

ControlPlex[®] Rack User Manual

RCI10 Remote Control Interface



Date of issue:

Date of publication: March / 2020

This document replaces the following documents:

Anwenderhandbuch B_19BGTCP_d_010320

Editor:

E-T-A Elektrotechnische Apparate GmbH

Industriestraße 2-8 . 90518 Altdorf

GERMANY

Tel. 09187 10-0 . Fax 09187 10-397

E-Mail: info@e-t-a.de . www.e-t-a.de

Copyright © 2020 E-T-A GmbH

The contents of this document is the property of E-T-A GmbH. No part of this publication must in any way be reproduced or distributed without prior written consent of E-T-A GmbH. Any person acting illegally with regard to this publication can be prosecuted.

Limitation of liability

Although all provisions were taken when creating this document, the editor does not accept any responsibility for errors or omissions or for damages caused by using the information contained in this document. The information contained in this document may be revised at any time without pre-advise.

Brands

All references to software and hardware in this document are generally protected by brands or patents.

© E-T-A GmbH 2020. All rights reserved

About this manual

This manual describes the configuration for start-up and the operation of the integral SSH, web browser and SNMP interfaces by means of a control and configuration PC connected to the **Remote Control Interface RCI10**. The RCI10 sub-assembly provides ease of monitoring and remote control of the **ControlPlex® Rack** system in connection with a control computer or a management system. Typical application is mainly the control and monitoring of decentralised telecommunication systems.

Besides this document, more information about the E-T-A **ControlPlex® Rack** can be found in the following documents.

ControlPlex® Rack

Data sheet

Here you will find more technical data and figures as well as approval information on the various components of the **ControlPlex® Rack** system

ControlPlex® Rack

Installation Instruction

Here you will find the instructions for installation and start-up of the hardware of the **ControlPlex® Rack** system as well as helpful information for component replacement and troubleshooting on site.

ControlPlex® Rack

Release Notes RCI10_SW_VX.X

Here you find the information of the extended performance features of the current software for the **RCI10** sub-assembly.

ControlPlex® Rack

Application examples EAI300

Here you find further configuration and connection examples for the **EAI300** module

The latest documents can be found on our website under:
www.e-t-a.de/controlplex_rack

All documents contain important instructions for connection and safe operation of the **ControlPlex® Rack** system. Safety instructions have to be observed. All users have to be informed about all safety instructions. The documents have to be accessible for the user.

Contents

| | |
|---|-----------|
| About this manual | 3 |
| Contents | 4 |
| General information | 6 |
| 1 Introduction | 7 |
| 2 Minimum requirements for start-up of the RCI10 sub-assembly | 8 |
| 3 Important information and safety instructions | 9 |
| 4 Schematic system design and network connection | 10 |
| 5 General: RCI10 Start-up with web browser surface | 11 |
| 5.1 Start-up: Useful information on the web browser surface | 11 |
| 5.2 Start-up: IP settings on the configuration PC | 11 |
| 5.3 Start-up: Status and installation of the hardware. | 12 |
| 5.4 Start-up: Starting the web browser surface | 12 |
| 5.5 Start-up: Configuration by means of web browser surface | 13 |
| 6 General: RCI10 Start-up with the SSH v2 surface | 15 |
| 6.1 SSH tools: Installation SSHv2 Client programme LePutty [®] | 15 |
| 6.2 SSH tools: Installation SSHv2 Client programme LePutty [®] | 15 |
| 6.3 Start-up: Configuration via SSH surface | 16 |
| 6.4 Start-up: Table of SSH configuration parameters and factory settings | 17 |
| 6.5 Start-up: RCI10 configuration file download | 22 |
| 6.6 Start-up: RCI10 configuration by means of configuration file upload | 23 |
| 7 General: RCI10 Additional functions SSH surface | 24 |
| 7.1 Operation with SSH surface: Display RCI10 inventory data | 24 |
| 7.2 Operation with SSH surface: Download of log data and measuring data file | 25 |
| 7.3 Operation with SSH surface: Reset to factory settings | 25 |
| 7.4 Operation with SSH surface: RCI10 software update / upgrade | 26 |

| | | |
|-----------|---|-----------|
| 8 | General: RCI10 operation with web browser | 27 |
| 8.1 | Operation with web browser: Function of the mask »Fuse Control« | 27 |
| 8.2 | Parallel connection of several ESX300-S | 29 |
| 8.3 | Operation with web browser: Function of the mask »External Alarms« | 30 |
| 8.4 | Operation with web browser: Function of the mask »Feed Settings« | 31 |
| 8.5 | Operation with web browser: Function of the mask »Fuse Settings« | 32 |
| 8.6 | Operation with web browser: Function of the mask »External Alarm- Labels« | 34 |
| 8.7 | Operation with web browser: Function of the mask »External alarms – functions« | 35 |
| 8.8 | Operation with web browser: Function of the mask »System Log« | 37 |
| 8.9 | Operation with web browser: Function of the mask »Error Log« | 38 |
| 8.10 | Operation with web browser: Function of the mask »Fuse Log« | 39 |
| 9 | General: RCI10 operation with management system | 40 |
| 9.1 | Operation with management system: Settings in the RCI10 sub-assembly | 40 |
| 9.2 | Operation with management system: Embed SNMP MIB | 41 |
| 9.3 | LDAP authentication | 42 |
| 10 | Appendix List of pictures | 46 |
| 11 | Appendix List of abbreviations | 47 |
| 12 | Appendix Legal references and licences | 48 |
| 13 | Appendix Template of configuration table | 49 |
| 14 | Appendix Example RCI10 configuration file (excerpt) | 54 |

General Information

Qualified personnel

The system must only be installed, connected and configured in connection with this document. Installation and operation of the device/system must only be carried out by qualified personnel. With regard to the safety instructions of this documentation, qualified persons are persons authorised to operate devices, systems and circuits according to the standards and rules of safety engineering.



Safety instructions

Please follow the installation and configuration instructions given in this document carefully. Failure to comply may lead to serious damages of the product or the system. E-T-A does not accept any liability for problems caused by improper installation or handling by the customer or a third person.

Symbols

You will find the following symbols in the entire manual. Their meaning is as follows:



Danger!

You are in a situation which might cause injury. Before working with one of the devices you have to be aware of the risks of electrical circuitries and you ought to be familiar with standard procedures of accident prevention.



Warning

There is a risk in this situation to do something which might cause damage of the devices or data loss.



Note

Here you receive information which might be particularly useful for the application.



Disposal guidelines

Packaging can be recycled and should generally be brought to re-use.

1 Introduction

You chose **ControlPlex® Rack**, a comprehensive, future-oriented protection system which combines safety, user convenience and service friendliness. It is a power distribution, measurement and control system which provides electronic and, in the event of a short circuit, current-limiting protection of various loads. By means of an internal bus system and an additional, hot-pluggable control interface module (optional), each load can remotely be controlled and monitored. In addition it allows recording of measuring data of every single load. Besides providing overcurrent and short circuit protection, it increases system availability by a multiple, because it disconnects faulty loads quickly, selectively and without voltage dips.

In connection with the RCI10 control interface module the **ControlPlex® Rack** system can be connected to a centralised management system (control computer). For this purpose an Ethernet interface is made available with SNMP v1, v2c or v3 protocol. The required private MIB for embedding is part of the delivery scope. An additional possibility for a centralised or also local monitoring/control is provided by the integral web server, which can be used without additional software on the control computer by means of the web browser. In addition great importance was attached to system security, against illegal access. Therefore the configuration of the RCI10 sub-assembly is effected via a secure Secure Shell (SSH) surface. It also offers a great number of configuration options to increase system security.

Thanks to its system properties the **ControlPlex® Rack** is the perfect solution for smart protection, control and energy measurement for DC-supplied minus switching system cabinets.

Further descriptions of the **ControlPlex® Rack** systems - mounting and connection procedures for the hardware as well as an instruction for start-up and trouble-shooting of the individual components can be found in the manual **ControlPlex® Rack** (www.e-t-a.de/produkte/intelligente_stromverteilung/controlplex/controlplex_rack/).

This document contains a configuration and operation instruction for the software of the RCI10 Remote Control Interface sub-assembly . You will learn more about

- how to configure the RCI10 sub-assembly via the SSH surface for the first operation and how to adjust it to your requirements;
- how to use the integral web surface for monitoring and controlling the **ControlPlex® Rack** system;
- how to embed the **ControlPlex® Rack** system into a management system.

2 Minimum requirements for start-up of the RCI10 sub-assembly

Please check if the components of the **ControlPlex® Rack** system were completely installed and work faultlessly, see document »**ControlPlex® Rack** Installation and operation instructions«. You require the following tools for configuration and start-up:

- PC with Ethernet interface (LAN) and operating system Windows 7.x or higher
Pre-installed internet browser such as IE from v9 or Mozilla Firefox from v28.8, please also see data sheet **ControlPlex® Rackk**.
- Ethernet cable 10 / 100 Mbit (standard network cable) in the required length.

3 Important information and safety instructions

The following table lists various information and safety instructions for start-up and use of the device.

| | |
|---|---|
|  | <p>DANGER: INSTALLATION AND OPERATION OF THE DEVICE This device has to be installed and operated in compliance with the given instructions. Failure to comply can lead to injury, damage of loads or of the ControlPlex® Rack system.</p> |
|  | <p>DANGER: TURN OFF THE SUPPLY VOLTAGE Before beginning with installation, the system has to be disconnected from the mains. A cable connection must only be established if the supply voltage is OFF.</p> |
|  | <p>DANGER: POSSIBLE IGNITION HAZARD The device must NOT be used in inflammable surroundings.</p> |
|  | <p>DANGER: HIGH VOLTAGE The cover must NEVER be opened. Access to the inner components is not allowed unless indicated otherwise in this manual.</p> |
|  | <p>CAUTION: WORK WITH ESD PROTECTION Electronic modules must only be touched and installed with ESD protection so as to ensure protection against electrostatic voltage. Failure to comply can cause damages on the ControlPlex® Rack system or the corresponding components.</p> |
|  | <p>WARNING: GROUNDING The device must be grounded before switching on.</p> |

Table 1: Important information

EMC installation directives

The **ControlPlex® Rack** hardware and accessories comply with the EMC directives. Thus electromagnetic interferences between the devices are avoided which would otherwise affect the system performance. A professional installation is mandatory. In order to ensure the best EMC conditions, the widest possible distance between the different electrical devices should be applied.

Technical Accuracy

All technical data in this manual were correct in all conscience at the time of printing. E-T-A cannot be held liable for any (inadvertent) errors. Due to continuous product improvements at E-T-A there could be discrepancies between the actual product and the manual. Product changes or amendments of the technical specifications will be carried out without prior notification. The latest versions of the **ControlPlex® Rack** documents are available on our website www.e-t-a.de.

4 Schematic system design and network connection

Schematic diagram of entire system

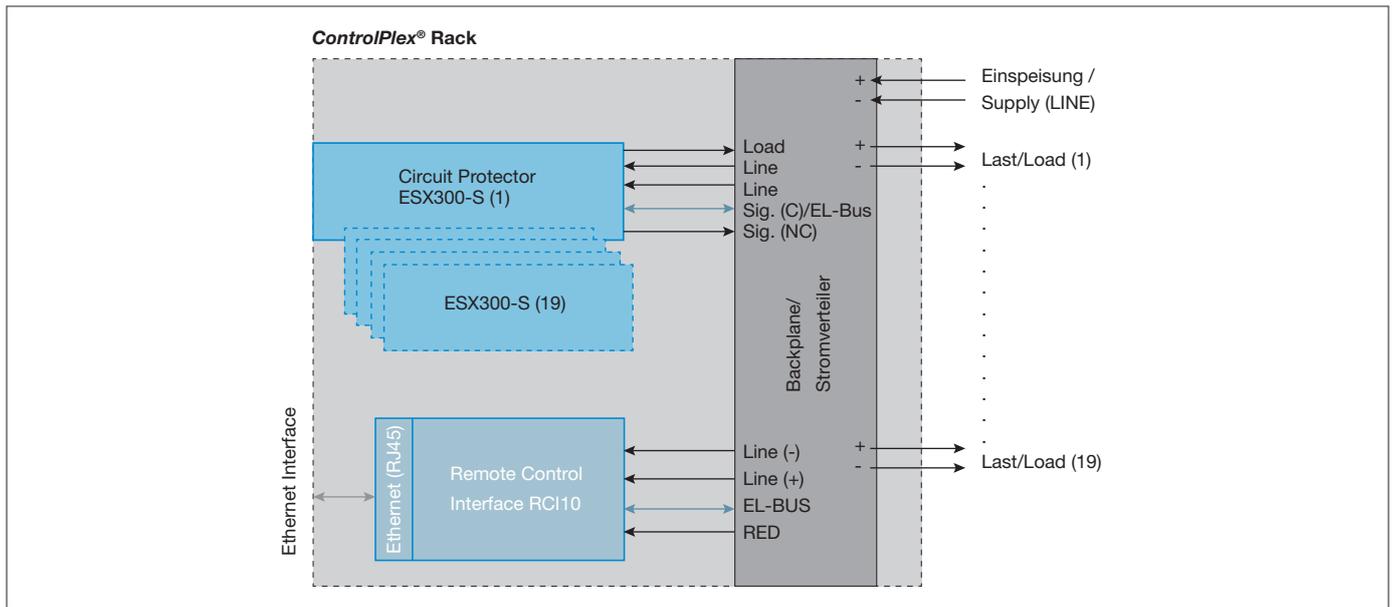


fig. 1: Schematic diagram ControlPlex® Rack

Connection example

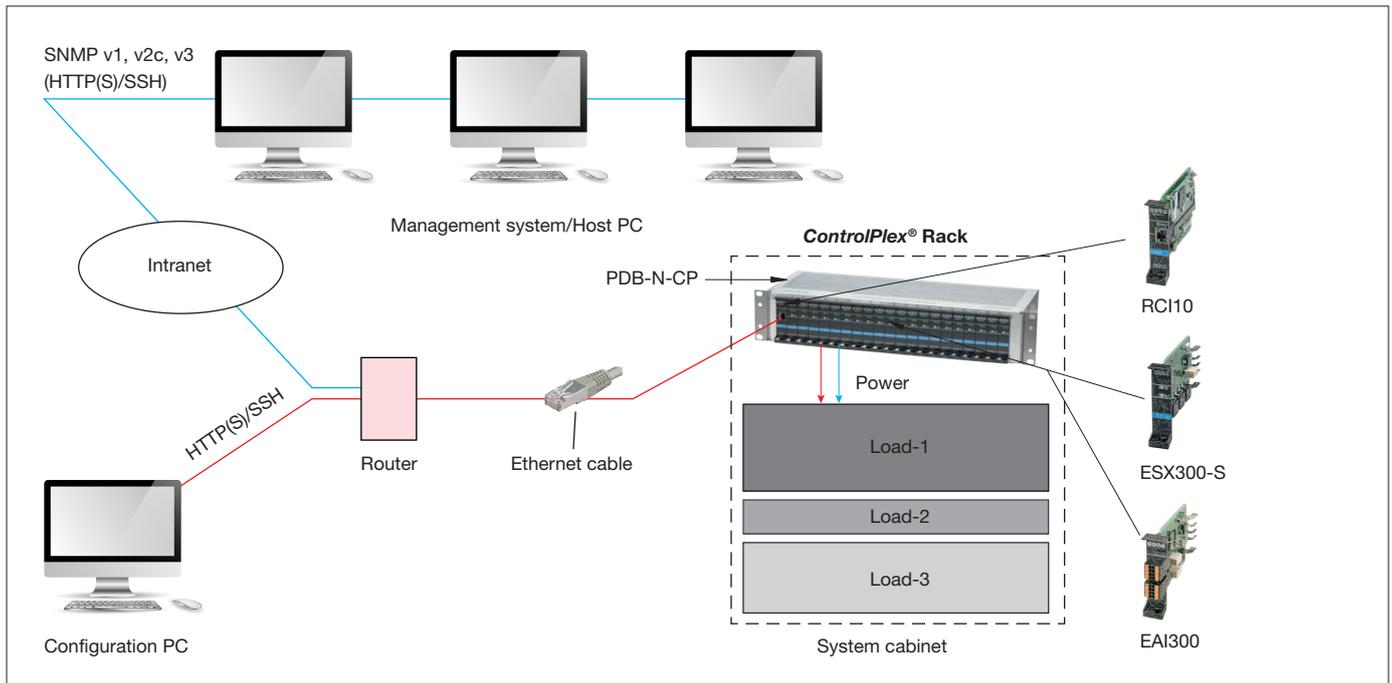


fig. 2: Connection example ControlPlex® Rack

5 General: RCI10 Start-up with web browser surface

The web server included in the RCI10 sub-assembly offers an easy and convenient option of adjusting the RCI10 sub-assembly and the **ControlPlex® Rack** system to your requirements during start-up. An extended configuration (for enhanced security settings of various protocols) can be carried out via the SSH surface. If you do not want to use the web browser surface, you may skip this chapter. Continue with chapter 6 General: RCI10 Start-up with the SSH v2 surface

The web browser surface provides the following adjustment options for network and start-up configuration:

- IP address data
- Web browser: log-on data
- System time
- Settings of the **ControlPlex® Rack** system - specific system designations
- Setting the system language of the web browser surface

5.1 Start-up: Useful information on the web browser surface

For using the web server function you only need a web browser on your PC. We tested the following browsers with regard to correction function and display:

- Internet Explorer Version 9
- Mozilla Firefox Version 28.8.1
- Google Chrome Version 26.0

You are of course free to use other web browsers or versions of the above listed browsers. However, in such a case we cannot ensure that all charts of the web browser surface will be shown correctly.

