD screen (see Paragraph 3.3.1 for details)



4.2.2 Parameters

Various parameters and variables can be viewed and changed in this menu item. The user can manage different parameter sets with the ability to set, rename, export and import them. A password can be applied for the import, export and set settings options. All parameters are part of a certain function block which can be individually opened or closed using the [+] or [-] symbol. Parameter values are displayed and can be modified in text fields, list boxes or check boxes.

Expand all Co	ollapse all	Print		
[+] Соммон				
-] VT4 MODULE				
	Device valı (Par set 1)	ie New value		
ange	Туре 100	Type 100	~	
onnection U1-3	Ph-N	Ph-N	~	
onnection U4	Ph-Ph	Ph-Ph	~	
rection U1-3	Normal	Normal	~	
rection U4	Normal	Normal	~	
T correction	100	100	÷ %	(100 - 115 / 1)
	100.00	100	÷ kV	(1.00 - 1000.00 / 0.01)
ated Primary U1-3	100.00	100		

Figure 4-6 Parameter settings

Buttons on the top of the parameter's sheet provide fast expanding and collapsing all the function panels and make finding a parameter easy. Print button generates a printer-friendly layout opened in a new browser window.

General layout of the parameter's sheet consists of columns:

The first column contains the name of the parameter, this text comes from the configuration of the device.

Second column displays the current values of the selected parameter set stored in the device. The parameter set can be chosen from the combo-box of the main menu (see Figure 4-7). Changing the parameter set here doesn't mean activating it, only loading to the fields. You can find more information on activation in this chapter later.

Third column is used by the user to enter the desired settings. The expected value range and step are shown on the right side of the parameter column.

Changing any setting in the third column will be marked with blue function block name and with blue text in the corresponding line of the first column.

The detailed description of fields are as follows:

Textfield - Text fields hold values that can be modified. To prevent invalid values from being loaded into the device, make sure that all values entered are within proper range. In case a wrong value is entered, the user will be alerted and the value is reset to the last correct value.

Listbox - By clicking on the list box, the user can choose from the available values listed within the box. (The list box represents enumerated type parameters.)

Checkbox - The user can enable or disable certain functions and properties with the check box, by clicking on the box. If the checkbox is ticked, the parameter is enabled. In contrast, if the check box is empty, the parameter is disabled. (The check box represents boolean or binary type parameters.)

▋¢**▋**Φ**┃**Φ **□**Φ**┃**Φ**┃**Φ

Unit - This displays the unit of parameter where applicable. Not all parameters have units.

Range/Step - This applies only to text fields; it displays the range a value can take. The step value represents the amount by which the value can be incremented/decremented. For example, if a parameter has a default value of 100 with a range of 1-1000 and a step value of .01, its value can be changed to 99.99, or 99.98, or 99.9, or 99 or 100.01, or 100.02, or 100.1, or 101, and so on. The value cannot go below 1.00 or above 1000.00, since that would be out of range. As another example, if the same parameter had a step value of 5, then we could only change the default value of 100 to 95, or 105, and so on.



Figure 4-7 Main menu view with and without multiple parameter sets

Modified parameter values can be written into the selected parameter set by clicking "Set parameters" button on the main menu panel. In case of a device with only one parameter set there is no parameter set selector combo-box, as it can be seen on the right side of Figure 4-7.

Values are checked for change before the user navigates away from the actual page or another parameter set is being loaded. By pressing Cancel, the browser will remain on the actual page. By pressing OK, the browser will ignore the changes made and navigates away to the page selected.



Figure 4-8 Unsaved data when leaving the page







4.2.2.1 Managing multiple parameter sets

Towards the bottom of the page there are options to manage parameter sets. These buttons and functions only appear if the device is configured to have more than one parameter set. The following buttons are available:

PARAMETER SET	Text fields				
Default_set_1	Rename	Save parameters		Load to editor	
Default_set_2	Rename	Save parameters	Activate	Load to editor	
EDITABLE FIELDS					
Reset to defaults	Load parameters				

Figure 4-9 Parameter set control field

Rename - This renames the selected parameter set after the user types in a desired name in the text field. Make sure that you use alphanumeric characters, spaces, dashes, or underscores as input and that no another set has the same name.

Save parameters - Corresponding parameter set can be saved as a *.par file.

Activate - This enables to activate the parameter set that in line with the button so the device will use the values from that specific set. This button only appears, if there is more than one parameter set and there are no other specified conditions in the configuration for activating the parameter set. The active parameter set name will be displayed in green.

NOTE: Activating a parameter set doesn't load the values to the edit fields above. Parameter set values can be loaded into the editable fields by using the combo-box placed on the left side of the main menu panel (see Figure 4-7) or by clicking on the Load to editor button.

Load to editor - This will load the parameter set in line with the button in the editable fields.

Reset to defaults - This resets the values on screen with the factory default settings.

Load parameters - This loads a previously saved parameter file and sets the values on the screen based on its contents.



4.2.3 System settings

In this menu item, some adjustments can be made to general device settings. The text fields, list boxes, and check boxes are almost the same as in the **Parameters** menu item except for one type of text field, the IP address field, which is found only here in the system settings menu item.

Main		Settings
Parameters		
System settings	Expand all Collapse all Print	
Online data		
Events	[+] System parameters	
Disturbance recorder		
Commands		
Network protectionHood	[+] STATION BUS SETTINGS	
Documentation		
Security		
Advanced	[+] FRONT ETHERNET SETTINGS	
Login		
Set settings	[+] ETHERNET COMM.	
*		
Active Security Alarm 🖄	[+] SERIAL COMM.	

Figure 4-10 System settings menu

The behavior of the **System settings** menu is very similar to the **Parameters** menu. Brief explanations of each item in the **System settings** menu are available below:

System parameters – This field is used for power system frequency setting.

Station bus settings – This field includes settings for the Ipv4 based communication like IP address, IP address mode, redundancy mode, mask, gateway, and DNS addresses.

Front ethernet settings – The front ethernet settings field is used to define the settings related to the ethernet port on the front panel of the device. Mode, Ipv4 address and netmask, VLAN settings can be keyed in here. Once again, caution is adviced in the use of the DHCP server setting here. Refer to paragraph 4.1.2.1 for more information.

Ethernet communication – The device can communicate using several Ethernet based protocols at the same time. Only the IEC61850 communication is licensed, all the other protocols are available by default.

Serial communication – Only one protocol can be selected for serial communication purposes, physical parameters can be set in this field. Note that serial communication needs appropriate CPU card.

Time synchronization – The device handles broad range of time synchronization protocols: NTP server (SNTP), serial communication, and different pulse inputs. If Time sync. Warning parameter is enabled and the device is not synchronized, an alarm is raised (status LED goes yellow).

Time zone settings – Use this field to set the offset to the GMT time and the settings of daylight saving.

LCD backlight – Parameters in this field control the behavior of the LCD panel. Backlight will switch off after its timeout. The Backlight group is useful if you have more than one device close to each other. Touching one of them will switch on the LCD screen of all devices that belong to the same group.

Alternative/additional menu items in fw versions 2.10.2.3013+

IP Network settings – The user can set IP addresses, netmask, default gateway etc. settings of different interfaces in the device. The user has the option to assign different ports to different networks and assign different IP settings. Refer to the Cybersecurity and Connectivity Guide for more information.

IP Routes – The user can define destination nodes and gateways through which specific device network interfaces can direct their packets. Refer to the Cybersecurity and Connectivity Guide for more information.

Ethernet interfaces – The physical state of the ethernet ports available in the device can be controlled here. The three settable states for each port are are "Enable", "Disable" and "Power off". The "MTU" setting is also available here.

Network protocols and services – Various device protocols and services can be enabled here. They can either be enabled on individual networks (defined under IP network settings) or on all of them (Global). More information is available in the Cybersecurity and Connectivity Guide.

More information about a particular setting can be obtained by hovering over the helptext question mark in the setting row.

4.2.4 Online data

This displays data measured by the device. The values on the screen are updated in every second. All data on this page is read-only, therefore they cannot be modified. In case there is a counter on the page, there will be a button next to it, which will reset it.

in	[+] Соммон			
rameters				
tem settings	[+] HMIBUTTONCLASSIC			
line data				
	[-] VT4 MODULE			
turbance recorder				
nmands	Voltage Ch - U1	28.63	V	
work protectionHood	Voltage Ch - U2	28.53	V	
umentation	Voltage Ch - U3	28.61	V	
urity	Voltage Ch - U4	0.00	V	
vanced	Angle Ch - 111	0	dag	
in	Angle Ch - U2	420	deg	
-	Angle Ch - 02	-120	deg	
	Angle Ch - U3	120	deg	
ive Security Alarm 🖄	Angle Ch - U4	0	deg	- 100.0 V
	[-] CT4 MODULE POS. T			
	Current Ch - I1	1.00	Α	
	Current Ch - I2	1.00	Α	
	Current Ch - I3	1.00	A	-
	Current Ch - I4	0.00	Α	$(//\Delta + \gamma)$
	Angle Ch - I1	4	deg	
	Angle Ch - 11	-1	deg	
	Angle Ch - 12	-121	deg	
	Angle Ch - I3	119	deg	
	Angle Ch - I4	0	deg	- 1.0 A

Figure 4-11 Online sheet

Binary data are displayed as checkbox, enumerated data will be presented as text information. If user has HTML5 compatible Internet browser, certain analogue measurements will be drawn as vectors.