5.2 Start-up: IP settings on the configuration PC

Before starting configuration, you have to check the IPv4 Ethernet settings on the configuration PC and amend them if required. For this purpose connect your PC with a LAN (Ethernet) cable to the RJ45 connector of the RCI10 sub-assembly.

The IPv4 Ethernet address of your configuration PC has be the following: **192.168.0.xxx**

Information: xxx = 1 ... 24, 26 ... 254 (the address 192.168.0.25 is occupied by RCI10, factory settings).

Example: Set an IPv4 address at the configuration PC, e.g. IPv4 = 192.168.0.20

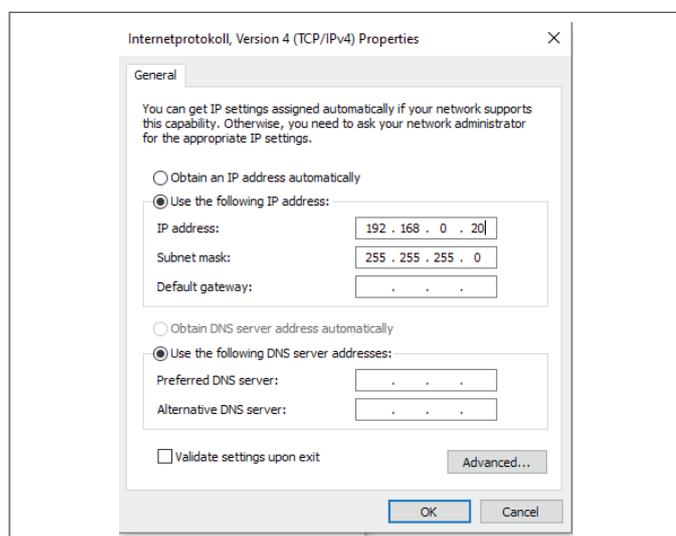


fig. 3: IPv4 setting of configuration PC

5.3 Start-up: Status and installation of the hardware.

The ControlPlex® Rack system with the components ESX300-S circuit protector and RCI10 Remote Control Interface, optionally the EAI300 External Alarm Interface, was installed correctly as described in the »ControlPlex® Rack« Installation Instruction«.

The LED status is as follows:

- RCI10 status LED: shows green
- ESX300-S fault LED(s): OFF
- ESX300-S OK LED(s): blink slowly or show green
- EAI300 status LED: (optional) shows green or green/cyan blue blinking

Your PC is connected with a LAN (Ethernet) cable to the RJ45 connector of the RCI10 sub-assembly. The PC and RCI10 sub-assembly can also be interconnected via a network, e.g. router. For this purpose please ensure that the RCI10 IPv4 factory pre-set address has not yet been assigned otherwise in your local network. For a list of all factory settings please see table 2, SSH configuration parameter list and factory settings.

5.4 Start-up: Starting the web browser surface

- Open a web browser window on your configuration PC e.g. with: InternetExplorer or Mozilla FireFox etc.
- Enter the URL: https://192.168.0.25 in the address line and confirm with the **Return** button
- Should a warning message appear such as " Problem with the safety certificate", please confirm with **continue** or **continue loading** of the indicated page.
- Enter user name and password. The factory pre-set user name is **user**, password: **user1234**. Confirm with **OK**



fig. 4: Web browser log-on IE

- The web browser surface opens with the tab: **Fuses (fuse control** of the RCI10 sub-assembly. Depending on the version of the **ControlPlex® Rack** systems, the appearance may slightly differ, depending on whether you installed a redundant system or not.

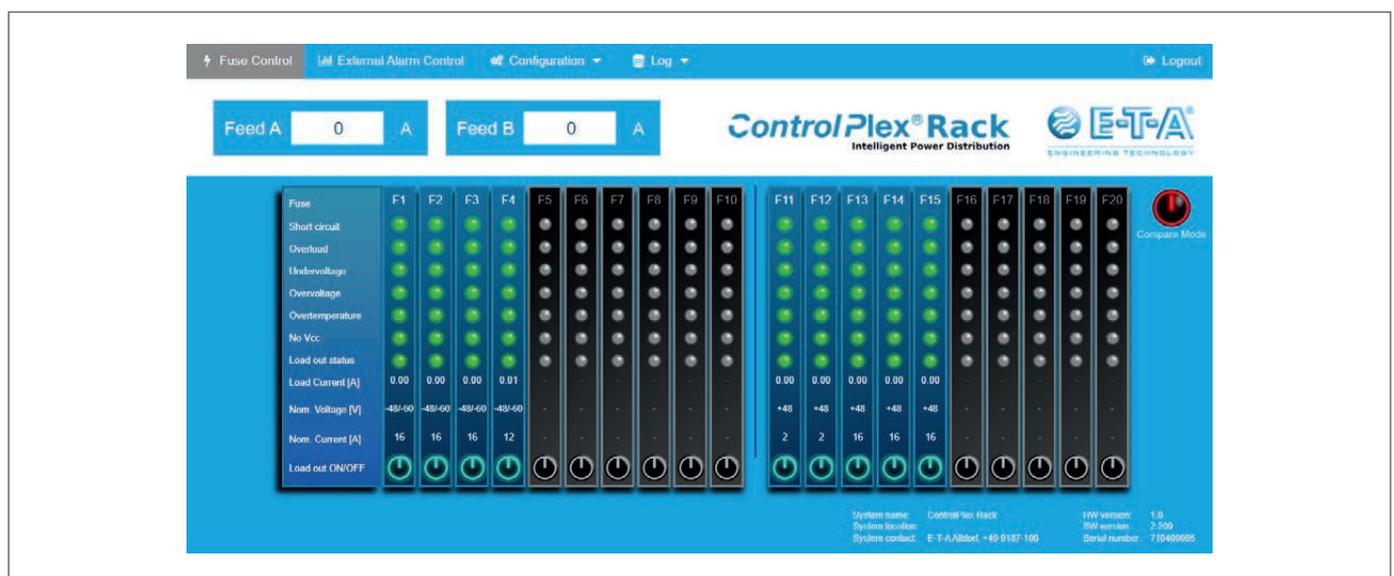


fig. 5: Web mask »fuses«

- Click on the tab **Configuration** on the left side of the surface. The configuration window **System Settings** opens.

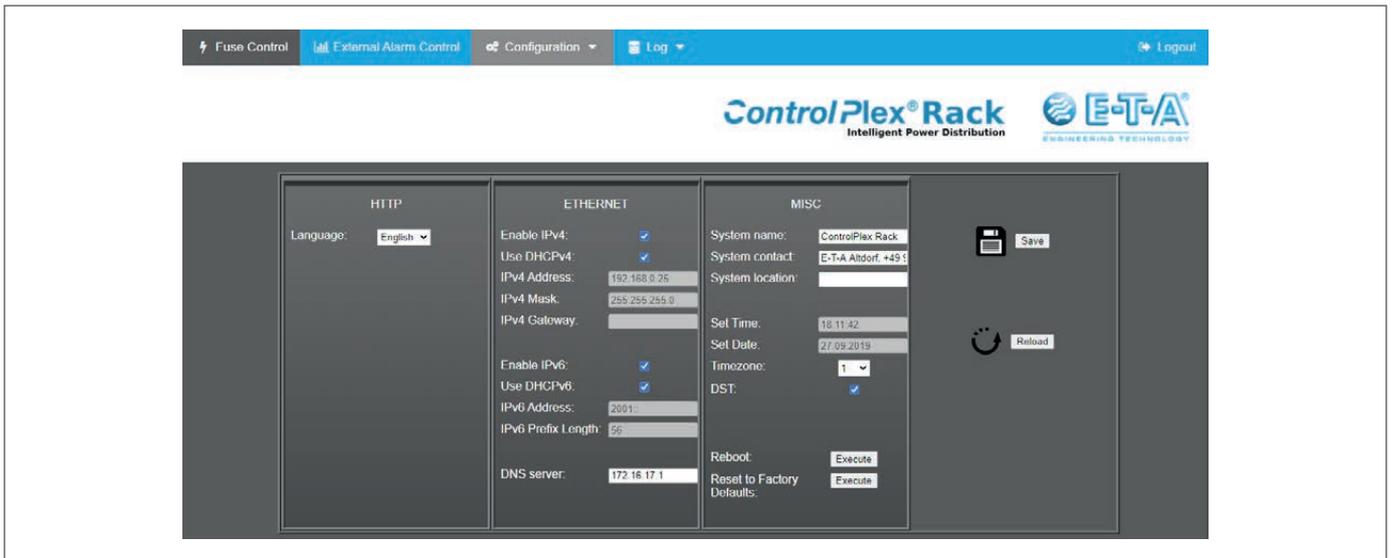


fig. 6: Web mask »Configuration / System settings«

5.5 Start-up: Configuration by means of web browser surface

The web browser configuration window shows the presently active factory settings. The tab **Configuration** contains three tabs (**System Settings**, **Feed Settings**, **Fuse Settings**). This chapter describes the setting options of the **System Settings**



Please observe that after the internal factory pre-set configuration or the configuration carried out by you via the SSHv2 interface, some functions may not be available.



Please make a note of all configuration changes with the newly entered values.

Overview of user rights (LDAP/internal)

1. **Admin user:** No restrictions
2. **Read/write users:** Unable to save system settings. (Error message: no authorisation).
3. **Read-only users:** Unable to switch outputs, unable to open or close relay contacts.
Unable to save system settings. (Error message: no authorisation).
Unable to save/delete feed settings (Error message: no authorisation).
Unable to delete back-up settings (Error message: no authorisation).

Please carry out the following adjustments in the category **HTTP**:

- Change the user name under **Login**
- Change the password under **Password**



The password is not shown (asterisks). No password is set in the event of no entry.

- Change the display language if required under **Language**. You can choose between the languages German and English.



In case of a password change in the HTTP area (web interface), a reboot has to be executed afterwards, so that an SSH login (for admins) with the new PW is possible.

In the category **ETHERNET** you can e.g. adjust the **IPv4** address settings. In addition you can

- activate the DHCP protocol (Dynamic Host Configuration Protocol) in your local network. For this purpose please select the check box **Use DHCP**.



After activation of the changed settings the DHCP protocol will automatically assign a new IPv4 address to the RCI10 sub-assembly. Please take down this address if you wish to connect your configuration PC with the system again later (without network). You then have to enter **https://<new IPv4 address>** as URL into the address bar of the web browser. <new IPv4 address> = the above noted address



Should you deactivate the check box **Enable v4**, no IPv4 address will be considered valid any longer, i.e. you do no longer have access to the RCI10 sub-assembly via IPv4. You will then always have to indicate an IPv6 address.

- If your network does not support an IPv6, we recommend to deactivate the check box **Enable v6**.
- If a DNS server (Domain Name Server) is available in your network, please enter the DNS URL under **DNS Server** .

In the category **MISC** you can

- enter a name for the **ControlPlex® Rack** system (**System name**)
- indicate a contact person (**System contact**)
- indicate an installation site (**System location**).
- In addition you can determine the time zone (**Timezone: 1** = CE winter time, **2**= CE summer time) and changeover summertime/wintertime(**DST**).



Date and clock time cannot be set because the factory settings include an NTP server (time server, network time protocol). The RCI10 sub-assembly will automatically get the valid time information from the NTP server. It may, however, happen that the NTP server cannot be reached by your local network, see chapter: 6.4 Start-up: Table of SSH configuration parameters and factory settings

- Click on **SAVE** to save the changed values. If you do not save, all changes will be lost.
- Click on the button REBOOT: **EXECUTE** to activate all changes, confirm with **OK**. The RCI10 sub-assembly carries out a reset with a re-load of the changed parameters. Re-booting may take up to 60 seconds. During this time you do not have a connection to the RCI10 sub-assembly.



The reset will **not** affect the plugged in circuit protectors ESX300-S, i.e. your connected loads remain active during the RCI10 re-start.

- Re-load the page in your web browser after approx. 60 seconds. Click on the Reload function of the web browser. Now all carried out changes should be activated and visible.

6 General: RCI10 Start-up with the SSH v2 surface

Secure Shell or **SSH** is the name of a network protocol and of corresponding programmes. For the purpose of a safe, encrypted connection between the configuration PC and RCI10 sub-assembly, also via an unsafe network, the SSH surface can be used both for a comprehensive configuration of all parameters and for upload and download of data such as measuring and log data. The SSH surface offers you the full scope of configuration options of the RCI10 sub-assembly. This particularly relevant for higher requirements of system safety. For a list of all factory settings please see table 2, SSH configuration parameter list and factory settings.

6.1 SSH tools: Installation SSHv2 Client programme ¹LePutty®

In order to be able to establish a safe SSH v2 connection, you require a terminal programme called SSH Client. The SSH Client programme has to be installed on the PC used for configuration. We recommend the freeware programme ¹LePutty®, which is available for download on our website www.e-t-a.de/controlplex_rack. The configuration of the SSH Client mentioned below exclusively refers to this version.

- After downloading the compressed file »CP-RCIxx_SSH-Client_Vxx.zip« into a suitable directory on the hard disk drive of your configuration PC.
- Among the unpacked files there is a file named E-T-A_Readme.txt, holding all information required for installation. Please follow the instructions given in this file.

6.2 SSH tools: Configuration of SSHv2 Client programme ¹LePutty®

To allow use of the full functional scope of ¹LePutty®, you have to configure the programme as follows::

1. Start the programme by clicking on the programme icon ¹Putty®. Carry out the steps 1 to 3 on right side of fig. 7; IP configuration ¹LePutty®.