4.2.5 Events

The **Events** menu displays the internal event list of the device. Every event is listed with time stamp, function block title, event type and event status. Time resolution is 1 ms, the device can contain approximately 10000 events in its non-volatile memory. If the list grows larger than this, the oldest events are erased.

If the mouse cursor hovers over a function block title for a short time, all event entries that belong to the same function block are highlighted in bold. Also, if the cursor is over an event type, all events of the same type will be highlighted (Figure 4-12).

The **Events** page is not refreshed automatically, the user can refresh it by clicking on the Refresh button.

Erasing all events and exporting them to a text file is also possible.

An **Event filter** can be utilized according to user's needs: there are filters for event row number, date and contained text, see rightmost part of the picture.

	Times	tamp	Func	tion block title	e Event ty	pe E	Event Status
Main		1			/		Events
Darameters		+				/	
System settings		Retresh	Erase al	l events Export	to file		
Online data			\		/		
Events	Eve	INT IST		↓			EVENT FILTER
Disturbance recorder	210		10.00.00	Distance contration	Charles 1.2		
Commande	218.	2022-11-29	16:22:20.010	Trip Logic	Start L2	* *	Ordinal:
commandy	219.	2022-11-29	16:22:28.538	Trip Logic	General Trip	+	-
Network protectionHood	220.	2022-11-29	16:22:28.538	Distance protection	71 Start	+	
Description	222	2022-11-29	16:22:28.530	Distance protection	Z1 Trip	+	Date:
Documentation	222.	2022-11-29	16:22:28.538	Distance protection	Z1 Faulti oon	11-12	dd/mm/yyyy 🗖 -
Security	223.	2022-11-29	16-22-28 538	Distance protection	Start L1	+	da/ ==/ , , , , , , , , , , , , , , , , ,
	224.	2022-11-29	16:22:28.538	Distance protection	Start L2	+	dd/mm/yyyy
Advanced	225	2022-11-29	16:22:28 558	Distance protection	72 Start	÷	
logout	227	2022-11-29	16:22:28.558	Distance protection	72 Faulti oop	11-12	Contains:
	227.	2022-11-29	16:22:28.558	Distance protection	73 Start	+	
Active Security Alarm	220	2022-11-29	16:22:28 558	Distance protection	Z3 Faulti oon	11-12	
Active Security Autoritie	230	2022-11-29	16-22-28 562	Distance protection	74 Start	+	
User: admin Role: Full Access	231	2022-11-29	16:22:28 562	Distance protection	74 Faulti oon	11-12	
59:36	232	2022-11-29	16:22:28 562	Distance protection	75 Start	+	
Change Decement	233.	2022-11-29	16:22:28.562	Distance protection	Z5 Faulti oop	11-12	Reset
change Password	234	2022-11-29	16:22:29.006	Distance protection	72 Trin	+	
	235.	2022-11-29	16:22:29.506	Distance protection	Z3 Trip	+	
S.	236.	2022-11-29	16:22:29.510	Distance protection	Z4 Trip	÷.	
	237.	2022-11-29	16:22:29.510	Distance protection	Z5 Trip	÷.	
	238.	2022-11-29	16:22:29.722	Distance protection	Z1 Start	Ļ	
	239.	2022-11-29	16:22:29.722	Distance protection	Z1 Trip	1	
	240.	2022-11-29	16:22:29.722	Distance protection	Z4 Start	Ļ	
	241.	2022-11-29	16:22:29.722	Distance protection	Z4 Trip	+	
	242.	2022-11-29	16:22:29.722	Distance protection	Z5 Start	Ļ	
	243.	2022-11-29	16:22:29.722	Distance protection	Z5 Trip	Ļ	
	244.	2022-11-29	16:22:29.726	Distance protection	Z2 Start	+	
	245.	2022-11-29	16:22:29.726	Distance protection	Z2 Trip	+	
	246.	2022-11-29	16:22:29.726	Distance protection	Z3 Start	+	
	247.	2022-11-29	16:22:29.726	Distance protection	Z3 Trip	+	
	248.	2022-11-29	16:22:29.726	Distance protection	Start L1	+	
	249.	2022-11-29	16:22:29.726	Distance protection	Start L2	+	
	250.	2022-11-29	16:22:29.730	Trip Logic	General Trip	+	
	251.	2022-11-29	16:22:29.774	Distance protection	Fault Loc. km	42.0 km 🚽	
							PROTECTA

Figure 4-12 Sample event list

4.2.6 Disturbance recorder

The **Disturbance recorder** (Figure 4-13) page allows the user to download or view the recorded disturbances. Every record is stored in COMTRADE format in the device's non-volatile memory and can be downloaded in a zipped file (with CFG, INF and DAT files inside). The displayed recording time information is used as a reference to the stored records. Records can be downloaded individually or as a batch. By clicking the "Download all" button, all records will be downloaded into one compressed (.zip) folder.

0 0

NOTE: The disturbance recorder function has a limited storage capacity, after which the records are overwritten on a FIFO basis.



Figure 4-13 The disturbance recorder page

A simple built-in preview function makes work easier (Figure 4-14 to Figure 4-17). This previewer allows for a quick evaluation of the disturbance. Both analogue and binary channels are displayed on the screen.

On the right side there is a floating panel with buttons to control the behavior of the display. Buttons with plus and minus sign are used for adjusting the horizontal zoom of the picture. Clicking on the "1:1" button resets the view to the default horizontal size. Scale mode is a toggle button to change the way of the analogue channel drawing. By default, it is drawn using a common vertical scale calculated from all available analogue channels with the same unit parameter. In other words, it uses a grouping of the channels according to their unit. If the user clicks on this button, every analogue channel will be drawn with its individual scale calculated from the maximal value of that channel.

Time evaluation is possible by placing markers on the time functions of the recorded disturbances. Upon opening a record preview file,

- 1. A permanent marker along the time domain indicates the trigger time of the disturbance.
- 2. A hovering marker indicates the post-trigger time.
- 3. The marker could also indicate the pre-trigger time by hovering over the reverse side of the permanent marker.
- 4. By clicking anywhere along the record, the time stamp is removed from the permanent marker and placed on the newly-clicked position. After this, again, a hovering marker (similar to the pre-trigger/ post-trigger duration) displays the time window.



Figure 4-14 Record preview – analogue channels showing post-trigger time



Figure 4-15 Record preview – pre-trigger time



ф ф ф ф ф ф





Figure 4-17 Disturbance record's binary channels



4.2.7 Commands

The device may contain function blocks with controllable objects whose commands appear on this page. A command can be issued by clicking the appropriate button on the field of the function. A confirmation dialog will ask the user to confirm the command (Figure 4-19).

Main					Commands
Parameters					
System settings	Соммон				
Online data	Mode of device	On	Blocked	Test	
Events		Test/Blocked	Off		
Disturbance recorder	LEDReset	Off	On		
Commands	Simulation	Off	On		
Network protectionHood					
Documentation	1DIR. COMMUNICATION MODULE				
Security					
Advanced	LDC Diagostic Reset	On			
logout					
	HV AUTORECLOSING				
Active Security Alarm 🖄	AR block	Release	Block		
User: gideon Role: Full Access 50:33					
Change Password	CD WEAR				
	Counter Clear	Off	On		

Figure 4-18 Command sheet

Main Parameters	Common			192.168.80.11 says Are you sure to execute the following command: Common Mode of device Test/Blocked?	
System settings				OK Co	incer
Unline data	Mode of device	On	Blocked	Test	
Events		Test/Blocked	off		
Disturbance recorder	LEDReset	Off	On		
Commands	Simulation	Off	On		
Network protectionHood					
Documentation					
Security	1DIR. COMMUNICATION MODULE				
Advanced	LDC Diagostic Reset	On			
logout					
** 🗖	HV AUTORECLOSING				
Active Security Alarm 🖄	AR block	Release	Block		
User: gideon Role: Full Access 02:04:43	CB WEAR				
Change Password	CD ITEAR				
	Counter Clear	Off	On		

Figure 4-19 Confirmation dialog

The mode of device defined in the **Common** function block has 5 setting options based on IEC61850-7-410 definition; these commands are present in all EuroProt+ devices:

- "On" mode is meant for the normal operation of the device, where all the inputs are received, displayed, processed, outputs generated, and events reported to client.
- In "Blocked" mode, the inputs are received, displayed, but are not processed. No outputs are generated, nor events reported to client.
- In "Test" mode, all inputs are received, displayed, processed, outputs generated, but the events are flagged as "test" as they are reported to client.
- The "Test/Blocked" mode enables the device to receive, display and process the inputs. Like in test mode, event reporting is flagged as "test". The device does not generate any outputs. The outputs are blocked.
- In "Off" mode, the inputs are received but not displayed, not processed, no outputs are generated, no events are generated.

The table below summarizes the operation of each mode as specified by the standard.

MODE OF DEVICE:	ON	BLOCKED	TEST	TEST/ BLOCKED	Off
Function	active	active	active	active	not active
Outputs (to process)	generated	not generated	generated	not generated	not generated
Reporting (to client)	yes	no reporting	flagged as test	flagged as test	no reporting
Control services (from client)	accepted	rejected	accepted	accepted	rejected
Functional (process related) data	visible	visible	visible	visible	not visible

Table 4-1 Mode of operation commands

4.2.8 Network protectionHood

U U U U

This menu shows devices that are located on the same network as the device. Compatible devices are identified and information is displayed about them. The currently accessed device is highlighted in red. By clicking on the other links, the user will be redirected to the corresponding device.

٠	[] D									
meters	[-] 014	ICES FOUND ON T	HE NETWORK							
tem settings										
line data	Health	IP Address	Platform	Station name	Device name	Version	Functionality	RDSP/Xilinx	CDSP rev.	Station bus MAC
nts	0	192.168.18.106	EuroProt+	Unnamed station	Unnamed device	2.10.2	SuperDev	2.10.2.3010-rc2-146-gc6e07baee/0.12	2.10.2.3010-19-ge15f4f5-dirty	00:22:DD:00:57:37
turbance recorder	0	192.168.88.12	EuroProt+	Kristof_RTS_device	SideB	2.8.13	I>, Id, Z<	2.8.13.2080-H5/0.6	2.8.13.1550-H4	00:22:DD:00:3D:3
dibunce recorder	0	192.168.79.21	EuroProt+	Applikáció	DIS21 teszt	2.8.13	I>, Id, Z<	2.8.13.2080-H6-rc1/0.6	2.8.13.1560-H5	00:22:DD:00:37:36
nmands	0	192.168.85.97	EuroProt+	Unnamed station	Unnamed device	2.8.13	I>, Id	2.8.13.2030/0.6	2.8.13.1520-H1	00:22:DD:00:19:38
	0	192.168.27.77	EuroProt+	Unnamed station	Unnamed device	2.10.2	Busbar	2.10.2.3010-rc2/0.13	2.10.2.3010-19-ge15f4f5-dirty	00:22:DD:80:15:38
work protectionhood	0	192.168.18.46	ACOS-300	Unnamed station	Unnamed device	2.10.2	I>	2.10.2.3010-H1-rc1/0.7	2.10.2.3010	00:22:DD:80:08:44
umentation	0	192.168.176.176	EuroProt+	CALDONAZZO	TR-ROSSO	2.8.13	I>, Id, Z<	2.8.13.2063-H1/0.6	2.8.13.1551	00:22:DD:00:30:4
	<u> </u>	192.168.21.232	EuroProt+	Protecta_MEO	Mennydörgés	2.8.13	I>, Id	2.8.13.2080-rc3-5-gec29e8c6a/0.6	2.8.13.1560	00:22:DD:00:2A:5
urity	0	192.168.77.59	EuroProt+	Unnamed station	Unnamed device	2.10.1	I>, Id	2.10.1.3000/0.13	2.10.1.3000	00:22:DD:80:18:6
vanced	0	192.168.166.87	EuroProt+	Végbemérés	ATO output	2.8.13	I>, Id, Z<	2.8.13.2080-rc3-5-gec29e8c6a/0.6	2.8.13.1560	00:22:DD:00:07:6
	0	192.168.28.105	EuroProt+	Égető FL Torony	Robotkutyi	2.8.13	I>, Id	2.8.13.2060-H2/0.6	2.8.13.1550	00:22:DD:00:06:68
out	0	192.168.0.155	EuroProt+	Egeto	ZoliTeszt - Robotkutya	2.8.13	I>, Id, Z<	2.8.13.2051-rc2-141-gaef38aa43/0.5	2.8.13.1540	00:22:DD:00:00:7
	0	192.168.21.62	EuroProt+	Unnamed station	Unnamed device	2.10.1	I>, Id	2.10.1.3000/0.13	2.10.1.3000	00:22:DD:80:18:7
ive Security Alarm 🖄 👘	0	192.168.0.43	EuroProt+	Állomás Állomás	vágány vágány	2.8.13	I>, Id, Z<	2.8.13.2081/0.6	2.8.13.1560-H5	00:22:DD:00:48:7
er: admin	0	192.168.230.220	EuroProt+	Protecta	Tápszekrény vezérlés	2.8.13	I>	2.8.13.2070/0.6	2.8.13.1560	00:22:DD:00:00:99
e: Full Access	0	192.168.28.95	EuroProt+	Égető FL Torony	DV7500 no.1 CPU1501	2.8.13	I>, Id, Z<	2.8.13.2080-rc1/0.6	2.8.13.1550-H2	00:22:DD:00:23:96
:27:10	0	192.168.80.10	EuroProt+	Protecta	E1-Line-H PRP	2.8.13	I>, Id, Z<	2.8.13.2050-H2/0.6	2.8.13.1530-H1	00:22:DD:00:24:A
ange Password	0	192.168.93.2	EuroProt+	Application	Gen Protection Test	2.8.13	I>, Id, Z<	.8.13.2080-H6-rc1/0.6	1008	00:22:DD:00:18:A
	0	192.168.19.5	EuroProt+	Feri bácsi mérőpadja	DRL - SelfCalibration	2.8.13	I>, Id, Z<	2.8.13.2080-H1/0.6	2.8.13.1560-H2	00:22:DD:00:38:B
	0	192.168.0.23	EuroProt+	Unnamed station	Unnamed device	2.8.13	I>, Id, Z<	2.8.13.2080-H5/0.7	2.8.13.1560-H5	00:22:DD:80:1A:B
S /	0	192.168.80.2	EuroProt+	Unnamed station	Unnamed device	2.10.2	I>, Id, Z<	2.10.2.3010-rc2/0.7	2.10.2.3010-rc4	00:22:DD:80:16:B
0	0	192.168.85.100	EuroProt+	Feilesztés - HW	SDRAM -7 és SRAM teszt	2.8.13	Busbar	2.8.13.2080-H1/0.7	2.8.13.1560-H5	00:22:DD:00:50:B
U U	0	192.168.80.40	EuroProt+	132kV GIS	E08 DGYD	2.8.13	Busbar	.8.13.2080-H1/0.6	1008	00:22:DD:00:3F:B5
	0	192.168.15.22	EuroProt+	Feilesztés	HB klima	2.8.13	I>, Id, Z<	2,8,13,2020/0,6	2.8.13.1530-rc10-428-g2e5b7491	00:22:DD:00:0A:B
	0	192.168.73.56	EuroProt+	Geri asztala	AdmLocTest	2.8.13	I>, Id, Z<	2.8.13.2080-H4/0.6	2.8.13.1560-H5	00:22:DD:00:04:C
	0	192.168.80.3	EuroProt+	TE	ACOS 351 AnaConf Teszt	2.10.2	Busbar	2.10.2.3010-H1-rc1/0.7	2.10.2.3010-rc4	00:22:DD:80:14:C
	0	192.168.80.1	EuroProt+	Unnamed station	Unnamed device	2.10.2	I>, Id, Z<	2.10.2.3010-rc1-dirty/0.7	2.10.2.3010-rc1	00:22:DD:80:14:C
	0	192.168.11.3	EuroProt+	Feilesztés	RTD	2.8.13	I>, Id, Z<	2.8.13.2070-H1/0.6	2.8.13.1560-H2	00:22:DD:00:01:D
	0	192.168.15.254	EuroProt+	Kiss F.	MSZ modell	2.8.13	I>	2.8.13.2064-rc3-149-q0a28ab903/0.6	2.8.13.1560-H5-rc1	00:22:DD:00:0F:DI
	0	192.168.22.64	EuroProt+	Unnamed station	Unnamed device	2.10.1	I>, Id	2.10.1.3000/0.13	2.10.1.3000	00:22:DD:80:15:E
	0	192,168,10,11	EuroProt+	Application	E2-Line	2.10.2	I>, Id, Z<	2.10.2.3010/0.7	2.10.2.3010	00:22:DD:80:0F:D
	0	192.168.16.64	EuroProt+	BNP	07VB-01	2.8.13	Busbar	.8.13.2070-H2/0.6	1008	00:22:DD:00:02:E9
	Ø	192.168.10.99	EuroProt+	Miko	MSZ modell	2.8.13	I>	2.8.13.2060-H2/0.6	2.8.13.1561-rc2	00:22:DD:00:49:FF
	0	192,168,80,81	EuroProt+	Feilesztés	CPU Faragó 3000	2.8.13	I>, Id, Z<	2.8.13.2070-H1/0.6	2.8.13.1560-H2	00:22:DD:00:08:F8
	Ö	192 168 18 144	FuroProt+	Unnamed station	Unnamed device	2813	IN	2 8 13 2080-H5/0 7	2 8 13 1550-H5	00-22-DD-80-19-FF

Figure 4-20 Network protectionHood

³² EuroProt+ Operating Manual with Troubleshooting Guide FW version 2.10 www.protecta.hu



4.2.9 Documentation

This panel displays the embedded and custom files uploaded to the built-in storage unit of the device. The **User documents** section allows the user to upload any type of documents and files, which will be saved on the device and will be accessible for later use. There is an 8 MB limit available, single file size maximum is 2 MB.

Embedded documents on the other hand, are uploaded by the manufacturer during equipment manufacture. The user cannot alter or delete them, but can read them.

Main	Documentation
Parameters System settings	EMBEDDED DOCUMENTS
Online data Events	Files not found
Disturbance recorder	User documents
Network protectionHood	Files not found File limit is 2048k per file. Available storage size is 8.0 MB.
Documentation	Upload
Advanced logout	
Active Security Alarm 🖄 User: admin Role: Full Access 04:06:53	
Change Password	PROTECTA
X	HUNGARY

Figure 4-21 User documentation

4.2.10 Security

The purpose of this menu is to allow the user to modify all security related settings in the device. A brief explanation of each menu item will be given in the subsections that follow.