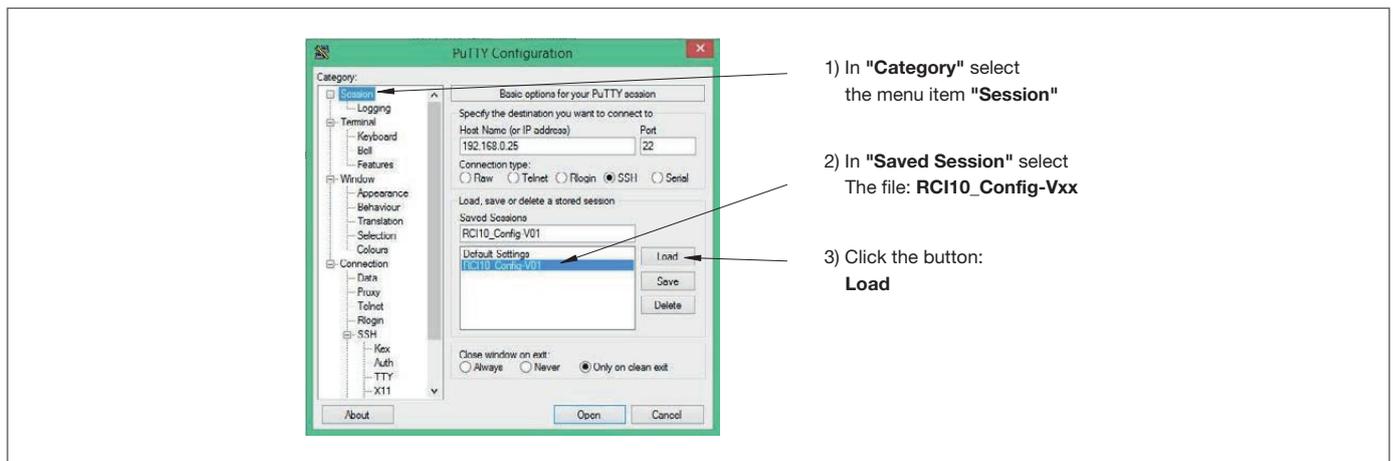


fig. 7: IP configuration ¹LePutty®

¹⁾ see chapter 12: Legal references and licences

2. Configure the ZModem settings, see fig. 8 bottom. Carry out the steps 1 to 5 beside the picture left and right.

1) In "Category:", select the menu item "ZModem".

2) Click the **Browse** button. It opens a browser window. Navigate and select the file **rz** saved in chapter 6.1 and click **open up**

3) Click the **Browse** button. It opens a browser window. Navigate and select the file **sz** saved in chapter 6.1 and click **open up**

4) Click the **Browse** button. It opens a browser window. Select the DIR in the the ControlPlex measurement and configuration data want to save.

5) Enter in the "Options" Fields the values **-e -v** on

fig. 8: ZModem configuration LePuTTY

- Mark the menu item **Sessions** in »Category«, see fig. 7, IP configuration ¹LePutty® above.
- Click the button **Save** to save the carried out ZModem settings in the configuration file **RCI10_Config-Vxx**.

6.3 Start-up: Configuration via SSH surface

Before starting configuration, you have to check the IPv4 settings on the configuration PC and amend them if required, see chapter 5.2 Start-up: IP settings on the configuration PC

1. Start the programme ¹LePutty® and load the saved configuration file **RCI10_Config_Vxx** as described in chapter 6.2 para 1.
2. Click on the button **Open** in the ¹LePutty® window. The programme now builds up a connection to the RCI10 sub-assembly and opens an SSH window.
3. Authenticate with User: **user** and password: **user1234** (factory settings). You now see the SSH configuration menu.



The »cursor« buttons (↑↓) allow navigation in the menu, menu items can be selected with the »enter« button. Parameters can be changed by the »+/-« buttons (e.g. Yes/No) or adjusted by direct entry of the value (e.g. name). The »F1« button helps to leave a submenu and also to close the SSH connection in the top menu.

fig. 9: SSH main menu

4. A list of all SSH configuration parameters with a short description can be found in chapter 6.4. below

 Please make a note of all configuration changes with the newly entered values. For this purpose you can print the table inserted in chapter 13 and enter the values manually.

 After changing the configuration settings you have to select the menu option »**Reboot RCI10**« in the SSH menu to activate the changes. Re-boot can also be effected by pressing the reset button of the RCI10 sub-assembly for 3 seconds on site. Re-boot is visually indicated by the green LED going out. Repeated access of the RCI10 is possible approx. 60 seconds after initiation of the re-boot.

 The RCI10 will **not** affect the plugged in circuit protectors ESX300-S in the system nor the optionally inserted EAI300 alarm sub-assemblies , i.e. your connected loads remain active during the RCI10 re-start.

 If you changed the IP address of the R sub-assembly, you are no longer able to open the RCI10 SSH surface. For this purpose you have to enter the changed RCI10 IP address also in the ¹LePutty© programme, see ¹LePutty© window, fig. 7, IP configuration¹LePutty© »Host Name (or IP address)«. Save the change with button »**Save**« in the ¹LePutty© window.

6.4 Start-up: Table of SSH configuration parameters and factory settings

Description of all available SSH configuration parameters including the factory setting when delivered.

 Please observe that after the internal factory pre-set configuration or the configuration carried out by you via the SSHv2 interface, some functions may not be available.

| HTTP settings Setting parameters | description | Factory settings |
|---|---|------------------|
| HTTP enable | Activation web server Allow access via web browser. Possible values {Yes; No}. | Yes |
| Access only using HTTPS | Web browser access only via HTTPS protocol possible (encrypted transmission). Possible values {Yes; No}. | Yes |
| Allow settings write | Parts of the configuration settings such as http/login, IP address etc. can be changed directly via the web browser. Possible values {Yes; No}. | Yes |
| Allow fuse switch via HTTP | Determines if the circuit protectors may be switched ON or OFF via the web browser surface. Possible values {Yes; No}. | Yes |
| HTTP access is: password protected | Web browser access only possible with user ID and password (http and https). Possible values {Yes; No}. | Yes |
| HTTP log-on | Defines the user name (user ID) for the web browser access Permitted characters: 20 characters [a-z; 0-9; _-]. | user |
| HTTP password | Defines the password for the web browser access Please observe upper and lower case. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#- _.:;<> ~] | user1234 |
| HTTP language | Defines the language for the web browser surface. Possible values {english; german}. | german |

¹⁾ see chapter 12: Legal references and licences

| SNMP settings Setting parameters | Description | Factory settings |
|-------------------------------------|--|-------------------------------------|
| SNMP enable | Activation of SNMP access. In OFF condition no SNMP commands will be accepted by a management system. Possible values {Yes; No}. | Yes |
| SNMP protocol | Determination of the permitted SNMP protocol. The RCI10 supports SNMP v1, v2, v3. Data are transmitted encrypted only with v3. Possible values {v1; v2; v3}. | v3 |
| Enable traps | Permit the sending of SNMP traps. If in the ON condition, alarm message can immediately be reported without a query from the superordinate system / management system. Possible values {Yes; No}. | Yes |
| Trap target | The IP address or the host name of the system to which the SNMP traps (alarm or status indication) shall be sent. When entering more than one address, they have to be separated by a semicolon. | |
| Allow fuse switch | Determines if the circuit protectors may be switched ON or OFF via the SNMP protocol. Possible values {Yes; No}. | Yes |
| Allow settings write | Parts of the configuration settings such as snmp/login, IP address etc. can be changed directly via SNMP (management system). Possible values {Yes; No}. | Yes |
| SNMP community string | SNMP »community string« of the RCI10 sub-assembly. If the protocol version SNMPv1 or SNMPv2c is used, the management system has to know the string indicated here. The value entered here is valid for the parameters »read« and »write«. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<>] | private |
| SNMP login | Defines the user name (user ID) for the web browser access Permitted characters: 20 characters [a-z; 0-9; _-]. | user |
| SNMP password | Defines the password for an SNMP v3 connection. Please observe upper and lower case. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<>] | user1234 |
| SNMP authentication | SNMPv3 authentication method. Possible values {MD5; SHA} | MD5 |
| SNMP encryption method | SNMPv3 encryption method. Possible values {AES; off; DES} | AES |
| SNMP encryption key | SNMPv3 key used for data encryption. Permitted characters: 500 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<>] | ControlPlex® Rack-ESX300 |
| NTP settings Setting parameters | Description | Factory settings |
| NTP enable | Activate NTP Client (automatic time synchronisation via external server). Possible values {Yes; No}. | Yes |
| Server | IP address or URL of the NTP server from where the time information shall be obtained. Permitted characters: 100 characters [a-z; A-Z; 0-9; _-]. | ptbtime1.ptb.de |
| Time zone | Adjust time zone (time difference between local time and UTC). Possible values {-12..-1; 0; 1..12}. Example: 1 = Central European Time (CET), 2 = Central European Summer Time (CEST) | 1 |
| DST | Calculate with summer time and winter time Possible values {Yes; No}. | Yes |
| LDAP settings Setting parameters | Description | Factory settings |
| LDAP Enable Value | Defines the users: Internal user = NO, user of LDAP server = YES | NO |

| | | |
|---|---|----------------------------|
| LDAP SSL Value | Encryption options: SSL encryption = on, encryption via TLS connection =startTls, no encryption = off | on |
| Server Value | Host name or IP address of LDAP server | |
| Port Value | LDAP port | 389 |
| Base DN Value | Entry point (DN) for user search | Dc=base, dc=com |
| Login attribute mapping Value | Value of attribute is the user name used | uid |
| Password attribute mapping value | Value of attribute is the user name used | userPassword |
| User object class value | Determines the object class of the user | posixAccount |
| Uid number attribute mapping value | Determines which value of the attribute shall be used as uid number (min. 4-digit number) | uidNumber |
| Additional filter value | User-defined filter (optional) | |
| Group member attribute mapping value | The value of the attribute "isMemberOf" is the DN of the group where the user is 8is used for authorisation) | isMemberOf |
| Admin group value | DN of admin group | Cn=admin, dc=base, dc=com |
| User (read write) group value | DN of the read-write group | Cn=userrw, dc=base, dc=com |
| User (read write) group value | DN of the read-only group | Cn=userrr, dc=base, dc=com |
| Ethernet settings Setting parameters | Description | Factory settings |
| Enable IPv4 | Activation of the IPv4 address range for addressing the RCI10 sub-assembly.  Should you set this value to »No«, the RCI10 can no longer be addressed via IPv4. Possible values {Yes; No}. | Yes |
| Use DHCP for IPv4 | Activate DHCP or IPv4 If activated, an IPv4 address is automatically assigned via the connected network. Possible values {Yes; No}. | No |
| IP address | IPv4 address, RCI10 sub-assembly. Example format {xxx.xxx.xxx.xxx} | 192.168.0.25 |
| Network mask | IPv4 network mask, RCI10 sub-assembly example format {xxx.xxx.xxx.xxx} | 255.255.255.0 |
| Gateway | IPv4 gateway of the current network segment example format {xxx.xxx.xxx.xxx} | |
| DNS server IPv4/IPv6 | IPv4 address of the »Domaine Name Server« (DNS). Example format {xxx.xxx.xxx.xxx} | |
| Enable IPv6 | Activation of the IPv6 address range for addressing the RCI10 sub-assembly. Possible values {Yes; No}. | Yes |
| Use DHCP for IPv6 | Activate DHCP or IPv6 If activated, an IPv6 address is automatically assigned via the connected network. Possible values {Yes; No}. | Yes |
| IP address | IPv6 address, control interface RCI10 Example format {2001:db8:1:2:3C5:811::1} | |
| Network prefix length | Enter the IPv6 length of the network prefix Possible values: 3 characters [0-9]. | 56 |
| DNS server IPv4/IPv6 | IPv6 address of the »Domaine Name Server« (DNS). Example format {2001:db8:1:2:3C5:811::1} | |

| RCI10 settings Setting parameters | Description | Factory settings |
|--|--|---|
| Fuse log periodicity | Period duration in seconds, with which measuring values of each ESX300-S circuit protector will be written into the log file, e.g.: load current, voltage and temperature values. Possible values {off, 30 ... 600}. | 30 |
| Allow reset to factory defaults | Option to reset all setting parameters listed in this table to the factory settings. When entering »No« the menu option »Reset to factory default« will disappear. Possible values {Yes; No}. | Yes |
| System name | Freely selectable system name. Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> \`'] | ControlPlex Rack |
| System contact | Freely selectable system contact name (e.g. person to contact on site). Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> \`'] | E-T-A Altdorf, +49 9187-100 |
| System location | Freely selectable system location. Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> \`'] | |
| Time / Date settings Setting parameters | Description | Factory settings |
| time | Enter present time, if no NTP server (see NTP settings) was indicated or is available. The parameter »NTP enable« has to be set to »no« for that. Format {hh.mm.ss} | |
| Date | Enter present date, if no NTP server (see NTP settings) was indicated or is available. The parameter »NTP enable« has to be set to »no« for that. Format {DD.MM.YYYY} | |
| Time zone | Adjust time zone (time difference between local time and UTC). Possible values {-12..-1; 0; 1..12}. Example: 1 = Central European Time (GET), 2 = Central European Summer Time (CEST) | 1 |
| DST | Calculate with summer time and winter time Possible values {Yes; No}. | Yes |
| Fuse Labels Setting parameters | Description | Factory settings |
| Label for fuse 1...20 | Freely selectable system name for the circuit protector ESX300-S in the slot. A1...A20 (A1 – A10 and B1 – B10). Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> \`'] | F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, F13, F14, F15, F16, F17, F18, F19, F20 |

E/A Alarm Interface sub-assembly type EAI300

| EAI300 settings selection menu | Setting parameters | Description (for these parameters you require the RCI10 SW 2.0 or higher) | Factory settings |
|-----------------------------------|--------------------|--|------------------|
| EAI300 Slot 1. | Label for output 1 | Freely selectable alarm denomination for the EAI300 sub-assembly in slot A1 – alarm output 1. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> \`'] | EAI1Out1 |
| | Label for output 2 | Alarm denomination for EAI300 in slot A1 – alarm output 2 | EAI1Out2 |
| | Label for input 1 | Alarm denomination for EAI300 in slot A1 – digital input 1 | EAI1In1 |
| | Label for input 2 | Alarm denomination for EAI300 in slot A1 – digital input 2 | EAI1In2 |
| | Label for input 3 | Alarm denomination for EAI300 in slot A1 – digital input 3 | EAI1In3 |

| | | | |
|--|-------------------------------|---|------------------------------|
| | Label for input 4 | Alarm denomination for EAI300 in slot A1 – digital input 4 | EAI1In4 |
| | Label for input 5 | Alarm denomination for EAI300 in slot A1 – digital input 5 | EAI1In5 |
| | Label for input 6 | Alarm denomination for EAI300 in slot A1 – digital input 6 | EAI1In6 |
| | Label for input 7 | Alarm denomination for EAI300 in slot A1 – digital input 7 | EAI1In7 |
| | Label for input 8 | Alarm denomination for EAI300 in slot A1 – digital input 8 | EAI1In8 |
| | Label for analog input | Alarm denomination for EAI300 in slot A1 – analog input 1 | EAI1AnalogIn |
| | Logic function for output 1 | <p>Set up a logic link for EAI300 – slot A1 - alarm output 1</p> <p>Function: »AND«, »OR«, »NOT« link of e.g. status conditions of the circuit protectors and/or inputs of EAI300 sub-assemblies</p> <p><u>Syntax: Link EAI300 inputs</u> EAI<slot no><input no> <slot no> = 1 ... 20 <input no> = 1 ... 8 Example: eai19in1</p> <p><u>Syntax: Logical links</u> AND = * OR = + NOT = ! Example: eai19in1*eai18in1</p> <p><u>Syntax: Linking ESX300 status</u> ESX<slot no.><status> <slot no.> = 1 ... 20 <status> = out (load output); sho (short circuit); ol (overload); uv (undervoltage); ov (overvoltage); tem (excess temperature); nv (no voltage) Example: esx1sho</p> | |
| | Logic function for output 2 | Set up a logic link for EAI300 in slot A1 - alarm output 2 | |
| | Signalling group for output 1 | <p>Set up a group or single signalling function of the circuit protectors for EAI300 in slot A1 – alarm output 1.</p> <p>0 = no alarm signal for ESX300 status 1 = alarm signal for ESX300 status Example: 11111111110000000000</p> <p>Group signal for all circuit protectors in slots 1 to 10</p> | 00000000000000000000 |
| | Signalling group for output 2 | Set up a group or single signalling function of the circuit protectors for EAI300 in slot A1 – alarm output 2 | 00000000000000000000 |
| EAI300-Slot 2 ... EAI300-Slot 20 | | <p>Parameters, see description EAI300-Slot1.</p> <p>Here you can configure the parameters for additionally fitted EAI300 sub-assemblies in slots A2 ... A20 or for redundant Power-D-Box types in slots A2...A10 and B1...B10. The slot numbers depend on the Power-D-Box type.</p> | EAI2...1 ... EAI20...8 |

Table 2: SSH configuration parameter list and factory settings

6.5 Start-up: RCI10 configuration file download

In order to save the changed configuration settings locally on the configuration PC, navigate in the SSH menu with the »Cursor« buttons (↑) to menu item **Export all settings** and push **Enter**.