4.2.10.1 Security settings

Secure handling – secure handling settings allow the user to manage between convenience and security of the device. Settings such as enabling/disabling the LCD confirmation dialogue upon loading of settings, enabling/disabling the operation of the device HMI interface from the web, enabling/disabling LCD mirroring can be found here.

System services – Use this field to set the web interface mode, enable secure file transfer mode, discover devices on the local network, set up remote login feature and log server.

Client whitelist – If this function is enabled, only the allowed clients can access the device in the selected role i.e. SCADA, Management, or both.

If an IP address is whitelisted for the SCADA role, this means that the IP address will only be allowed to access the device from SCADA only (i.e. IEC 61850, IEC 101/104, Modbus, etc.), access via web browser or EuroCAP is not permitted. Similarly, if an IP address is whitelisted for Management role, the IP address is only allowed access to the device from the web browser or EuroCAP, access via SCADA is not permitted. Whitelisting for both roles is also possible.



Main					Settings
Parameters					
System settings	Expand all	Collapse all	Print		
Online data					
Events	[+] SECURE HANDLIN	NG			
Disturbance recorder					
Commands					
Network protectionHood	[+] SYSTEM SERVICE	S			
Documentation					
Security	[.] C				
Security settings	[+] CLIENT WHITELI	ST			
User manager					
Certificate handling					
Alarms / Logging					
Audit trails				PRO	TECŤA
Advanced				HU	NGARY-
logout					
Set settings					
Active Security Alarm 🖄					
User: admin Role: Full Access 01:50:29					
Change Password					

Figure 4-22 Security settings menu

4.2.10.2 User manager

Not just any person can access the webpage functionality of the device. Users must be authenticated. Before the device is commissioned for use, a full user management setup is recommended to be completed. This menu is used for this purpose.

Users – Here, the names and roles of the personnel allowed to operate the device can be added, edited or deleted.

Roles – Here, the role rights management can be viewed. With a CyberProtect licence, the rights of the standard roles can be modified, while new roles can be added.

LDAP authentication, authorization – Apart from local IED device authentication, the device also allows for central server authentication. This menu is used to manage the settings of this type of authentication. This option is only available with a CyberProtect license.

Session handling – The settings related to the management of clients' sessions with the device can be managed here. These include parameters such as session timeout, maximum number of sessions, maximum number of users, etc. This is also recommended to be done before device commissioning.

Import / Export – If there are more than one EuroProt+ devices being managed by the same people, users in one device can also be authorized in the other. This menu allows for uploading an encrypted authentication file from another device. If this is done, the same users in one device can be found in the other.

NOTE: Initially, the user is allowed full access to the device through the "Guest" user. It's highly recommended that the "Guest" user rights be limited before the device is commissioned for use.

Additionally, the device is configured with an "admin" user with default password During the system security setup, it is also recommended that the "Admin" user be deleted or the password changed.

|--|--|--|--|--|--|--|--|

Main	User Manager
Parameters	
System settings	[+] Users
Online data	
Events	
Disturbance recorder	[+] ROLES
Commands	
Network protectionHood	[+] LDAP AUTHENTICATION, AUTHORIZATION
Documentation	
Security	
Security settings	[+] Session Handling
User manager	
Certificate handling	
Alarms / Logging	[+] IMPORT / EXPORT
Audit trails	
Advanced	
logout	PROTECTA
Active Security Alarm 🖄	НОИРУКА
User: admin Role: Full Access 11:41	
Change Password	

Figure 4-23 User manager menu

4.2.10.3 Certificate handling

In this menu, HTTPS and IEC 61850 security certificates can be uploaded. Please contact your system administrator for the proper settings.

HTTPS Certificate – This is an option for uploading a server's certificate, which has been signed by a publicly trusted certificate authority (CA). Therefore, the browser can accept that any identifying information included in the certificate has been validated by a trusted third party.

IEC 61850 TLS Configuration – The requisite parameters and certificates for securing IEC 61850 communication can be uploaded here.

Main			Certificate handling
Parameters			
System settings	[-] HTTPS CERTIFICATE		
Online data	PEM file		
Events	BEGIN PRIVATE KEY		A
Disturbance recorder	0f/8e0keZqmWudaXQSpTDzH5bH2f	2PolpF6Oci+kFIgYJdd09Yey1xuqq/3vHruc	-
Commands	GH7P2zRDyK6MgkmeoouZy8Y8r+Gb LXJpNzNECTKIWE31h+cfYPj8tkrO	xsnsBKwNiLOL6IwMt773NLMq6oUzitz8HMD1 4guMNsiBvDVyGolKDmQeMb1GWAZpDMnUUyDX	
Network protectionHood	OeYQwEizZly4CmxB2muSt384Fj4/ 4BoNzTkxQIk080b4lf58msN383PY	xJ0UqFP5U6YgI/p8sLE7QjRvTz2nvySIa7FC mof+1YoEz5kt63xGk2WDOizcrzy8SF9DP8Cj	
Documentation	r0ovh3GXAgMBAAECggEASZB9iAtW	oNey4EnU1t06MXwsOYYyaacuMtb6VxeCx4Vg	•
Security	Upload Certificate		
Cocurity cottings			
Uses menses			
User manager	[-] IECOIDSU TES CONFIGURA	TION	
Certificate handling	TIS Enabled	_	
Alarms / Logging			
Audit trails	Server Key Password:		
Advanced	Server Key (PEM format)	Upload	
logout	Server Certificate	Upload	
	Client Root Certificate	Upload	
Active Security Alarm 🖄	Client certificates	Add new client certificate	
User: admin Role: Full Access 04:21:31	Save Refresh Reload IEC	61850 Service	

Figure 4-24 Certificate handling menu



4.2.10.4 Alarms / Logging

This menu contains the settings for alarms generated by the device; and the settings for the level of system log events.

Entries – Alarms/alerts from device with all the relevant details e.g. facility, severity, time etc. are automatically logged here.

1ain									Alarms /	Logg
arameters										
	[-]	ENTRIES								
system settings										
Online data										
vents										
	Id	Facility	Severity	Time	User Se	ource	Destination	Activity	Details	Remove
isturbance recorder	738	User	Notice	2022-06-09 06:25:59			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
	739	User	Notice	2022-06-09 16:06:59			192.168.10.11	Startup	Device started	Dismiss
ommanos	740	Daemon	Notice	2022-06-09 16:07:17			192.168.10.11	Card	A card is missing or has a mismatch	Dismiss
etwork protectionHood	760	User	Notice	2022-06-09 16:19:58			192.168.10.11	Startup	Device started	Dismiss
	764	User	Notice	2022-06-09 16:23:22			192.168.10.11	Startup	Device started	Dismiss
ocumentation	778	User	Notice	2022-06-09 16:45:55			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
ecurity	784	User	Notice	2022-06-09 18:25:21			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
	786	User	Notice	2022-06-09 18:39:08			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
Security settings	789	User	Notice	2022-06-10 08:41:44 a	dmin 19	2.168.4.121	192.168.10.11	Options	Restart of RDSP is requested	Dismiss
	790	User	Notice	2022-06-10 08:43:27			192.168.10.11	Startup	Device started	Dismiss
Oser manager	796	User	Notice	2022-06-14 14:24:44			192.168.10.11	Startup	Device started	Dismiss
Certificate handling	797	User	Notice	2022-06-14 14:25:15			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
	799	User	Notice	2022-06-14 14:27:49			192.168.10.11	Time Sync	Time signal from ntp1 is out of tolerance (3 secs, max: 2 secs)	Dismiss
Alarms / Logging	803	Daemon	Notice	2022-06-14 15:22:21 a	dmin 19	2.168.1.1	192.168.10.11	Restore	User refused the restore	Dismiss
Audit trails	805	Daemon	Notice	2022-06-14 15:29:54 a	admin 19	2.168.1.1	192.168.10.11	Restore	Restore failed, this is not a backup file!	Dismiss
	812	User	Notice	2022-06-15 06:43:42			192.168.10.11	Startup	Device started	Dismiss
dvanced	856	User	Notice	2022-06-15 08:56:04			192.168.10.11	Startup	Device started	Dismiss
aout	862	User	Notice	2022-06-15 09:43:42			192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1	Dismiss
gour	874	User	Notice	2022-06-15 10:51:06			192,168,10,11	Startup	Device started	Dismiss
	878	User	Notice	2022-06-15 11:01:44			192.168.10.11	Startup	Device started	Dismiss
tive Security Alarm 🖄	891	User	Notice	2022-06-15 11:40:47			192,168,10,11	Startup	Device started	Dismiss
ser: admin	897	Daemon	Notice	2022-06-15 11:48:42 #	dmin 19	2.168.4.166	192,168,10,11	Epcs Upload	Epcs error: Unsupported config file version: 2.10.1. Supported version is: 2.10.2	Dismiss
ble: Full Access	900	User	Notice	2022-06-15 11:53:56			192,168,10,11	Startup	Device started	Dismiss
1.10.40	909	User	Notice	2022-06-15 12:08:45			192,168,10,11	Startup	Device started	Dismiss
aange Password	505						400 400 40 44	Charles P	Device stands	

Figure 4-25 A sample entries list

Syslog level settings – Alarm entry logs can be classified according to facility and severity. The facility defines the entity in the device which is responsible for the specific alarm. For example, a user is probably a client from a PC, a daemon is the device CPU itself, etc.

Main				Alarms / Loggin
Parameters				
System settings	[+] ENTRIES			
Online data				
Events				
	[-] SYSLOG LEVEL SETTI	NGS		
)isturbance recorder				
Commands				
Network protectionU.e.d				
Network protectionnood	Activity	Facility	Severity	Edit
Documentation	Login	Auth	Notice	Edit
	Logout	Auth	Notice	Edit
ecurity	Upload	Auth	Notice	Edit
Security settings	Settings	User	Notice	Edit
	Parameters	User	Notice	Edit
User manager	Options	User	Notice	Edit
Castificate bandling	User Manager	User	Notice	Edit
certificate handling	Role Manager	User	Notice	Edit
Alarms / Logging	Pfw Upload	Daemon	Notice	Edit
	Psp Upload	Daemon	Notice	Edit
Audit trails	Epcs Upload	Daemon	Notice	Edit
dvanced	Restore	Daemon	Notice	Edit
	Command	Daemon	Notice	Edit
gout	Download	Daemon	Notice	Edit
	Audit	User	Notice	Edit
ctive Security Alarm 🖄	Time Sync	User	Notice	Edit
sar: admin	Startup	User	Notice	Edit
ole: Full Access	Card	Daemon	Notice	Edit
1:17:19	IO Simulator	liser	Notice	Edit
		U.S.	Notice	E dit

Figure 4-26 Syslog level settings from the alarms / logging menu



4.2.10.5 Audit trails

An audit trail is a log of activities meant to log different entries that monitor the usage of the device. These activities are stored in a non-erasable database in the device.

lain								Audit Tra
arameters								
ystem settings	[-] E	NTRIES						
nline data								
vents	Id	Facility	Severity	Time User	Source	Destination	Activity	Details
isturbance recorder	1972	USEI	NOLICE	2025-03-01 11:99:99		192.100.10.11	time Sync	WIPI Sync restored with server 192.100.1.1
	1330	Auth	Notice	2022-09-01 11:33:53 admin	192.168.4.113	192.168.10.11	Login	success
ommands	1331	Auth	Notice	2022-09-01 11:34:03 admin	192.168.4.113	192.168.10.11	Upload	filename: 'E2-Line_F_polediscrepancy.epcs'
etwork protectionHood	1332	Daemon	Notice	2022-09-01 11:34:52 admin	192.168.4.113	192.168.10.11	Epcs Upload	Configuration updated successfully. Restarting device.
	1333	User	Notice	2022-09-01 11:36:33		192.168.10.11	Startup	Device started
ocumentation	1334	User	Notice	2022-09-01 11:37:07		192.168.10.11	Time Sync	NTP1 sync restored with server 192.168.1.1
curity	1335	Auth	Notice	2022-09-01 12:17:35 admin	192.168.4.113	192.168.10.11	Login	success
concy	1336	User	Notice	2022-09-01 12:17:56 admin	192.168.4.113	192.168.10.11	Parameters	Parameter change is initiated from Web, no confirmation required
Security settings	1337	User	Notice	2022-09-01 12:34:35 admin	192.168.4.113	192.168.10.11	Parameters	Parameter change is initiated from Web, no confirmation required
	1338	Auth	Notice	2022-09-01 16:32:37 admin	192.168.4.113	192.168.10.11	Logout	session timout
User manager	1339	User	Notice	2022-09-02 08:02:50		192.168.10.11	Startup	Device started
Certificate handling	1340	User	Notice	2022-09-02 08:03:17		192.168.10.11	Time Sync	NTP1 sync restored with server 192.168.1.1
	1341	User	Notice	2022-09-02 16:25:07		192.168.10.11	Time Sync	NTP1 sync lost with server 192.168.1.1
Alarms / Logging	1342	User	Notice	2022-09-02 16:28:39		192.168.10.11	Time Sync	NTP1 sync restored with server 192.168.1.1
Audit trails	1343	User	Notice	2022-09-05 06:25:46		192.168.10.11	Startup	Device started
	1344	User	Notice	2022-09-05 06:26:12		192.168.10.11	Time Sync	NTP1 sync restored with server 192.168.1.1
lvanced	1345	User	Notice	2022-09-05 14:18:41		192.168.10.11	Startup	Device started
aout	1346	User	Notice	2022-09-05 14:19:08		192.168.10.11	Time Sync	NTP1 sync restored with server 192.168.1.1
jour	1347	Auth	Notice	2022-09-05 16:17:34 admin	192.168.4.213	192.168.10.11	Login	success
	1348	Auth	Notice	2022-09-05 16:18:37 admin	192.168.4.213	192.168.10.11	Upload	filename: 'E2-Line_F_4chtest.epcs'
tive Security Alarm 🜁	1349	Daemon	Notice	2022-09-05 16:18:57 admin	192.168.4.213	192.168.10.11	Epcs Upload	Epcs error: Unsupported config file version: 2.10.1. Supported version is: 2.10.2
er: admin	1350	User	Notice	2022-09-05 16:34:54 admin	192.168.4.213	192.168.10.11	Parameters	Parameter change is initiated from Web, no confirmation required
le: Full Access	1351	User	Notice	2022-09-05 16:36:16 admin	192.168.4.213	192.168.10.11	Settings	System settings change is initiated from Web, no confirmation required
.30.02	1352	User	Notice	2022-09-05 16:38:13		192.168.10.11	Startup	Device started
ange Password	1353	User	Notice	2022-09-05 16:38:40		192 168 10 11	Time Sync	NTP1 sync restored with server 192 168 1 1

Figure 4-27 A sample audit trail entry list



NOTE: This is not a setting menu, but a reference point for auditors to assess whether the device is being used in the right manner.

4.2.11 Advanced

The advanced menu contains three items: Maintenance, I/O tester, and Update manager.

4.2.11.1 Maintenance

The following fields are found on the maintenance menu:

Ф Ф Ф Ф Ф Ф

In the **Cards** field (Figure 4-28), it is shown how the hardware of the device matches the hardware layout defined in its configuration (created in EuroCAP \rightarrow Rack Designer). In case of any mismatch, the device stops operating and goes to Error mode (Status LED turns red)

This field provides more detailed information about the hardware.

There are three rules for matching the configured and the actual hardware in the devices:

- **1.** These types of modules must match entirely:
 - **ATO+** modules (analogue outputs)
 - COM+ modules (communication modules for busbar and line diff. protections)
 - **CT+** modules (CT inputs)
 - INJ+ modules (for DRL arc suppression coil controller)
 - RAI+ modules (rotor earth fault injector/measurement)
 - **VT+** modules (VT inputs)
- **2.** For all other modules, those of the same type (see highlighted as **bold** below) can be interchanged. Here are some examples:
 - **O12+**/2201 ← → **O12+**/1101 (and all other **O12+** modules)
 - **CPU+**/1201 \leftarrow **> CPU+**/1501 (and all other **CPU+** modules)
 - PS+/4201 ← → PS+/2301 (and all other PS+ modules)
 - PSTP+/2101 ← → PSTP+/4201 (and all other PSTP+ modules)
- 3. Special cases that are not covered by the previous two rules:
 - HMI+ and HMIT+ modules (remote HMI) are also interchangeable
 - If a module can be equipped with different connector types (e.g. VT+/2211 and VT+/2211F and VT+/2211T), these also can be interchanged.

Main		Maintenance
Parameters		
System settings	Cards	
Online data	Slot Configured Detected Serial Nr. Status	
Events	V CPU+/1291 CPU+/1201 21125400 compatible T(1) CT+/5151 CT+/5151 13102503 matched	
Disturbance recorder	S(2) CT+/5151 CT+/5151 21104897 matched R(3) VT+/2211 VT+/2211 17118584 matched	
Commands	0(5) TRIP+/2201 TRIP+/2201 17119265 matched N(6) TRIP+/2201 TRIP+/2201 10025264 matched	
Network protectionHood	L(8) K8+700 K8+700 20125736 matched J(10) COM+/9901 COM+/9901 18117093 matched	
Documentation	A(19) PS+/2301 PS+/2301 11013695 matched	
Security	BUS BUS+/8401 passive bus	

Figure 4-28 Card info field

Device nameplate (Figure 4-29) contains product information and basic data of the device.





In **LOG files** field (Figure 4-30) internal information about the specific part of the device (RDSP, system, LCD, etc.) can be found.

LOG FILES				
System log files	RDSP log	System messages	Security log	
HMI log files	LCD log			
Communication log files	SPORT comm. log	Serial comm. log	IEC61850 log	PMU log

Figure 4-30 LOG files field

Serious errors (red status LED) and warnings (yellow status LED) are listed in the **Warnings** and Errors field (Figure 4-31). In the example below, time synchronization error is generated when time synchronizaton is lost with the timesync setting checkbox ticked from the **system settings**-> **Time synchronization** tab. For more information please refer to the <u>Troubleshooting guide</u>.

WARNINGS AND ERRORS			
CDSP warning: 0x0040 (Time s	synchronization,)		

Figure 4-31 Warnings and Errors

In case of any error, it is recommended to generate a system state report file (Figure 4-32) using the button in the **Backup / Report** field and send it to the <u>support team</u>. The file has .prf extension and includes various crucial device logs, current configuration, currently set parameters and other parameter sets, current system and security settings, and current licences. However, it does not include disturbance records. Oscillographic fault records can be downloaded as illustrated in paragraph 4.2.6.

Make sure to check the size of the downloaded .prf file: it should be above 10 kB. If it is below this, try to download it again with a different or an updated browser.



Communication files (Figure 4-33) for various protocols can be downloaded by clicking the appropriate button.