Please ensure that no file with the file name »exportSettings.ini« exists on the configuration PC in the path selected in chapter 6.2, para-2, step-4, because in the event of access authorisation problems it might cause the abortion of the download.

1. A submenu opens.

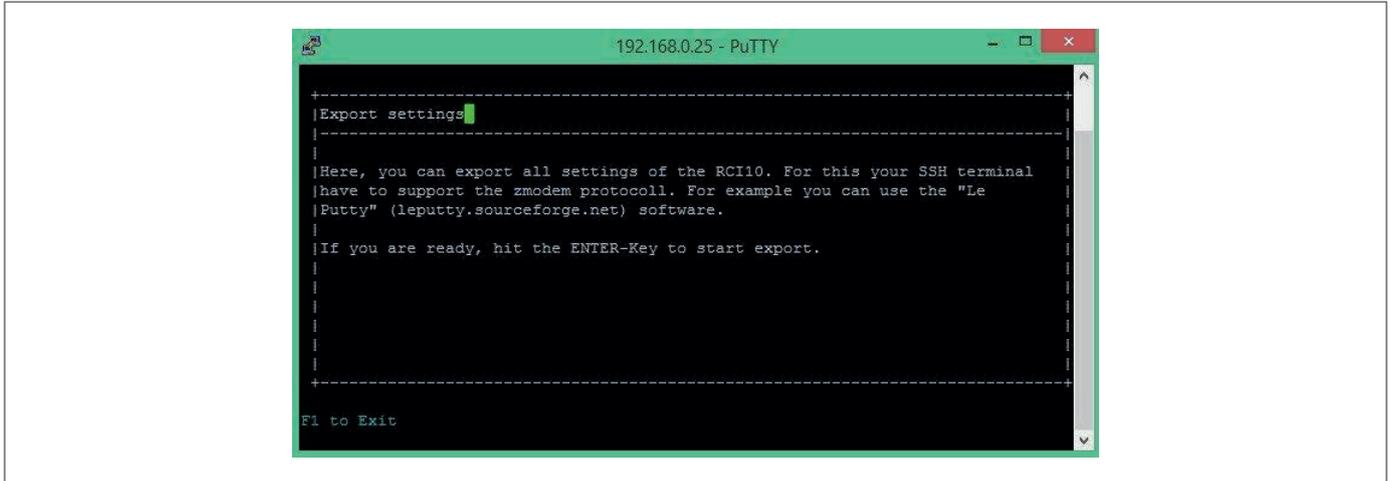


fig. 10: SSH – Export Settings

2. Start the file export with the **Enter** button

3. Navigate with the mouse on the upper SSH window frame. Press the right mouse button and select the menu option **Zmodem Receive**.

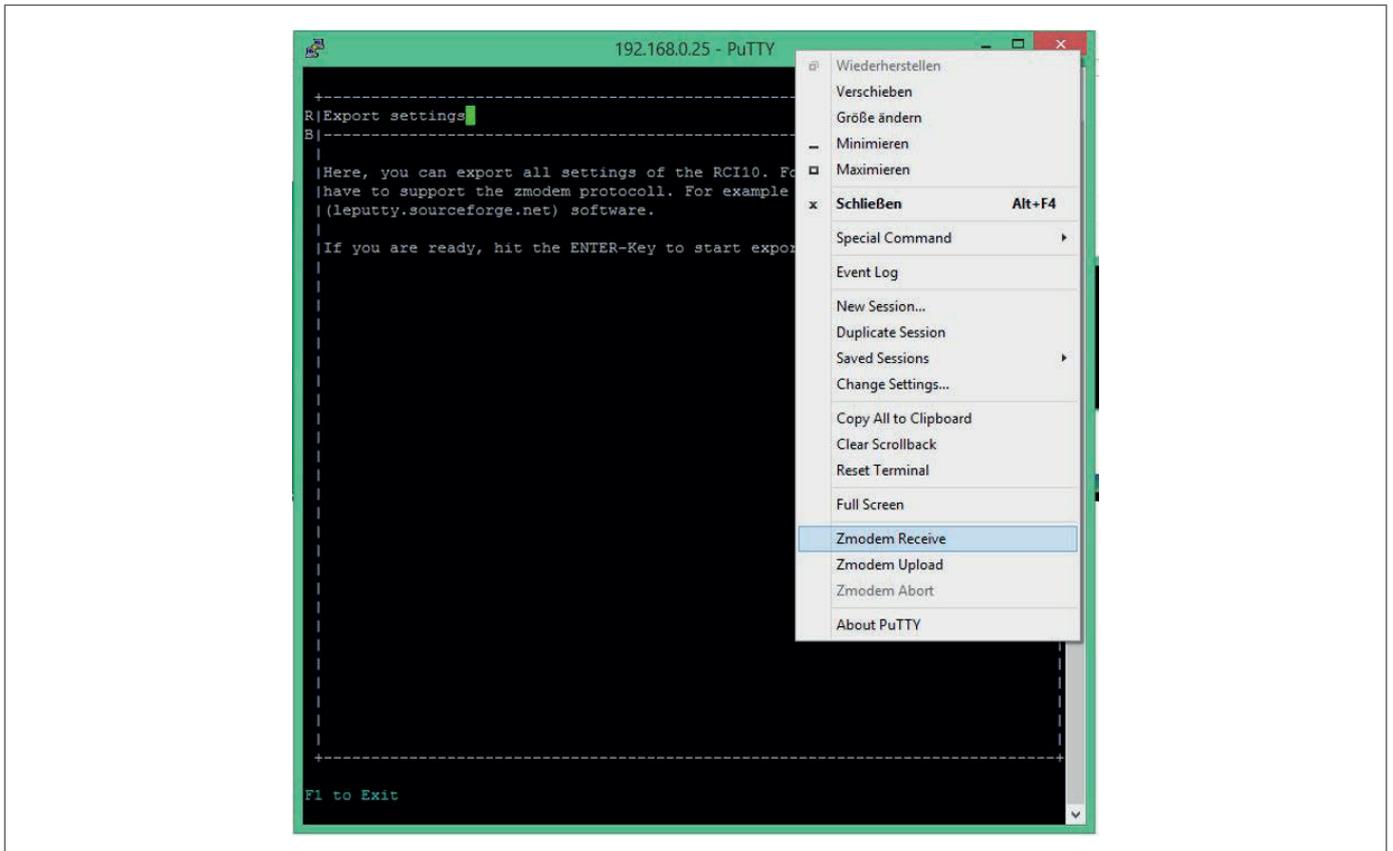


fig. 11: SSH - Zmodem pull down menu

- The RCI10 configuration file will be saved on your configuration PC under the name exportSettings.ini. The memory location on the configuration PC is the path selected in chapter 6.2, para-2, step-4.

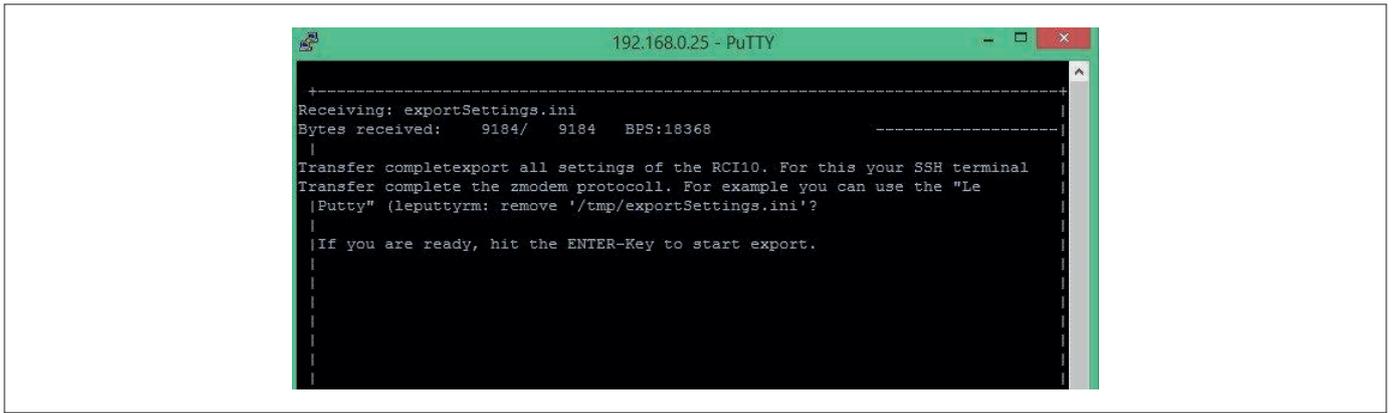


fig. 12: SSH- successful exportation of configuration file

- Press **ESC** to return to main menu.
- Change the name of the saved configuration file exportSettings.ini. A meaningful name is for instance the assigned system name or the installation site of **the ControlPlex® Rack** system.

6.6 Start-up: RCI10 configuration by means of configuration file upload

For a software update or when replacing RCI10 sub-assemblies you can re-input the configuration file saved in chapter 6.5 into the system. Should you operate several **ControlPlex® Rack** systems where e.g. only the IPv4 data are different, you are able to edit the configuration file *.ini and save anew (TXT format). Afterwards you can input the changed file into a new **ControlPlex® Rack** system.



Passwords and user names cannot be changed in the *.INI file. Non-observance will cause loss of RCI10 access.



When changing the INI file, you have to strictly observe the predetermined syntax. Incorrect data, e.g. regarding the IP address format, can cause loss of the functionality of the RCI10 sub-assembly as well loss of access to it.



The configuration file available for upload must not hold any dots or space characters in the file name. Example of correct file name: »Config_CPR_Raum-1_Gestell-5.ini«

- Open an SSH window by means of **LePutty®** to the **ControlPlex® Rack** System
- Log on to the system with your SSH user name and the password.
- Navigate in the SSH menu window with the »Cursor« buttons (↑↓) to the menu option **Import all settings** and press Enter.
- A submenu opens. Start importing the configuration file by pressing the **Enter** button again.
- Navigate with the mouse on the upper SSH window frame. Press the right mouse button, a menu opens. Select the menu option **Zmodem Upload**, see also fig. 11.
- A browser window opens. Mark the configuration file meant for uploading (*.ini) on your configuration PC and click on Open.
- Wait until the upload to the RCI10 has successfully been completed. The SSH window will close automatically.
- Open a new SSH window.
- Navigate in the SSH menu with the Cursor buttons (↑↓) to the menu option **Reboot RCI10 a confirm with Enter** .



The RCI10 sub-assembly carries out a re-boot. The re-boot activates the input configuration data in the RCI10. It can take up to 60 seconds until you can access the RCI10 sub-assembly again.

7 General: RCI10 additional functions SSH surface

Other helpful SSH functions include the storage of current log or measuring value files and the query of RCI10 system information. These functions can be made available to you by means of the web surface.

In addition you have the possibility to reset all settings you changed to the factory setting in the event of a wrong configuration. Upon availability of new functions or bug fixes you can input a software update into the RCI10 sub-assembly



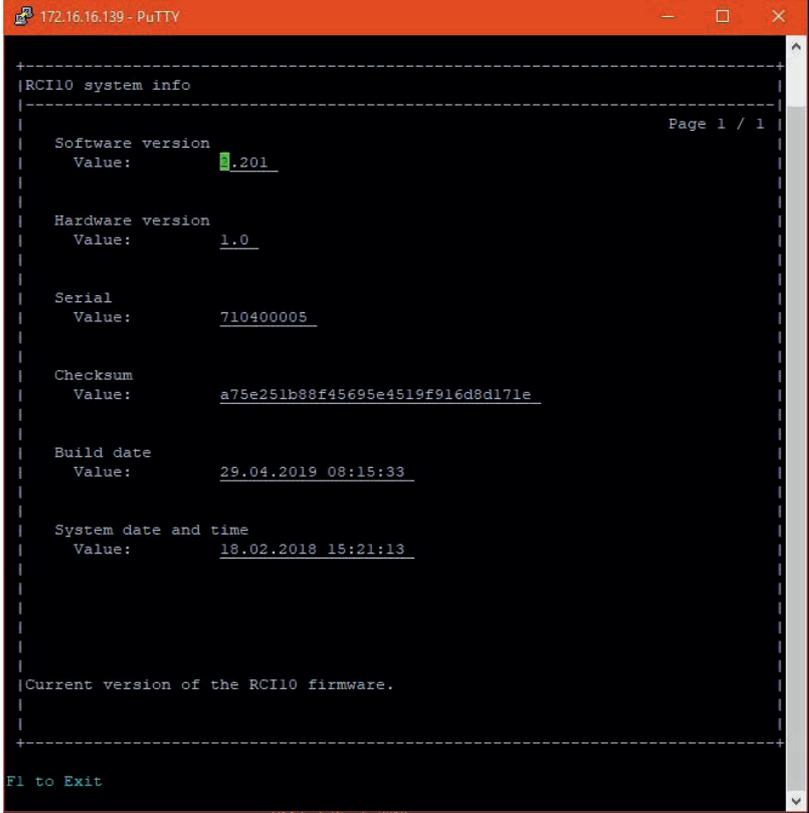
Please observe that after the internal factory pre-set configuration or the configuration carried out by you via the SSHv2 interface, some functions may not be available.

7.1 Operation with SSH surface: Display RCI10 inventory data



These data can also be obtained via the web surface or the SNMP interface.

The SSH menu item **System Info** allows you to view inventory data of the RCI10 board such as software, hardware version, serial number and additional data such as .



```
172.16.16.139 - PuTTY
|RCI10 system info |-----| Page 1 / 1
| Software version |
| Value: 2.201 |
| Hardware version |
| Value: 1.0 |
| Serial |
| Value: 710400005 |
| Checksum |
| Value: a75e251b88f45695e4519f916d8d171e |
| Build date |
| Value: 29.04.2019 08:15:33 |
| System date and time |
| Value: 18.02.2018 15:21:13 |
|-----|
|Current version of the RCI10 firmware.
|-----|
F1 to Exit
```

fig. 13: SSH - system information submenu

7.2 Operation with SSH surface: Download of log data and measuring data file



This function is also available via the web surface.

Open a submenu via the menu option **Export Log** with the option to download the following log files

- **System Log** → messages concerning the **ControlPlex® Rack** system such as adding or removing a circuit protector, short circuit trip etc.
- **Error Log** → internal failure indication of the RCI10 sub-assembly
- **Fuse Log** → measuring data regarding current, voltage and temperature of all installed circuit protectors. The storage time in the RCI10 sub-assembly is at least 30 hrs, depending on the number of circuit protectors and the pre-set measuring cycle time.



The saved measuring data file is saved in a CSV (excel) format, i.e. it can be analysed and processed further by means of a simple excel script.

Download can be carried out following the description in chapter 6.5 start-up: Download RCI10 configuration file via the Z-Modem function of the SSH Client programme **LePutty®** .

7.3 Operation with SSH surface: Reset to factory settings



This function is also available via the web surface.

In the event of faulty configuration entries or if you cannot remember which value you entered how and where, you reset all configuration parameters to the factory setting under menu option **Reset all settings to default**.

1. Navigate in the SSH menu window with the Cursor buttons (↑↓) to the menu option **Reset all settings to default and press Enter**.



There will be no feedback from the system. However, the factory settings were copied into the memory.

2. Navigate in the SSH menu window with the Cursor buttons (↑↓) to the menu option **Reboot RCI10** and press **Enter** . The factory settings will now be re-activated.



Re-boot is visually indicated by the green LED going out. Repeated access of the RCI10 is possible approx. 60 seconds after initiation of the re-boot. The IPv4 and the login settings for new log on into the system can be found in .tab7 2 SSH configuration parameter list and factory settings.

7.4 Operation with SSH surface: RCI10 software update / upgrade

On our website www.e-t-a.de/Controlplex_rack you can check if a new software version is available for download for your RCI10 sub-assembly. In the event of a software update please proceed as follows:

1. Load the new software version onto your configuration PC.
2. Save the configuration data as described in chapter 6.5: start-up: RCI10 configuration file download
3. Navigate in the SSH menu window with the »Cursor« buttons (↑↓) to the menu item **Firmware update** and push **Enter**.
4. Navigate with the mouse on the upper SSH window frame. Press the right mouse button, a menu opens. Select the menu option **Zmodem Upload**, see also fig. 11.
5. A browser window opens. Mark the configuration file meant for uploading on your configuration PC and click on **Open**.
6. The software upload starts automatically. Please wait until the upload to the RCI10 has successfully been completed with the message ».... Reboot«.



The RCI10 sub-assembly automatically carries out a re-boot. Re-boot activates the RCI10 software. It can take several minutes until you can access the RCI10 sub-assembly again.

7. Open a new SSH window.



Please check if the software update was carried out successfully. For this purpose to the menu option **System Info** in the main menu, see chapter 7.1, and check the software version and the build date.

8 General: RCI10 operation with web browser

The web surface offers a comprehensive use of the **ControlPlex® Rack** system. Besides a graphic surface for monitoring and manual switching of the circuit protectors, there is a second level for configuring threshold values for automatic ON and OFF operation of the circuit protectors. Over a third level the log and measuring data files can be reviewed and saved.

8.1 Operation with web browser: Function of the mask »Fuses« (Fuse Control)

The mask »Fuses« or »Fuse Control« serves for monitoring the individual electronic circuit protectors with regard to short circuit, overcurrent trip, under- or overvoltage indication etc. In addition the individual circuit protectors can be switched on or off manually and additional information can be retrieved.

Retrieving additional information about a circuit protector:

Move the mouse pointer to the status indication bar of a circuit protector and the following information will be shown:

- slot number of circuit protector
- current rating of the circuit protector
- hardware version of circuit protector
- serial number of circuit protector
- software version of circuit protector
- present load current of circuit protector
- present voltage on circuit protector
- present temperature of power MOSFET of the circuit protector
- name of circuit protector if applicable

| | | | | | | | | | | |
|------------------------|-----------|----|----------------|-----------|-------------|--------|----------------------|------|------------------------|----|
| Additional Information | Slot No.: | F1 | Type: | 0x70 0x2C | SW-Version: | 1.0.1 | Nominal Current [A]: | 16 | Operating Voltage [V]: | 49 |
| | Label: | F1 | Serial Number: | 720500067 | HW-Version: | 0x0001 | Load Current [A]: | 0.00 | Temperature [°C]: | 31 |

fig. 14: Web mask »Fuses«, additional information ESX300-S

Example: Mask »Fuses«, version with redundant supply

total current indication power input A

total current indication power input B only redundant version

status indication circuit protector F1 via LED colours, see table WEB LED colours. Below, the load-/rated current and the nominal voltage is visualised.

ON/OFF switch circuit protector F3

system information

compare related circuit protectors e.g. F1 with F11 only redundant version

fig. 15: web mask »Fuses« with description

The table below gives a description of the colours for the LED status indication on the web surface.

| field name | status bar: LED colour coding of the circuit protectors on the web surface |
|---------------------------|---|
| short circuit | <p>green: no short circuit $I \leq I_N$ of the circuit protector red: short circuit failure $I > 1.2 \times I_N$ (load output was immediately switched off) grey: empty slot</p> |
| overcurrent | <p>green: no overcurrent $I \leq I_N$ of the circuit protector yellow: overcurrent failure $I > I_N < 1.2 \times I_N$ (load output ON, max, 30 seconds) red: overcurrent failure $I > I_N < 1.2 \times I_N$ (load output was switched off after 30 seconds overcurrent) grey: empty slot</p> |
| undervoltage | <p>ESX300-S minus green: Voltage ≥ 37 V yellow: undervoltage failure $U \leq 36$ V (load output connected) red: undervoltage failure $U \leq 36$ V (load output disconnected; load output was off upon occurrence of the failure or was disconnected manually/automatically during the failure) grey: empty slot</p> <p>ESX300-S plus With the ESX300-S plus, the voltage value must be set manually by means of a slider on the ESX300-S plus. (24 V, 48 V, 60 V). The values indicated below change in accordance with the setting.</p> <p>green: Voltage ≥ 24 V / ≥ 48 V / ≥ 60 V yellow: undervoltage failure $U \leq 18$ V / $U \leq 40$ V / $U \leq 54$ V (load output OFF) red: undervoltage failure $U \leq 36$ V (load output disconnected; load output was off upon occurrence of the failure or was disconnected manually/automatically during the failure) grey: empty slot</p> |
| overvoltage | <p>ESX300-S minus green: Voltage < 72 V yellow: overvoltage failure $U \geq 72$ V (load output connected) red: overvoltage failure $U \geq 73$ V (load output disconnected) grey: empty slot</p> <p>ESX300-S plus With the ESX300-S plus, the voltage value must be set manually by means of a slider on the ESX300-S plus. (24 V, 48 V, 60 V). The values indicated below change in accordance with the setting.</p> <p>green: Voltage $U < 30$ V / < 57 V / < 72 V yellow: overvoltage failure $U \geq 30$ V / ≥ 57 V / ≥ 72 V (load output OFF) red: overvoltage failure $U \geq 31$ V / ≥ 58 V / ≥ 73 V (load output disconnected) grey: empty slot</p> |
| excess temperature | <p>green: temperature of circuit protector ≤ 100 °C red: Excess temperature failure (load output was disconnected, reset is only possible after temperature reduction) grey: empty slot</p> |
| No VCC | <p>green: supply voltage ≥ 15 V grey: no supply voltage</p> |
| Load output | <p>green: load output of circuit protector ON (connected) grey: load output of circuit protector OFF (locked out)</p> |
| Switch output | <p>When actuating (clicking) the button, the load output of the related circuit protector is switched ON or OFF. This is indicated by the LED load output: ON (green) or OFF (grey).</p> |

Table 3: web mask, LED colours

8.2 Parallel connection of several ESX300-S

By connecting several ESX300-S in parallel, loads > 24 A (up to 60 A) can be protected. This functionality is available for the current ratings 16 A, 20 A and 24 A of the ESX300-S plus or ESX300-S minus. Parallel connection of the ESX300 can be configured both at no voltage condition of the box as well as under voltage. It is possible to connect two three ESX300-S in parallel via front-side jumpers and load output jumpers.

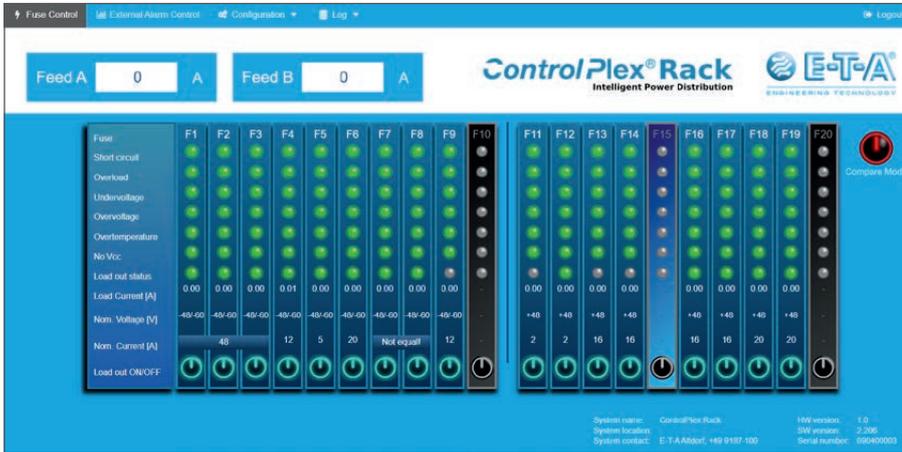


fig. 16: Parallel connection ESX300-S

The slots F2-F4 are fitted with ESX300-S rated 16A. The total current is displayed in the line »rated current [A]« across all circuit protectors connected in parallel ($3 \times 16 \text{ A} = 48 \text{ A}$).

ESX300-S with different current ratings must not be connected in parallel. The slots F7 and F8 are fitted with circuit protectors with different ratings each. If ESX300-S with different ratings are connected in parallel, the user will see the error »Not equal!« in the line current rating [A].

ESX300-S connected in parallel can be switched on or off via any of the circuit protectors in the parallel connection. Example from fig. 16: In order to switch the 48 A group on or off, it is sufficient to switch one output of the slots F2-F4.

It remains possible to read back the information regarding the individual devices even with the parallel connection in place.

It is not possible to enter reference value specifications in the configuration settings with ESX300-S connected in parallel. Use can lead to malfunction.

8.3 Operation with web browser: Function of the mask »External Alarms«

This mask is optional and the EAI300 **External Alarm Interface** sub-assembly must be installed in the Power-D-Box.



For display of the mask you require the RCI10 software version 2.0 or higher.

The mask »**External Alarms**« or »**External Alarm**« serves for monitoring the »external« alarm contacts connected via the the EAI300 sub-assembly such as fire alarm boxes, door contacts or temperature sensors etc. Additionally two alarm outputs can be manually switched on or off. Additional information on hardware and software of the corresponding EAI300 sub-assembly can be displayed.

Recalling additional information about an I/O alarm sub-assembly:

Move the cursor to the status indication bar of an EAI300 alarm sub-assembly (slot S19 in the picture below) and the following information will be shown:

- slot number of the alarm sub-assembly
- sub-assembly type (internal)
- serial number number of the alarm sub-assembly
- software version of alarm sub-assembly
- hardware version of alarm sub-assembly

Example: Mask »External Alarms«

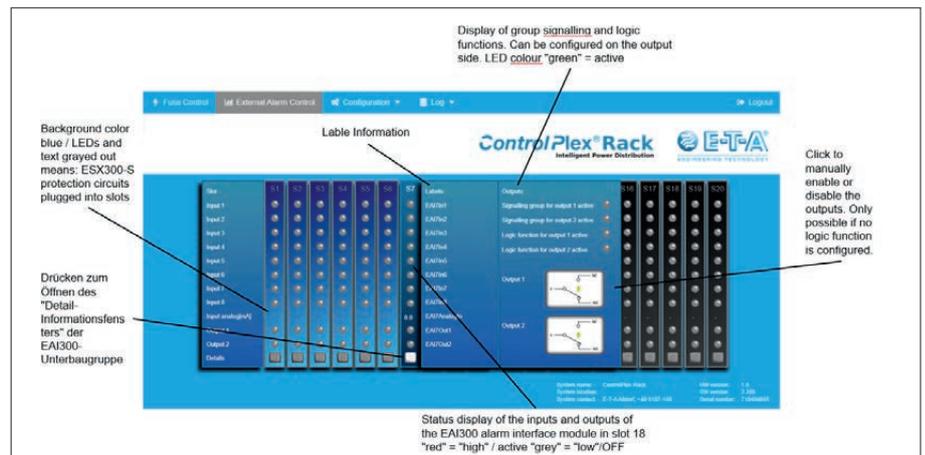


fig. 17: Web mask »External Alarms« with description

8.4 Operation with web browser: Function of the mask »Feed settings«

The mask »**Feed Settings**« offers the possibility to completely and automatically switch on or off all load outputs of a feed group depending on the limit value settings. The following limit value settings are possible:

- Voltage value of feed group → automatic ON and OFF of feed
- Load current value of feed group (total current) → automatic OFF of feed
- Temperature value of feed group (medium value) → automatic ON and OFF of feed



Faulty settings may cause inadvertent failure of your system. We recommend testing activated threshold values before using them for continuous duty.



This function cannot be used if several ESX300-S are connected in parallel.

Example: Mask »Feed Settings«, version PDB-N-CP18R-RR-x with redundant supply

The screenshot shows the 'Feed Settings' web interface. It is divided into sections for 'FEED A' and 'FEED B'. Each section has a 'Save' button, a 'refresh' button, and a 'Delete' button. Annotations include:

- Entries valid for supply group A & B (Feed A & B):** Points to the top navigation bar.
- Checkboxes:** Points to the 'Aktivieren Feed-Monitor nicht-Default' checkbox.
- Fields for entering threshold values:** Points to the input fields for voltage (V), current (A), and temperature (°C) for both feeds.
- Save the entered values:** Points to the 'Save' button.
- refresh:** Points to the 'refresh' button.
- Delete and deactivate all entered values in memory:** Points to the 'Delete' button.
- If not enabled, all set thresholds are automatically disabled after an RC110 restart:** Points to the 'Save' button.

fig. 18: Web mask »Feed Settings« with description

Please proceed as follows for setting threshold values:

1. Activate the check box(es) on the left side of the entry field(s), e.g. for a voltage dependent ON and OFF operation.
2. Enter a threshold value in the corresponding field(s).
3. Save the settings in the RC110 sub-assembly by clicking the button »Save«. The entered settings will thus be activated.
4. If possible, test the activated values on the **ControlPlex® Rack** System.
5. Repeat steps 1 to 4 for each parameter-specific setting.



Should you wish to de-activate the set values, but you do not yet know if you will need them again at a later date, you only have to de-activate the check box(es) beside the input field(s) and save the change(s). Now all threshold values are de-activated, but still saved.

8.5 Operation with web browser: Function of the mask»- Fuse Settings«

The mask »Fuse Settings« offers the possibility to automatically switch on or off one single load output depending on on the threshold values. The following limit value settings are possible:

- Voltage value circuit protector → automatic ON and OFF
- Load current value circuit protector → automatic OFF



The value should be smaller than the current rating of the circuit protector which would otherwise never switch off.

- Temperature value circuit protector → automatic ON and OFF
- System time of RCI10 sub-assembly → automatic ON and OFF
- Free time indication (seconds) →remote RESET of load (power off/on).



Faulty settings may cause inadvertent failure of your system. We recommend testing activated threshold values before using them for continuous duty.



For empty slots, no fields for a threshold value entry will be shown.



This function cannot be used if several ESX300-S are connected in parallel.

Example: Mask »Fuse Settings«

fig. 19: Web mask »Fuse Settings« with description

Please proceed as follows for setting threshold values:

1. Select the load channel you wish to edit by means of the circuit protector number.
2. Activate the check box(es) on the left side of the entry field(s), e.g. for a voltage dependent ON and OFF operation.
3. Enter a threshold value in the corresponding field(s).
4. Save the settings in the RCI10 sub-assembly by clicking the button »Save Settings«. The entered settings will thus be activated.
5. If possible, test the activated values on the **ControlPlex® Rack** System. Repeat steps 2 to 5 for each parameter-specific setting of the circuit protector.