COMMUNICATION FILES		
Download IEC61850 files	Get .CID file	Get .ICD file
Download IEC60870-5-101/103/104 file	Get file in XML format	Get file in TEXT format
Download Modbus information file	Get Modbus file	
Download DNP3 configuration file	Get DNP3 file (html)	Get DNP3 file (csv)
Download SPA configuration file	Get SPA file (html)	Get SPA file (csv)
Export protection parameters	Export to XML format	
Export PMU header	Export to XML format	

Figure 4-33 Communication files

The status of the ports of the internal switch are displayed in the **Ethernet links** field (Figure 4-34).

ф ф ф ф ф

ETHERNET LINKS	
Primary station bus fiber optic port	Down
Redundant station bus fiber optic port (optional)	Down
RJ-45 port on rear side (optional)	Up
EOB/RJ-45 port on front panel	Down
Process bus fiber optic port (optional)	Down



The PRP/HSR Status and Test field appears on devices equipped with a PRP/HSR CPU module. The communication status and test mode are set here.

HSR module detailed status	Refresh	
Status: A: link:Up remoteFault:Nor B: link:Up remoteFault:Nor t A - Received Frames: 147216 t A - Sent Frames: 154014 t A - LAR CFror: 0 t A - LAN ID Error: 139297 t B - Received Frames: 151861		•
HSR test mode	Mode H	~



The memory info field (**Device housekeeping**) in Figure 4-36 provides information about the CDSP resources.

l system mem	ory	61856 kE	3	
e system mem	ory	24512 kE	3	
che memory		11956 kE	3	
Block size	Free block num.	Total free siz	ze	
8k	21	1		
64k	4	Ī		
128k	2			
256k	3			
512k	1			
1024k	2			
2048k	2			
4096k	2			
	1			

Figure 4-36 Memory info

The **Time synchronization** field (Figure 4-37) shows information about time synchronization supervision. In EP+ devices, time sychronization signal can be obtained from a variety of sources. Both GPS-based, ethernet-based, serial-based or a combination of any can be set. Depending on what hardware modules are available in the device, the following time synchronization protocols can be set: IRIG-B, PPS, PPM, Protecta Legacy, PTP, NTP, IEC101, IEC104, DNP3, MODBUS & ABB SPA.

If no external source is available and set, the time in the device can be synchronized manually from the PC time settings using the "set device" button.

TIME SYNCHRONIZATION	
From NTP1 source	Ok
From NTP2 source	Disabled
From legacy protocol	Disabled
From binary input (pinsync)	Disabled
Set device time	

Figure 4-37 Time synchronization info

4.2.11.2 I/O tester

The web page for advanced functions provides I/O simulation.

Ф Ф Ф Ф Ф Ф

Front panel LED test - by clicking on this button the front LEDs will be tested with a blink sequence.

Simulate binary inputs - by enabling this function user can simulate the inputs. For safety reasons, enabling this function must be confirmed on the LCD screen on the device. The LED symbol between the SET and RESET buttons shows the current state of the input: red if activated, green if inactive. Simulation mode can be disabled with the button on top of the input control buttons. While the simulator mode is active, the Status LED of the device is yellow.

CAUTION: The device is still fully functional in this mode, meaning that it can still generate trip signals!

SIMULATE BINARY INPUTS			
Input simulator mode	Disable		
CB off	Reset		Set
CB on	Reset		Set
Disconn. off	Reset		Set
Disconn. on	Reset		Set
BIn_C05	Reset		Set
BIn_C06	Reset		Set
BIn_C07	Reset		Set
BIn_C08	Reset		Set
BIn_C09	Reset		Set
BIn_C10	Reset		Set
BIn_C11	Reset		Set
BIn_C12	Reset		Set
TCS1	Reset		Set
TCS2	Reset	۲	Set

Figure 4-38 Input simulator mode

Direct control of the output contacts - prior to use this function the device should be switched to "Test/Blocked" mode in the **Commands** menu.

DIRECT CONTROL OF THE OUTPUT CONTACTS The device must be in Test/Blocked mode.

Ф Ф Ф Ф Ф Ф

Figure 4-39 Direct control of the output contacts (other modes)

In "Test/Blocked" device operation mode, all the functions of the device (i.e. protections, measurements, control functions etc.) are blocked from controlling the binary outputs. Once the mode is changed, the option to request direct control of the output contacts appears.

DIRECT CONTROL OF THE OUTPUT CONTACTS	
Start contacts testing	Request

Figure 4-40 Direct control of the output contacts (test/blocked mode)

Clicking on "Request" prompts a confirmation on the LCD screen. Upon confirmation, the output contacts can be controlled directly by the user. The LED symbol between the "Set" and "Reset" buttons shows the current state of the output: red if activated, green if inactive. To disable this function, change the Mode of the device to "On" state in the **Commands** menu.

DIRECT CONTROL OF THE OUTPUT CONTACTS		
Trip 1	Reset	 Set
Trip 2	Reset	Set
CB cmd on	Reset	Set
BOut_D02	Reset	Set
BOut_D03	Reset	Set
BOut_D04	Reset	Set
BOut_D05	Reset	Set
BOut_D06	Reset	Set
BOut_D07	Reset	Set
BOut_D08	Reset	Set

Figure 4-41 Output simulator mode



4.2.11.3 Update manager

The **Version info** field displays the EuroProt+ system version and the current firmware version in the device.



Figure 4-42 Version info window

In the **Restore** field the user can upload configuration and parameter settings from a system state report (.prf) file into the device.

[-] RESTORE			
Use this function to restore t	he device from backup file		
Upload PRF file			

Figure 4-43 Restore tab

Device firmware can be upgraded when a new version is available. This can be done from the **Firmware** tab. More detailed information about the current firmware is available in the text field (Figure 4-44).





To update, click on the "Update firmware" button, select the appropriate file and click OK. A dialog on the LCD will ask you to confirm updating. Detailed information about the latest firmware updates can be found on the Protecta website in the <u>release and revision history</u> (login required). If new firmware update is needed, please contact Protecta <u>support team</u>.

All digital outputs (relay contacts, trip contacts) must be disconnected from the protected object(s) before commencing firmware update.

.

CAUTION: Never load an older version of the firmware to the device! Firmware update must always be done with care, because mistakes in this process may cause devices malfunction. It is advisable to get the system state report of the device (.prf file) before commencing the update. This way the device can be restored in case anything goes wrong.

IMPORTANT: Before any firmware upgrade, the LCD will display a SHA-256 digest in form of a unique code. This code is used to verify whether the firmware file being uploaded is legitimate. The reference can be obtained from firmware release notes or by contacting the Protecta Application department. For a legitimate upgrade, the SHA-256 code displayed on the screen should match with the code provided in the release notes for the specific firmware. In Figure 4-45 below, 614b961a3b77 is the SHA-256 digest for firmware version 3010-H3.



ф ф ф ф ф

Figure 4-45 Firmware name and its SHA-256 digest for new firmware upon upgrade

In the **Configuration** field, the user can download the configuration file (.epcs) from the device. Here, a digitally signed configuration file (.epcs) can also be uploaded to the device, depending on the privileges of the user.

[-] CONFIGURATION		
File name: E4-Feeder_F Configuration type: E4 Configuration version: Customer ID: Last modified: 2022-12 Load date: 2022-12-16	_variant_sumCT.epcs -Feeder 5.1 -16 13:48 13:50:05	
Download EPCS file	Update EPCS file	

Figure 4-46 Configuration tab for a user with "manage configuration" rights



Once again, it is advisable to download the system state report (.prf) file before commencing a configuration update from a previously active device. This is again to ensure that in case of any malfunction due to a configuration update, the device can be restored.

The **Manufacturer Settings** tab can be used to view and manage the PSP file. A PSP (Protecta Settings Package) is a file provided by the manufacturer to the device owner, containing various licences and functionality level of the CPU.

The first PSP file is determined and loaded in the factory based on the ordering info of the device. If a future upgrade is required, the manufacturer may send another PSP file to the customer in due course, to cover for licence upgrades, feature software upgrades or functionality level upgrades.

NOTE: The PSP file cannot be downloaded, as it is device specific. Downloading implies that it can be uploaded to other devices, which should have their own PSP file from the manufacturer.

[-] MANUFACTURER SETTINGS	
CyberProtect license: disabled IEC61850 license: disabled Function level: I>, Id, Z< (2) PRP/HSR license: disabled	
Upload PSP file	

Figure 4-47 The "Manufacturer Settings" tab showing the enabled licenses & CPU functionality level from the current PSP file

5 Troubleshooting

This section helps the user to evaluate warnings and errors experienced during device operation. If further support is required, please contact Protecta through the <u>web support tool</u> with detailed error description and all the information described in paragraph 5.2.

5.1 Warning and Error Messages

Inappropriate or faulty conditions cause the device to give warning or error messages which can be seen in the **Advanced** -> **Maintenance** -> **Warnings and Errors** tab. In some cases, the warning/error message can also be seen on the local display of the device.

5.1.1 Warning messages in the web browser

In case of warnings the status LED would usually turn yellow. Any exceptions are shown in the table below. A warning sign (yellow triangle) also appears below the menu bar on the web interface. In this case, depending on the error, several functions can be paralysed. The possible messages are listed in the table below.

	System log files	RDSP log	System messages	Security log	
	HMI log files	LCD log			
	Communication log files	SPORT comm. log	Serial comm. log	IEC61850 log	PMU log
e: Full Access 08:19 inge Password	WARNINGS AND ERRORS Application warning: 0x0010 (Mo CDSP warning: 0x0040 (Time sy	ode not ON) nchronization)			

Figure 5-1 Warning messages in the web browser

The following tables summarize the warning messages.

WARNING MESSAGE (RDSP RUNTIME)	EXPLANATION
0x0001 (noPSAD)	PS modules with auxiliary voltage measurement do not transmit the measured value to the CPU properly. Suspected HW error.
0x0002 (vlanMismatch)	In line protection and binary signal exchange applications the VLAN settings are inconsistent. Consistency check recommended.
0x0004 extRtcCalibMode	CPU Real Time Clock accuracy is out of the tolerance range. Internal device clock won't work accurately, while the device is switched off. Suspected HW error.
0x0010 psVoltUnstab	The device internal power supply voltage (+/-12V) is unstable on the CT/VT module. Possible power supply or backplane failure.
0x0400 siliconRevMismatch	The RDSP firmware and the CPU chip hardware versions are different.
0x8000 adControlWarn	AD converter failure on an analogue input module. The faulty module can be determined from the RDSP log, which can be opened from the Advanced -> Maintenance -> LOG files tab. Suspected HW error.

Table 5-1 RDSP Runtime warning messages



Table 5-2 CDSP warning messages

WARNING MESSAGE (CDSP)	EXPLANATION
0x0001 (System)	System level warning (e.g.: Parallel DRL message version discrepancy)
0x0002 (Config)	Configuration inconsistency or structural problem. The system is still operating.
	Parameter problem, such as:
0x0004 (Param)	 during startup the device is unable to determine the number of parameter sets parallel DRL addressing warning (same master and slave address used)
0x0008 (LCD application)	System level warning, which is hampering LCD startup. It may happen when the device is building up communication between the RDSP and the CDSP via the high-speed bus application (sport).
0x0040 (Time synchronization)	Time synchronization warning. Check the Time synchronization settings in the System settings menu and verify the signal source.
0x0100 (RDSP comm. error)	RDSP communication problem. Software inconsistency or hardware error possible.



Table 5-3 Application warning messages

WARNING MESSAGE (APPLICATION)	EXPLANATION
0x0001 (diff3wVgroup)	The connection of the primary winding in primary- secondary and primary-tertiary relation is selected in contradiction (eg. Y and D) in the Transformer Differential protection function block. The function is disabled in this situation.
	This error typically occurs when a protection function works with two or more quantities that must be on the same secondary basis.
0x0002 (rangeMismatch)	Example: For <i>SumCT</i> function block, the IED needs to perform addition of currents coming from two or more CTs. If the secondary rating parameter of one current input module is set to 5A while the other is set to 1A, the IED generates this warning. Indicated with red LED.
0x0004 (nompeakMismatch)	Example: Summed currents used in certain function blocks are measured by different types of CT modules, for which the max. measured current is different (e.g.: CT+5151 module 50x In, CT+5101 module 4. channel 12,5x In).
0x0008 (frSourceMissing)	Frequency based function blocks are used in the configuration but no frequency source is configured.
0x0010 (modeNotOn)	The mode of device according to IEC 61850 is not "On". It can be switched to "On" in the Commands -> Common field.
0x0020 (userUKE)	The 'External Warning' binary status input signal of the Common function block is TRUE. This is defined by the user in the graphical logic editor. Possible reasons are status feedback failure, VT MCB failure, etc
0x0040 (mvDistVolt)	The 'Connection U1-3' parameter of the VT4 module function block is set to Ph-Ph while the 'Operation' parameter of any distance protection or directional overcurrent function block is not Off. These functions are disabled in this situation.
0x0080 (eventRecSize)	The number of the configured events channels has reached the limit.
0x0100 (simulatorMode)	Binary input simulator mode enabled.
0x0200 (wrongSysFrv)	The set 'Power system frequency' from System settings -> System parameters tab and the frequency of the measured voltage are different. 50Hz measured and 60Hz set or vice versa.
0x0400 (maxILoadHigh)	The 'Max.I_load' parameter of the Busbar differential protection is set higher than the "Base sensitivity" of the differential characteristics.
0x0800 (genParamError)	Other parameter mismatch. (E.g set value is out of range after a firmware upgrade). For more details see the RDSP log.



WARNING MESSAGE (APPLICATION)	EXPLANATION
0x00010000 (Analogue connection warning)	Either of the analogue inputs of a function block with graphical analogue inputs is not connected on the EuroCAP logic editor. To fix, make sure all the required analogue inputs of function blocks are connected.
0x00020000 (Analogue range parameter missing)	Parameter assignment to analogue inputs not complete in the configuration. Error can only be fixed by contacting <u>Protecta Support</u> .
0x00040000 (Analogue channel preprocessing not initialized)	Incorrect relay task execution order. Relay task execution order should be optimized in order to properly initialize functions with analogue inputs. Please contact Protecta Support to fix the problem.

5.1.2 Error messages in the web browser

Ф Ф Ф Ф Ф Ф

In case of errors the status LED turns red. If the web page is accessible, a red STOP sign can be seen below the menu bar. When an error occurs, the Fault Relay NO contact opens as well. The device is unable to operate in this state. The error messages inform the user about the hardware errors.

Advanced						
Maintenance	LOG FILES					
I/O tester	System log files	RDSP log	System messages	Security log		
Update manager	HMI log files	LCD log				
logout	Communication log files	SPORT comm. log	Serial comm. log	IEC61850 log	PMU log	
Active Security Alarm 🖄						
Jser: admin Role: Full Access 58:09	WARNINGS AND ERRORS					
hange Password	RDSP runtime error: 0x8040 (Si RDSP runtime warning: 0x8000	ngle AD module, AD control ch (AD control ch. warning)	. error)			
STOP	BACKUP / REPORT					
	Build and download system state is suitable to make backup from	e report. This function the device.	Get file			

Figure 5-2 Error message in the web browser

The following tables summarize the error messages.

Table	5-4	RDSP	Runtime	error	messages
IUNIC	U T	I DOI	I COLLEGE	GIIGI	messages

ERROR MESSAGE (RDSP RUNTIME)	EXPLANATION
0x0004 (moduleNotAvailable)	The CPU does not detect a module during operation. Suspected HW error.
0x0008 (flashError)	Suspected HW error.
0x0010 (pldSelfCheckFailed)	Connection failure between the RDSP and the backplane communication logic. Suspected HW error.
0x0020 (relayStoppedByFwConfigUpdate)	The device has not restarted automatically after a configuration or firmware download. Repeat the download procedure.
0x0040 (singleModuleADErr)	Double AD control failure: One analogue input module is affected, which can be determined from the RDSP log based on the card serial number.
0x0080 (multiModuleADErr)	Double AD control failure: Multiple analogue input modules are affected, which can be determined from the RDSP log based on the card serial numbers.
0x0100 (allModuleADErr)	All analogue input modules are failed. Suspected power supply module or backplane failure.
0x0800 (paramLoadingFailed)	After "Set parameters" command the RDSP dataflash content is invalid. Repeat parameter setting.
0x1000 (psSecondaryVoltFailed)	Power supply internal voltage (+/-15VDC, +12VDC or 3,3VDC) is out of the specified limits.
0x4000 (psVoltFailed)	Power supply module with auxiliary voltage monitoring function detects voltage out of the limits. Check the auxiliary voltage.
0x8000 (adControlErr)	There is an error occurred in one/some of the analog input modules (e.g.: CT, VT, AIC, RTD). Replacement of the faulty module required.



Table 5-5 RDSP Init error messages

ERROR MESSAGE (RDSP INIT)	EXPLANATION
0x0001 (hwPostError)	HW test during device start-up has detected a failure. See the RDSP log for more details.
0x0002 (configError)	Configuration download from the data flash was not successful. Reload the configuration.
0x0004 (paramError)	Parameter download from the data flash was not successful. Reload parameter set.
0x0008 (anaCorrFailed)	It was not successful to load all the analogue channel corrections from the analogue input module. Possible failure of the analogue module, CPU or backplane.
0x0010 (cardConfMismatch)	Mismatch between the detected and configured modules. More details can be found in Advanced -> Maintenance -> Cards tab.
0x0020 (failed2LoadVars)	Reloading the configuration will rectify the problem, if there is no HW error.
0x0080 (failedNonvolVarFormat)	Suspected HW error.
0x0200 (noValidPSCard)	Unable to detect Power Supply module. Possible failure of the power supply module, CPU or backplane.
0x0800 (fwConfMismatch)	RDSP firmware does not fulfill the configuration version requirement. Certain function blocks used in the configuration are not implemented in the RDSP firmware, therefore a firmware update is recommended.
0x1000 (noClearForcedModeStat)	For R&D purposes only.
0x2000 (funcLevelMismatch)	The function level of the CPU is lower than that of the downloaded configuration file. Configuration file or CPU module level modification shall be executed by Protecta staff.



Table 5-6 CDSP error messages

ERROR MESSAGE (CDSP)	EXPLANATION
0x0001 (System)	Critical system error. Corrupted file or hardware error possible. The system cannot operate reliably.
0x0002 (Config)	Critical configuration error, inconsistency or internal structural problem. The system cannot operate reliably.
0x0004 (Param)	Critical parameter error or data inconsistency on the CDSP or RDSP.
0x0020 (TCP communication)	TCP communication system error. Hardware or other system error possible.
0x0080 (File I/O)	File system error. The device cannot generate the RDSP log.
0x0100 (RDSP comm. error)	RDSP communication problem. Software inconsistency or hardware error possible.