The voltage dependent thresholds can each be indicated with values accurate to a tenth of a volt. Between on and off operation, there must be at least a 1 V difference due to the hysteresis overrun. The threshold values for current and temperature must be indicated without fractional digit.



Please note that the internal date and time configuration of the RCI10 sub-assembly will be used when activating the function **clock time ON / OFF**. If a valid system time is not available, the ON or OFF operation may not be carried out correctly. In the event of a supply voltage failure, date and time indication will be lost (not real time clock available). A possible solution is the configuration of an NTP server, please also see chapter 6.3 Start-up: Configuration via SSH surface



If the function »**condition after reset**« is set to »**OFF**« and the checkbox is activated, the load output of the circuit protector will not automatically be reset in the event of a power failure of the supply voltage and power return or after a re-start of the RCI10 sub-assembly. This function shall prevent an automatic re-start, e.g. of a motor, in the event of a power failure (safety-relevant function).



The function »Monoflop« was implemented specially for »Power Off/ On« of equipment, keeping up the physical connection of the **ControlPlex® Rack** system and the control computer, i.e. even in the event of a disruption of the connection during switching off, the load output will be reset after a pre-set time and the connection will be restored.



Should you wish to de-activate the set values, but you do not yet know if you will need them again at a later date, you only have to de-activate the checkbox(es) beside the input field(s) and save the change(s). Now all threshold values are de-activated, but still saved.

8.6 Operation with web browser: Function of the mask »External Alarm – Labels«

This mask is optional and the EAI300 External Alarm Interface sub-assembly should be pre-installed in the Power-D-Box.



For display of the mask you require the RCI10 software version 2.0 or higher.

The mask »External Alarms – Labels« offers you the possibility to assign a name to every alarm contact input and alarm contact output of an EAI300 sub-assembly. Meaningful names are e.g. »Door_alarm_housing-3 cabinet-1« or »fire-alarm_housing-3 room-6«

Example: Mask »External Alarms - Labels«

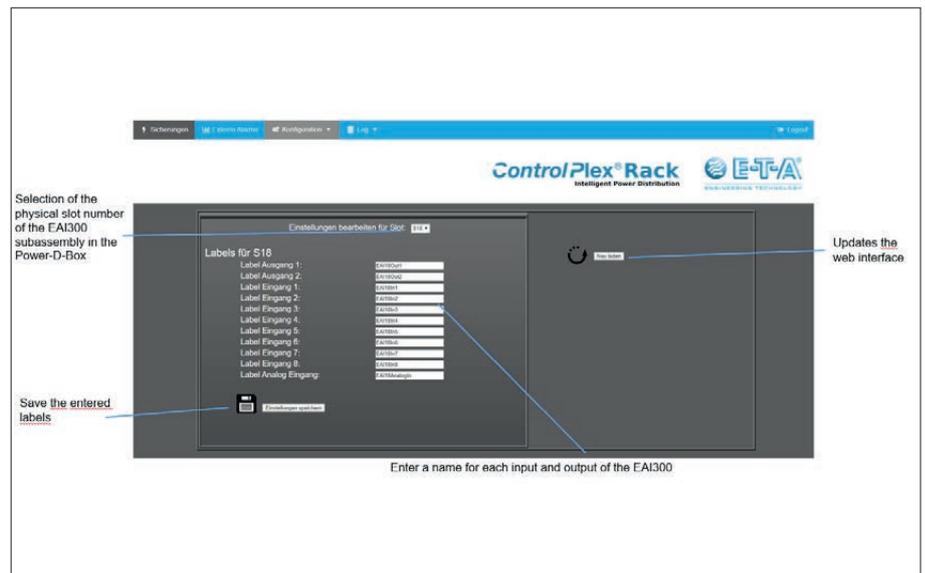


fig. 20: Web mask »External Alarms- Labels« with description



If you select an empty slot (without EAI300 sub-assembly), you can nevertheless already configure a future EAI300 sub-assembly for this slot. However, you need to keep in mind that these parameters will automatically be activated in the event of a later installation of an EAI300 sub-assembly.

Confirm the warning message with **OK** if you wish to configure this slot for an EAI300 sub-assembly all the same.

Confirm the warning message with **Cancel** if you wish to select a different slot.

8.7 Operation with web browser: Function of the mask »External Alarm – Functions«

This mask is optional and the EAI300 External Alarm Interface sub-assembly should be pre-installed in the Power-D-Box.



For display of the mask you require the RCI10 software version 2.0 or higher.

The mask »External Alarms - Functions« allows you to assign a specific (e.g. logically linked) function to each alarm contact output of an EAI300 sub-assembly.

Example: Mask »External Alarm - Functions«

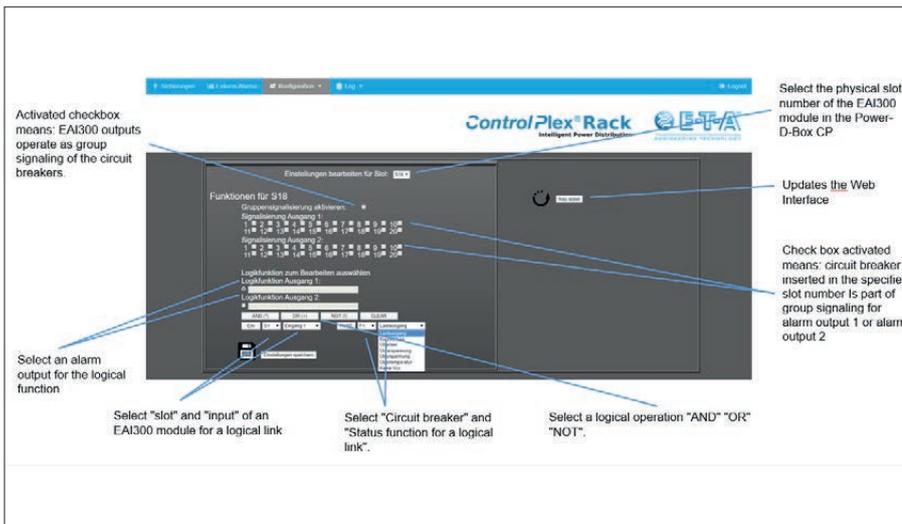


fig. 21: Web mask »External Alarms functions« with description



If you select an empty slot (without EAI300 sub-assembly or occupied by an ESX300-S circuit protector), you can nevertheless already configure a future EAI300 sub-assembly for this slot. However, you need to keep in mind that these parameters will automatically be activated in the event of a later installation of an EAI300 sub-assembly.

Confirm the warning message with **OK** if you wish to configure this slot for an EAI300 sub-assembly all the same.

Confirm the warning message with **Cancel** if you wish to select a different slot.

Please proceed as follows for entering logical functions:

1. Select the output of the EAI300 sub-assembly to which you wish to assign a logic function.
2. Function with status of EAI300 inputs
 - a. Select the slot no. of the EAI300 sub-assembly with selection menu: **S1 – S20** whose input you wish to link.
 - b. Select the input you wish to link by means of selection menu input **1 – 8**
 - c. Click on the button **EAI** (value will be set in the respectively selected field »output 1 or 2«)
 - d. Click on the button **AND** or **OR** or **NOT** depending on how you wish to link this signal logically with another one
 - e. Select the signal to be linked, e.g. an ESX300-S status condition
 - f. Repeat steps a through e depending on how many signals you wish to link

3. Function with ESX300-S status conditions

- A. Select the slot no. of the ESX300-S circuit protector with selection menu: F1 – F20
- b. Select the status condition of the ESX300-S with selection menu: **Load output, short circuit, overload, undervoltage, overvoltage, excess temperature, no VCC**
- c. Click on the button **FUSE** (value will be set in the respectively selected field »output 1 or 2«)
- d. Follow steps 2d through 2f

4. Click on the button **save settings**



In the event of inappropriate entries, there will normally be a warning message and the function will not be adopted. However, these cannot be ensured for all nonsensical configurations.



Nonsensical configurations without error message:

If the group signal function was configured for an EAI300 output (even when selecting only one circuit protector as group signal), but no circuit protector is available in this slot or the slot is occupied with an EAI300, the EAI300 alarm output configured for this purpose is set nevertheless.

The reason is the error »No ESX300 available«. During the configuration, no error message is issued.

Also when configuring a logical function, you can indicate one or more circuit protectors not physically there in the slot (e.g. occupied with EAI300). In this case the EAI300 alarm output is also activated. Cause of the failure as above, no error message during configuration.

In the event of a simultaneous configuration for an EAI300 alarm output, as group signal and as logical function (duplicate assignment) the group signal function takes precedence. In the web mask (detail view) only the LED for the group signal function will be lighted green for the corresponding output. No error message during the configuration.

8.8 Operation with web browser: Function of the mask »System Log«

The mask »**System Log**« allows retrieval and display of all system-relevant events that occurred in *the ControlPlex® Rack*. The log file can additionally be loaded up onto the configuration PC.

Example: Mask »System Log«

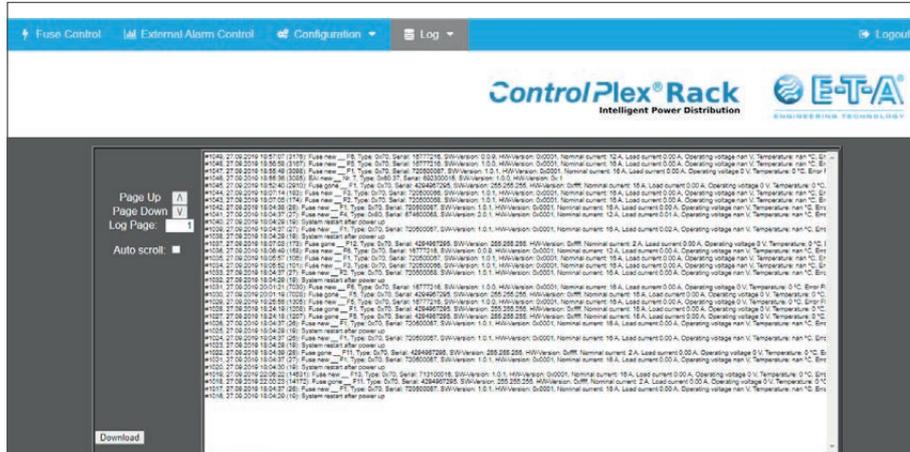


fig. 22: Web mask »System Log«



By clicking on the button »**Download**« you open the log file in a CSV format (excel) or save it on your PC.

8.9 Operation with web browser: Function of the mask »Error Log«

In the mask »**Error Log**« you can retrieve and display all internal messages of the RCI10 interface sub-assembly. The log file can additionally be loaded up onto the configuration PC.

Example: Mask »Error Log«

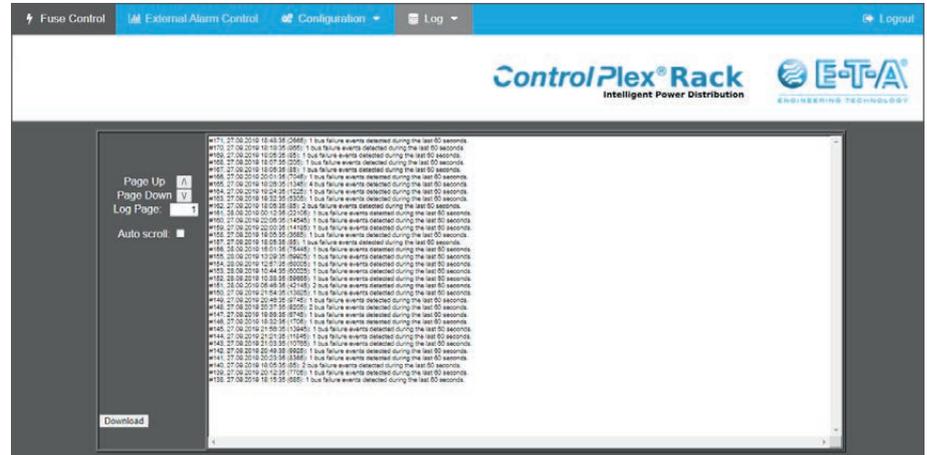


fig. 23: web mask »Error Log«



By clicking on the button»**Download**« you open the log file in a CSV format (excel) or save it on your PC.

Description of system flags:

A: Load output is OFF

S: Short circuit

L: Overload

U: Undervoltage

O: Overvoltage

T: Temperature > 105°C

N: Voltage < 15 V

9 General: RCI10 operation with management system

The supported SNMP protocol allows control of the **ControlPlex® Rack** system centrally by means of a management system. For this purpose the available RCI10-MIB has to be integrated into the management system. Advantages include a centralised alarm surveillance as well as an automation option by connecting various threshold values (also of other systems) within the management system.



For integration of the **ControlPlex® Rack** SNMP-MIB into your management system you possibly require special expert knowledge and the complete documentation of your management system. In the event of any questions please feel free to contact the manufacturer of the management system.

Via the SNMP protocol (MIB tree) you have the following setting options for the network configuration.

- IP address data
- SNMP: log-on data
- System time
- Settings of the **ControlPlex® Rack** system - specific system designations

9.1 Operation with management system: Settings in the RCI10 sub-assembly

Before you can integrate the SNMP MIB into your management system, the RCI10 SNMP settings have to be configured via the SSH interface according to the requirements of the management system. For this purpose you require the following information:

1. Which version of the SNMP protocol is supported by the management system (v1, v2c, v3)?
2. The IP address of the management system to which the alarm and status messages of the RCI10 sub-assembly are to be sent.
3. If you use SNMP v1 or v2c, you need the Community String used by the management system.
4. If you use SNMP v3, you need the SNMPv3 authentication method (MD5, SHA) of the management system.
5. If you use SNMP v3, you need the SNMPv3 encryption method (AES, Off, DES) of the management system.
6. If you use SNMP v3, you may need the SNMPv3 data key entered in the management system.

If all data listed above are known, you configure the SNMP settings of the RCI10 sub-assembly as described in: Chapter 6.3, Start-up: configuration via SSH surface et sqq.

Please also see excerpt below table 4 SSH SNMP settings

| SSH settings Setting parameters | Description | Factory settings |
|------------------------------------|--|------------------|
| SNMP enable | Activation of SNMP access. In OFF condition no SNMP commands will be accepted by a management system. Possible values {Yes; No}. | Yes |
| SNMP protocol | Determination of the permitted SNMP protocol. The RCI10 supports SNMP v1, v2, v3. Data are transmitted encrypted only with v3. Possible values {v1; v2; v3}. | v3 |
| Enable traps | Permit the sending of SNMP traps. If in the ON condition, alarm message can immediately be reported without a query from the superordinate system / management system. Possible values {Yes; No}. | Yes |
| Trap target | The IP addresses or the host name of the system to which the SNMP traps (alarm or status indication) shall be sent. When entering more than one address, they have to be separated by a semicolon. | |
| Allow fuse switch | Determines if the circuit protectors may be switched ON or OFF via the SNMP protocol. Possible values {Yes; No}. | Yes |

| | | |
|-------------------------------|---|------------------------|
| Allow settings write | Parts of the configuration settings such as snmp/login, IP address etc. can be changed directly via SNMP (management system). Possible values {Yes; No}. | Yes |
| SNMP community string | SNMP »community string« of the RCI10 sub-assembly. If the protocol version SNMPv1 or SNMPv2c is used, the management system has to know the string indicated here. The value entered here is valid for the parameters »read« and »write«. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{[]+*#-_.,;<>] | private |
| SNMP login | Defines the user name (user ID) for the web browser access Permitted characters: 20 characters [a-z; 0-9; _-]. | user |
| SNMP password | Defines the password for an SNMP v3 connection. Please observe upper and lower case. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{[]+*#-_.,;<>] | user1234 |
| SNMP authentication | SNMPv3 authentication method. Possible values {MD5; SHA} | MD5 |
| SNMP encryption method | SNMPv3 encryption method. Possible values {AES; off; DES} | AES |
| SNMP encryption key | SNMPv3 key used for data encryption. Permitted characters: 500 characters [a-z; A-Z; 0-9; !\$%&/()=?{[]+*#-_.,;<>] | ControlPlexRack-ESX300 |

Table 4: SSH-SNMP Settings

9.2 Operation with management system: Embed SNMP MIB

The SNMP MIB (file: CP-RCIxx_SNMP-MIB_Vxx.mib) can be downloaded from our website www.e-t-a.de/controlplex_rack free of charge or from an Ethernet connection with an RCI10 sub-assembly or by means of a web browser.