ERROR MESSAGE (HW INIT) EXPLANATION 0x0004 (FRAMError) FRAM failure indicating CPU HW error. Real Time Clock reset generator failure 0x0008 (extRTCError) indicating CPU HW error. SRAM test failed at power up indicating CPU 0x0010 (sramError) HW error. Flash IC no. 13 failed on the CPU module 0x0020 (codeFlashError) indicating CPU HW error. Flash IC no. 14 failed on the CPU module 0x0040 (dataFlashError) indicating CPU HW error. SDRAM test failed indicating CPU HW error. 0x0080 (sdramError) 0x0100 (xilinxInitError) CPU HW error caused by the Xilinx. If the IED started with power supply off/on switching, it tries to write a control data string in 0x1000 (pldSRAMMagicStrFillFailed) the SDRAM. If this operation fails, the error message appears indicating the CPU HW error. Self-check function detected a failure. 0x2000 (pldSelfCheckFailed) Suspected CPU HW error.

Table 5-7 Hardware Init error messages



ф ф ф ф ф ф

If there is a fault while uploading a configuration to the device or updating the firmware, the device enters the emergency mode, which also means that it is unable to operate. The following error messages may appear on the LCD screen if an unsuitable firmware has been loaded to the device (e.g. lower than the minimum required by the configuration).



Figure 5-3 Error messages on the LCD screen

If this happens, the web page of the device will be different (see Figure 5-4), but the system state report file can still be downloaded by using the *Get report file* button on it. This file is important for troubleshooting for the Protecta Support team, as it contains all necessary information about the device (configuration file, all the logfiles, parameters, settings, licences, etc.).

In these cases please contact Protecta Support on the web-based support system.



The screenshot below shows the device in emergency mode with all the log files and the system state report download button.

In the **Log and Report files** tab, the user can download the system state report from the device. Other types of log files can also be downloaded by clicking on the respective link within the tab.

The primary way of restoring a device from emergency mode is by uploading a backup or system state report file (.prf) from the last known working state of the device. This is done from the **Restore device** tab.

NOTE: It is highly likely that a .prf file downloaded from a device in emergency mode cannot restore a device. This is why it is recommended that before any upgrade, a system state report file should be downloaded. This way, if the device enters emergency mode, a .prf file from a working system can be uploaded.

Other ways of restoring a device may involve uploading a firmware (.pfw), configuration (.epcs) or manufacturer settings (.psp) file. This is done from **Firmware update** tab.

Prior to entering emergency mode, if the device had role-based access control activated, restoration will require authentication from the <u>Authenticate with user and password</u> tab. See Figure 5-4 below.

← → C ▲ Not secure 192.168.80.4						07	Ê	☆		G :
Ooops!										
The device is in emer	gency mode									
Something bad happened with this o	device. Possible reaso	ns could be uns	supported o	configuration or	wrong firmwa	are ver	sion.	You	can st	udy the
We are sorry for the inconvenience.		,								
- Authonticato with usor a	nd paceword									
Authenticate with user a	nu passworu									
Give user and password here if a	uthentication is requir	ed.	I	Login						
0361	1 4330014			Login						
— LOG and Report files —										
Build and download system state <u>U-boot messages</u> <u>System messages</u> <u>Relay log</u> <u>SPORT log</u> <u>LCD log</u> <u>Serial log</u> <u>IEC61850 log</u> <u>PMU log</u> <u>Httpd error log</u> <u>Additional info</u> <u>Overall info</u>	a report.	Get report file								
Restore device	ri Chasa	a Eila Na fila ab			Destere					
Restore the device from backup	file Critos		losen		Restore					
Firmware update										
Firmware update	Choos	e File No file ch	iosen		Update					
EPCS Upload	Choos	e File No file ch	iosen		Upload					
PSP Upload	Choos	e File No file ch	iosen		Upload					
. rocess Log										

Figure 5-4 Web page of a device in emergency mode



A de-energized fault relay indicates an error in the following three scenarios:

- The device is switched off or it is starting up (while the Status LED is red)
- Errors (red Status LED)

▋¢**▋**Φ**┃**Φ **□**Φ**┃**Φ**┃**Φ

The ExtWarning input of the Common function block is active (user-defined warning)

In any other case (normal operation, or other, non-user-defined warnings that cause a yellow status LED), the fault relay is energized.

5.2 Necessary data before contacting Protecta Support

Sending the system state report file is the preferred method in order to provide all important information to the support team. If the file cannot be downloaded for some reasons, the data below have to be provided when contacting us, so the device can be identified quickly:

- Serial No. of the device
- Firmware version
- Configuration name and date

5.2.1 Serial Number of the Device

The device serial number can be found on the Device Nameplate which is located on the upper right side of the device, close to the backplane.



Figure 5-5 The device name plate

There are cases when the physical Nameplate cannot be accessed because of the location of the device. In these cases, connect to the IED on its Service Port, and open its web page. Here the serial number can be found on the virtual nameplate located in the **Advanced -> Maintenance -** > **Device nameplate** tab.

PLATFORM:	IED-EP+
TYPE:	DTIVA
CONFIG:	E2-DTI_F
ORD.CODE:	B4401301101-B120000000100401-4D
U aux PS:	90-300VDC,80-255VAC
In, Un:	200/100V
U aux BI:	220V
SERIAL No:	140739
Firmware ver.	: 2.8 Made in Hungary

Figure 5-6 The device virtual nameplate

5.2.2 Information about firmware and configuration versions

The firmware and configuration versions can be shown on the second page of the device home screen, which can be accessed by touching the info icon.



Figure 5-7 Firmware (Revision) and configuration information on the LCD

If the local screen cannot be accessed, the web page can also be used to obtain the Version info from Advanced -> Update manager menu.

Main	Update
Parameters	
System settings	VERSION INFO
Online data	System version: 2.10
Events	FW Revision: 2.10.2.3010
Disturbance recorder	
Commands	[-] Restore
Network protectionHood	
Documentation	Use this function to restore the device from backup file
Security	Upload PRF file
Advanced	
Maintenance	[-] FIRNWARE
I/O tester	
Update manager	[epp] A System version: 2.10
logout	FW Revision: 2.10.2.3010 SHA-256: 31226da0d00f
Active Security Alarm M	[linux boot]
User: admin	Version: U-Boot 2013.07 sd128-git2500 (Jan 15 2021 - 16:21:45) SHA-256:
Role: Full Access 41:48	Active firmware: 'B'
Change Password	[linux] 5H2-256: 882ar5#407#5
	EuroProt+ system version: 2.10.2 kernal – linux release 3.10.108.enn huild #2 Eri Aug 10.13:30:18 UTC 2022
X	toolchain: /bfin-uclinux-gcc release gcc version 4.3.5 (ADI-2013R1-RC1)
0 G.	Skip HMI confirmation:
	Update firmware
	[-] CONFIGURATION
	File name: E2-Line_F_polediscrepancy.epcs Configuration type: E2-Line_F Configuration version: 1.1 Customer ID: Functional test Last modified: 2022-09-01 11:28 Load date: 2022-09-01 11:34:44
	Skip HMI confirmation:
	Download EPCS file Update EPCS file

Figure 5-8 Firmware and configuration information on the web



The table below contains the typical faults and errors that may occur during commissioning or operating the device with possible reasons and solutions. If necessary, please contact the <u>Protecta Support Team</u>:

STATUS LED	LCD DISPLAY STATUS	FRONT PANEL BUTTONS	POSSIBLE FAULT	SUGGESTION
Dark	Dark	Do not react on touch.	 a. No supply voltage. b. Supply voltage is out of range. c. Power supply module failure 	Check the supply voltage and the LED on the power supply module.
Green	Dark	Do not react on touch.	a. LCD display failure b. In cases of CDSP version lower than 2.8.13.912 it is possible that the LCD screen froze.	In case of reason b., a CDSP firmware upgrade will fix the issue.
Green	Works but the time shown is wrong.	Working.	No time synchronization signal is received (or it is not received regularly enough). This way the time can go out of sync.	Use the Set device time button on the web page located in the Advanced-> Maintenance menu. This will set the time in the computer operating system to the device.
Yellow	Working.	Working.	There is an external time synchronization device connected and the "Timesync warning" parameter is set in the system parameters menu, but no synchronization signal is received. In this case on the web page in the Advanced - > Maintenance -> Warnings and Errors tab, a warning message can be seen (0x0040 Time sync warning)	Check the settings and connections of the time synchronization device

Table 5-8	Typica	l errors
-----------	--------	----------



STATUS LED	LCD DISPLAY STATUS	FRONT PANEL BUTTONS	POSSIBLE FAULT	SUGGESTION
Yellow	Working.	Working.	In the user logic there is a signal connected to the "ExtWarning" input of the Common function block, and this signal is TRUE. This will also be indicated by the Failure Relay and on the web page in the Advanced-> Maintenance -> Warnings and Errors tab, a warning message can be seen (0x0020 User warning)	Check the configuration of the device using the EuroCAP tool. Look for the Common function block in the graphic editor and see what kind of signal is connected to the ExtWarning input. The most common signals may be switchgear status signal errors or VT fuse errors etc.
Red	Working	Do not react on touch	a. a HW module is faulty b. the actual HW configuration is different than the one defined in the configuration	See if there are any issues with the HW modules. These can be checked on the web page in the Advanced -> Maintenance -> Cards tab. Contact Protecta personnel using the web-based support system.