Link: <https://<IP-Adresse RCI10>/esx300cgi.cgi/download/mib>
 <IP-address RCI10> = the IP-address configured on the RCI10



For operation with the sub-assembly “External Alarm Interface EAI300“ you require the RCI10 software version 2.0 or higher and the SNMB-MIB version 2.0 or higher.

For integration of the RCI10 MIB into the management system please follow the instructions of the manufacturer of the management system.

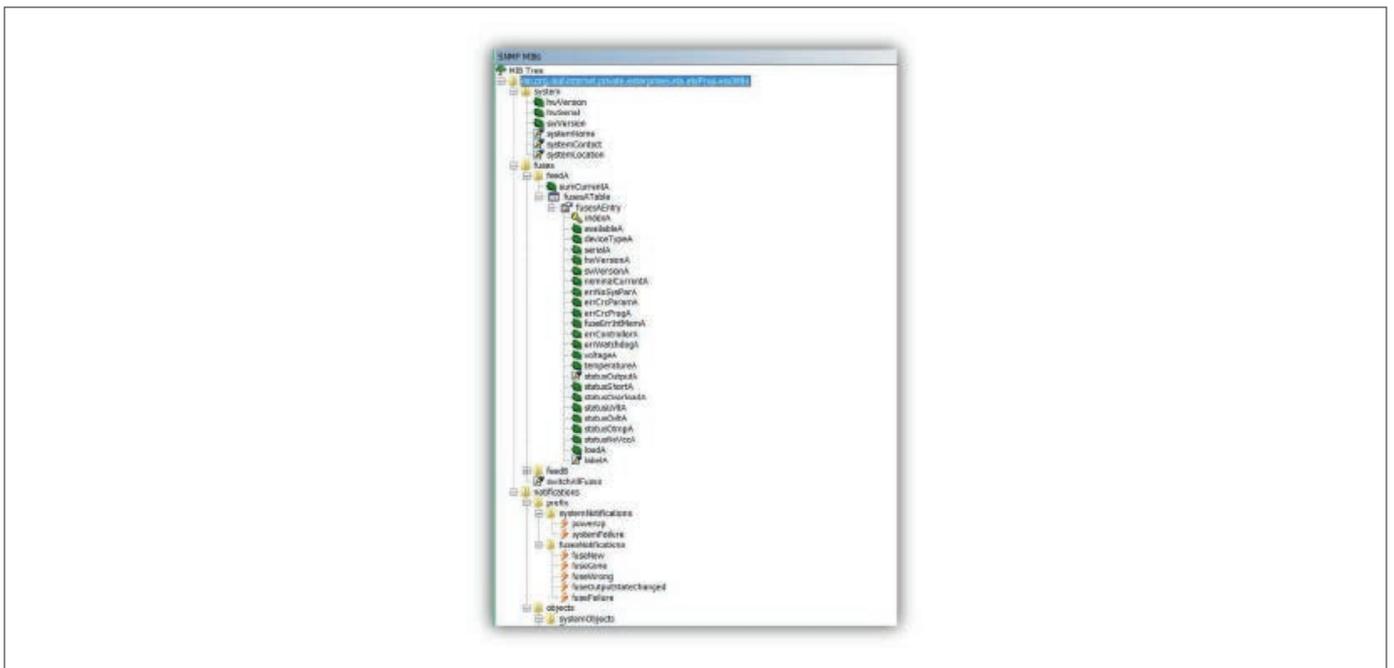


fig. 25: SNMP MIB Tree

9.3 LDAP authentication

The LDAP configuration is done in the SSH menu. Configuration options are described in chapter 6.4.



To accept the configuration, the RCI10 must be re-booted.

For enabling the LDAP users, tick LDAP authentication in the log-on mask of the web interface.

An LDAP user of the Admin group has full access to all configurations/settings. He has the same rights as an internal Admin user (full access, all rights).

The network protocol LDAP allows involving centrally (in one directory server) stored users/user groups into the user structure of the RCI10. The LDAP itself is not a directory, but the protocol. A directory service entry consists of a list of attributes and a "mandatory object" - the name of the object itself, the Distinguished Name (DN) "DN"="CN" and "dc".

A Distinguished Name represents an object in an hierarchical directory and the DN is written from the lower to the superordinate hierarchy levels from left to right. Each hierarchy level is written as follows → keyword=object

There are the following attribute types for the DN:

CN: commonName (user name)

dc: domainComponent

L: localityName

ST: stateOrProvinceName

O: organizationName

OU: organizationalUnitName

C: countryName

STREET: streetAddress

uid: userid

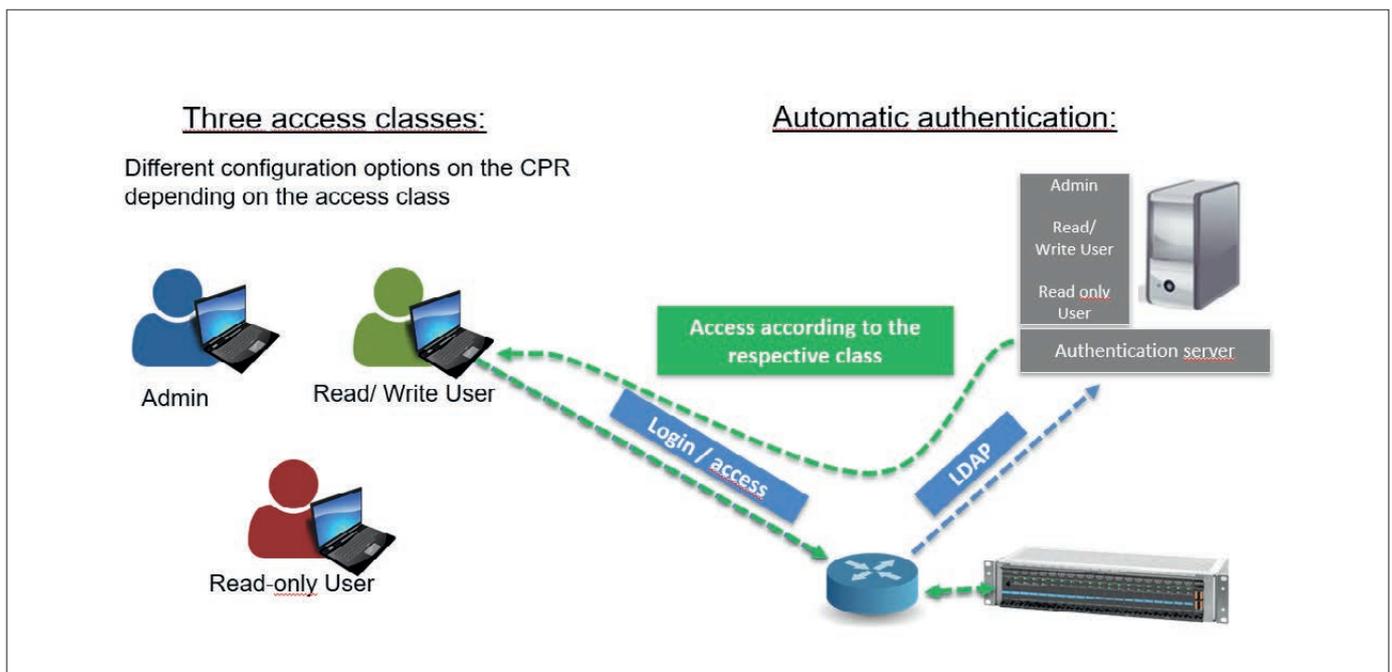


fig. 26: Definition of different access classes on the ControlPlex® Rack and automatic authentication by means of LDAP

Step-by-step explanation:

- Open SSH client (e.g. **LePutty**®)
- Establish connection to RCI
- 01 Set LDAP Enable Value to "YES" → More entry option will open.
- 02 Define encryption
- 03 Enter LDAP server address/IP and Port 389 (Port 389 can company-specifically differ)
- 04 Enter Base DN to define entry point of user search
- 05 Enter log-on and password attribute mapping values
- 06 Enter user object class value
- 07 Enter Uid and Gid number attribute mapping values
- 08 Enter group member attribute mapping value
- 09 Define admin/read write/read only groups
- 10 Enter Bind DN and password for a user bind; if an anonymous bind shall be used, this field must remain empty.
- Check the checkbox in the log-on mask for use of the web surface LDAP authentication→ see fig. 4
- Reboot RCI10 on SSH surface

```

LDAP
-----
01 LDAP Enable
   Value:      Yes

02 LDAP SSL
   Value:      off

Server
   Value:      172.16.61.31

03 Port
   Value:      389

04 Base DN
   Value:      Dc=mon,dc=lan

Login attribute mapping
   Value:      cn

05 Password attribute mapping
   Value:      userPassword

06 User object class
   Value:      user

07 Uid number attribute mapping
   Value:      uidNumber

Gid number attribute mapping
   Value:      gidNumber

Additional filter
   Value:

08 Group member attribute mapping
   Value:      MemberOf

Admin group
   Value:      Cn=TestGroup2,dc=mon,dc=lan

09 User (read write) group
   Value:

User (read only) group
   Value:
    
```

```

LDAP
-----

Bind DN
   Value:      Cn=Tum,DC=mon,dc=lan

10 Bind password
   Value:      ***
    
```

| Attribute | Value |
|-----------------------|---|
| objectClass | inetOrgPerson |
| objectClass | organizationalPerson |
| objectClass | person |
| objectClass | posixAccount |
| objectClass | top |
| cn | 1 |
| gidNumber | 1002 |
| homeDirectory | /home |
| sn | admin |
| uid | ldap-admin1 |
| uidNumber | 1002 |
| userPassword | ***** |
| createTimestamp | 20191001161205Z |
| creatorName | cn=Directory Manager,cn=Root DNs,cn=config |
| entryDN | uid=ldap-admin1,dc=base,dc=com |
| entryUUID | 142ae95+c0bb-4654-04df-0be09e15d39e |
| ctag | 0000000066190a12 |
| hasSubordinates | false |
| memberOf | cn=admin,dc=base,dc=com |
| modifiersName | cn=Internal Client,cn=Root DNs,cn=config |
| modifyTimestamp | 20191001164113Z |
| numSubordinates | 0 |
| pwdChangeTime | 20191001164113.8417 |
| pwdPolicySubentry | cn=Default Password Policy,cn=Password Policies,cn=config |
| structuralObjectClass | inetOrgPerson |
| subschemaSubentry | cn=schema |

fig. 27: LDAP configuration via SSH

Exemplary settings Microsoft Active Directory

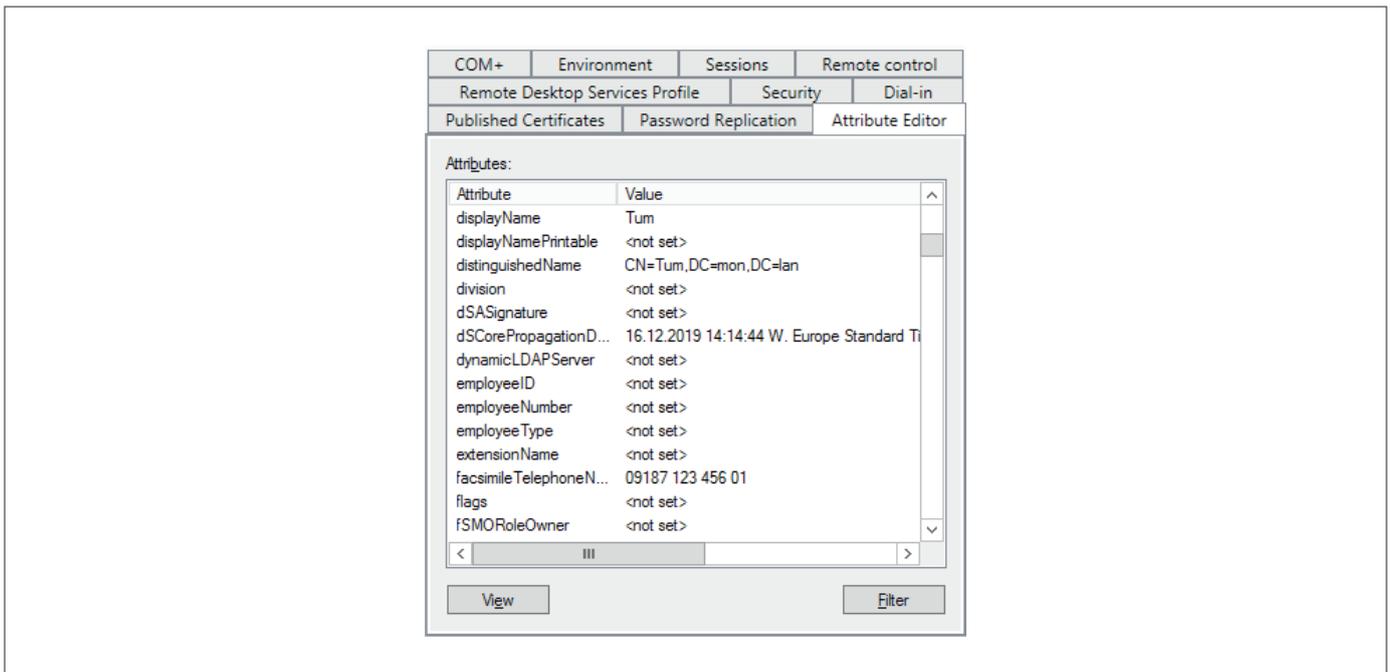


fig. 28: Attribute and values of the LDAP server (Microsoft Active Directory)

Example: SSH configuration:

- LDAP Enable Value = YES → authentication via LDAP protocol is activated
- LDAP SSL Value = off → SSL encryption deactivated
- Server Value = 172.168.0.100 → address of LDAP server
- Port Value = 389 → This port is used as standard for LDAP (alternatively on port 636 in a TLS-secured connection)
- Base DN Value = Dc=mon,dc=lan → entry point (DN) for user search
- Login attribute mapping Value = cn → value of attribute "cn" is the user name
- Passwort attribute mapping Value = userPassword → The value of the attribute "userPassword" is the user password
- User object class Value = user → determines the object class of the user
- Uid number attribute mapping Value = uidNumber → the value (>1000) of the attribute mapping value is the uid number
- Gid number attribute mapping Value = gidNumber → the value of the attribute is the gid number
- Additional filter Value = → no additional filter for the user search (user-defined filter would be possible)
- Group member attribute mapping Value = memberOf → the value of the attribute "isMemberOf" is the DN of group of which the user is a member (is used for authorisation)
- Admin group Value = Cn=anyGroup,dc=mon,dc=lan → complete DN
- User (read write) group Value = Cn=userrw,dc=mon,dc=lan → Distinguished Names defining the read-write users
- User (read only) group Value = Cn=userr,dc=mon,dc=lan → Distinguished Names (under which values are saved which) define the read-only users
- Bind DN Value = CN=bestehenderUser,CN=Users,DC=mon,DC=lan → existing user, via whome anew user can be searched
- Bind password Value = → PW of the user to be reached

Please note: (Bind DN & Password): If both fields remain empty, an anonymous bind is carried out; otherwise a user bind will be carried out.

Example: BASE DN:

In an active directory "bsp.intern", a new user called "Schmidt, Thomas" is set up while the selection was set on the root directory bsp.intern. It is shown as a distinguished name:

```
CN=Thomas Schmidt,DC=bsp,DC=intern
```

The object is now shifted into an OU called "Persons" and the DN is reviewed.

```
CN=Thomas Schmidt,OU=Personen,DC=bsp,DC=intern
```

Within the OU Persons, the admin will set another OU to improve orientation. It will be called "fictitious staff" and the user object of Herr Schmidt will be assigned to this new OU. Hence the DN is:

```
CN=Thomas Schmidt,OU=Fiktive Mitarbeiter,OU=Personen,DC=bsp,DC=intern
```

Explanation of "attribute mapping":

On the tab attributes, you can determine how the attributes shall be shown in the Active Directory or in the LDAP directory on user properties.

Depending on the server configuration, you will have to change these values or complete them. Enter the same values for the attributes that are defined in the scheme file for the active directory server or the LDAP server.

10 Appendix:

List of pictures

| | |
|--|----|
| fig. 1: Schematic diagram ControlPlex® Rack | 10 |
| fig. 2: Connection example ControlPlex® Rack | 10 |
| fig. 3: IPv4 setting of configuration PC | 11 |
| fig. 4: Web browser log-on IE | 12 |
| fig. 5: Web mask »fuses« | 12 |
| fig. 6: Web mask »Configuration/System settings« | 13 |
| fig. 7: IP configuration LePutty® | 15 |
| fig. 8: ZModem configuratio LePUTTY | 16 |
| fig. 9: SSH main menu | 16 |
| fig. 10: SSH – Export Settings | 22 |
| fig. 11: SSH - Zmodem pull down menu | 22 |
| fig. 12: SSH– successful exportation of configuration file | 23 |
| fig. 13: SSH - system information submenu | 24 |
| fig. 14: Web mask »Fuses«, additional information ESX300-S | 27 |
| fig. 15: Web mask »Fuses« with description | 27 |
| fig. 16: Parallel connection ESX300-S | 29 |
| fig. 17: Web mask »external alarms« with description | 30 |
| fig. 18: Web mask »Feed Settings« with description | 31 |
| fig. 19: Web mask »Fuse Settings« with description | 32 |
| fig. 20: Web mask »External Alarms- Labels« with description | 34 |
| fig. 21: Web mask »External Alarms functions« with description | 35 |
| fig. 22: Web mask »System Log« | 37 |
| fig. 23: Web mask »Error Log« | 38 |
| fig. 24: Web mask »Fuse Log« | 39 |
| fig. 25: SNMP MIB Tree | 41 |
| fig. 26: Definition of different access classes on the ControlPlex® Rackk and automatic authentication by means of LDAP | 42 |
| fig. 27: LDAP configuration via SSH | 43 |
| fig. 28: Attribute and values of the LDAP server (Microsoft Active Directory) | 44 |

11 Appendix:

List of abbreviations

| | |
|--------------------------|---|
| ControlPlex® Rack | electronic power distribution system with ESX300-S electronic circuit protectors and RCI10 interface sub-assembly |
| DHCP | Dynamic Host Configuration Protocol |
| DC | Direct Current |
| EAI300 | alarm interface sub-assembly for »external« alarms |
| ESX300-S | electronic circuit protector for DC -48 V/ DC -60 V |
| Ethernet | standardised interface for wired data networks |
| EMC | electromagnetic compatibility |
| HTTP | Hypertext Transfer Protocol (open transmission) |
| HTTPS | Hypertext Transfer Protocol Secure (encrypted transmission) |
| IP | Internet Protocol |
| LDAP | Lightweight Directory Access Protocol (network protocol for reading and editing information if distributed directory services) |
| LePuTTY© | Client Programme with SSH protocol support |
| MIB | Management Information Base; programme part which can be embedded in a management system and which communicates via an SNMP protocol. |
| NTP | Network Time Protocol (automatic time synchronisation) |
| PDB | Power-D-Box (power distribution system) |
| RCI10 | Remote Control Interface sub-assembly |
| RSI10 | Sub-assembly for group signalling of the ESX300-S circuit protectors |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell (encrypted transmission) |
| Terminal | Client Programm, see LePutty® |
| URL | Uniform Resource Locator, the www address of a website. |
| Web browser | Programme for display of http / https protocol data such as the Microsoft internet explorer |

12 Appendix: Legal references and licences

SSH Client Programm **LePutty**[®]:

The programme **LePutty**[®] was not changed or adjusted by E-T-A in any way. E-T-A tests the software to our best knowledge before making it available for download on our website. However, E-T-A does not assume liability for failures caused by misuse or software errors in the programme or malicious code. The version tested and made available on the E-T-A website refers to **LePutty**[®] 0.53b. It is based on Putty[®] Beta Release 0.53" Build Date" 3rd October 2006.

LePutty[®] is based on the programme **Putty**[®].

See **PuTTY**[®] / **LePutty**[®] Homepage - legal notice, licenses and copyright

PuTTY[®]: PuTTY is copyright 1997-2015 Simon Tatham
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

LePutty[®]: <http://leputty.sourceforge.net>

E-T-A: **ControlPlex**[®] Rack; Download area - SSH-Client Software -
https://www.e-t-a.de/produkte/intelligente_stromverteilung/controlplex/controlplex_rack/

Software Lizenzen **ControlPlex**[®] Rack:
see <http://www.e-t-a.de/licenses>

13 Appendix: Template of configuration table

Print table and enter values

| SSH settings Setting parameters | Description | value |
|---|--|-------|
| SSH user login | Defines the user name (user ID) for the SSH login. Permitted characters: 20 characters [a-z; 0-9; _-]. | |
| SSH user password | Defines the password for the SSH login. Please observe upper and lower case. Permitted characters: 110 characters [a-z; 0-9; \$/.] | |
| HTTP settings Setting parameters | Description | value |
| HTTP enable | Activation web server Allow access via web browser. Possible values {Yes; No}. | |
| Access only using HTTPS | Web browser access only via HTTPS protocol possible (encrypted transmission). Possible values {Yes; No}. | |
| Allow settings write | Parts of the configuration settings such as http/login, IP address etc. can be changed directly via the web browser. Possible values {Yes; No}. | |
| Allow fuse switch via HTTP | Determines if the circuit protectors may be switched ON or OFF via the web browser surface. Possible values {Yes; No}. | |
| HTTP access is: password protected | Web browser access only possible with user ID and password (http and https). Possible values {Yes; No}. | |
| HTTP log-on | Defines the user name (user ID) for the web browser access Permitted characters: 20 characters [a-z; 0-9; _-]. | |
| HTTP password | Defines the password for the web browser access Please observe upper and lower case. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#- _.:;<>] | |
| HTTP language | Defines the language for the web browser surface. Possible values {english; german}. | |
| SNMP settings Setting parameters | Description | value |
| SNMP enable | Activation of SNMP access. In OFF condition no SNMP commands will be accepted by a management system. Possible values {Yes; No}. | |
| SNMP protocol | Determination of the permitted SNMP protocol. The RCI10 supports SNMP v1, v2, v3. Data are transmitted encryptedly only with v3. Possible values {v1; v2; v3}. | |
| Enable traps | Permit the sending of SNMP traps. If in the ON condition, alarm message can immediately be reported without a query from the superordinate system / management system. Possible values {Yes; No}. | |
| Trap target | The IP addresses or the host name of the system to which the SNMP traps (alarm or status indication) shall be sent. When entering more than one address, they have to be separated by a semicolon. | |
| Allow fuse switch | Determines if the circuit protectors may be switched ON or OFF via the SNMP protocol. Possible values {Yes; No}. | |
| Allow settings write | Parts of the configuration settings such as snmp/login, IP address etc. can be changed directly via SNMP (management system). Possible values {Yes; No}. | |

| | | |
|---|---|--------------|
| SNMP community string | SNMP »community string« of the RCI10 sub-assembly. If the protocol version SNMPv1 or SNMPv2c is used, the management system has to know the string indicated here. The value entered here is valid for the parameters »read« and »write«. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#- _.:; <> \] | |
| SNMP login | Defines the user name (user ID) for the web browser access Permitted characters: 20 characters [a-z; 0-9; _-]. | |
| SNMP password | Defines the password for an SNMP v3 connection. Please observe upper and lower case. Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#- _.:; <> \] | |
| SNMP authentication | SNMPv3 authentication method. Possible values {MD5; SHA} | |
| SNMP encryption method | SNMPv3 encryption method. Possible values {AES; off; DES} | |
| SNMP encryption key | SNMPv3 key used for data encryption. Permitted characters: 500 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#- _.:; <> \] | |
| NTP settings | Description | value |
| Setting parameters | | |
| NTP enable | Activate NTP Client (automatic time synchronisation via external server). Possible values {Yes; No}. | |
| Server | IP address or URL of the NTP server from where the time information shall be obtained. Permitted characters: 100 characters [a-z; A-Z; 0-9; _-]. | |
| Time zone | Adjust time zone (time difference between local time and UTC). Possible values {-12..-1; 0; 1..12}. Example: 1 = Central European Time (CET), 2 = Central European Summer Time (CEST) | |
| DST | Calculate with summer time and winter time Possible values {Yes; No}. | |
| LDAP settings | Description | value |
| Setting parameters | | |
| LDAP Enable Value | Defines the users: Internal users = NO, user of LDAP server = YES /NO | |
| LDAP SSL Value | Encryption options: SSL encryption = on, encryption via TLS connection =startTls, no encryption = off/on | |
| Server Value | Host name or IP address of LDAP server | |
| Port Value | LDAP port | |
| Base DN Value | Entry point (DN) for user search | |
| Login attribute mapping Value | Value of attribute is the user name used | |
| Password attribute mapping value | Value of attribute is the user name used | |
| User object class value | Determines the object class of the user | |
| Uid number attribute mapping value | Determines which value of the attribute shall be used as uid number (min. 4-digit number) | |
| Additional filter value | User-defined filter (optional) | |
| Group member attribute mapping value | The value of the attribute "isMemberOf" is the DN of the group where the user is 8is used for authorisation) | |
| Admin group value | DN of admin group | |
| User (read write) group value | DN of the read-write group | |

| | | |
|--|--|--------------|
| User (read write) group value | DN of the read-only group | |
| Ethernet settings | Description | value |
| Setting parameters | | |
| Enable IPv4 | <p>Activation of the IPv4 address range for addressing the RCI10 sub-assembly.</p> <p> Should you set this value to »No«, the RCI10 can no longer be addressed via IPv4. Possible values {Yes; No}.</p> | |
| Use DHCP for IPv4 | <p>Activate DHCP or IPv4 If activated, an IPv4 address is automatically assigned via the connected network.</p> <p>Possible values {Yes; No}.</p> | |
| IP address | <p>IPv4 address, RCI10 sub-assembly.</p> <p>Example format {xxx.xxx.xxx.xxx}</p> | |
| Network mask | <p>IPv4 network mask, RCI10 sub-assembly</p> <p>example format {xxx.xxx.xxx.xxx}</p> | |
| Gateway | <p>IPv4 gateway of the current network segment</p> <p>example format {xxx.xxx.xxx.xxx}</p> | |
| DNS server IPv4/IPv6 | <p>IPv4 address of the »Domaine Name Server« (DNS).</p> <p>Example format {xxx.xxx.xxx.xxx}</p> | |
| Enable IPv6 | <p>Activation of the IPv6 address range for addressing the RCI10 sub-assembly. Possible values {Yes; No}.</p> | |
| Use DHCP for IPv6 | <p>Activate DHCP or IPv6 If activated, an IPv6 address is automatically assigned via the connected network.</p> <p>Possible values {Yes; No}.</p> | |
| IP address | <p>IPv6 address, control interface RCI10</p> <p>Example format {2001:db8:1:2:3C5:811::1}</p> | |
| Network prefix length | <p>Enter the IPv6 length of the network prefix</p> <p>Possible values: 3 characters [0-9].</p> | |
| DNS server IPv4/IPv6 | <p>IPv6 address of the »Domaine Name Server« (DNS).</p> <p>Example format {2001:db8:1:2:3C5:811::1}</p> | |
| RCI10 settings | Description | value |
| Setting parameters | | |
| Fuse log periodicity | <p>Period duration in seconds, with which measuring values of each ESX300-S circuit protector will be written into the log file, e.g.: load current, voltage and temperature values.</p> <p>Possible values {off, 30 ... 600}.</p> | |
| Allow reset to factory defaults | <p>Option to reset all setting parameters listed in this table to the factory settings. When entering »No« the menu option »Reset to factory default« will disappear. Possible values {Yes; No}.</p> | |
| System name | <p>Freely selectable system name. Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;,;<> \`']</p> | |
| System contact | <p>Freely selectable system contact name (e.g. person to contact on site).</p> <p>Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;,;<> \`']</p> | |

| | | |
|---|---|--------------|
| System location | Freely selectable system location. Permitted characters: 100 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> '«'] | |
| Time / Date settings | Description | value |
| time | Enter present time, if no NTP server (see NTP settings) was indicated or is available. The parameter »NTP enable« has to be set to »no« for that. Format {hh.mm.ss} | |
| Date | Enter present date, if no NTP server (see NTP settings) was indicated or is available. The parameter »NTP enable« has to be set to »no« for that. Format {DD.MM.YYYY} | |
| Time zone | Adjust time zone (time difference between local time and UTC). Possible values {-12..-1; 0; 1..12}. Example: 1 = Central European Time (CET), 2 = Central European Summer Time (CEST) | |
| DST | Calculate with summer time and winter time Possible values {Yes; No}. | |
| Fuse Labels Setting parameters | Description | value |
| Label for fuse: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 | Freely selectable system name for the circuit protector ESX300-S in the slot. A1 .. A20 (A1 – A10 and B1 – B10). Permitted characters: 20 characters [a-z; A-Z; 0-9; !\$%&/()=?{}+*#-_.:;<> '«'] | |

E/A Alarm Interface sub-assembly type EAI300

| EAI300 settings | Setting parameters | Description | value |
|----------------------|-------------------------------|--|-------|
| EAI300 Slot . | Label for output 1 | Freely selectable alarm denomination for the EAI300 sub-assembly in slot A] alarm output 1. | |
| | Label for output 2 | Alarm denomination for EAI300 in slot A... - alarm output 2 | |
| | Label for input 1 | Alarm denomination for EAI300 in slot A... - digital input 1 | |
| | Label for input 2 | Alarm denomination for EAI300 in slot A... - digital input 2 | |
| | Label for input 3 | Alarm denomination for EAI300 in slot A... - digital input 3 | |
| | Label for input 4 | Alarm denomination for EAI300 in slot A... - digital input 4 | |
| | Label for input 5 | Alarm denomination for EAI300 in slot A... - digital input 5 | |
| | Label for input 6 | Alarm denomination for EAI300 in slot A... - digital input 6 | |
| | Label for input 7 | Alarm denomination for EAI300 in slot A... - digital input 7 | |
| | Label for input 8 | Alarm denomination for EAI300 in slot A... - digital input 8 | |
| | Label for analog input | Alarm denomination for EAI300 in slot A... - analog input 1 | |
| | Logic function for output 1 | Set up a logic link for EAI300 – slot A ... – alarm output 1 | |
| | Logic function for output 2 | Set up a logic link for EAI300 in slot A ... - alarm output 2 | |
| | Signalling group for output 1 | Set up a group or single signalling function of the circuit protectors for EAI300 in slot A... - alarm output 1. | |
| | Signalling group for output 2 | Set up a group or single signalling function of the circuit protectors for EAI300 in slot A....- alarm output 2 | |

14 Appendix: Example RCI10 configuration file (excerpt)

Excerpt from file: exportSettings.ini

```
[dhcp]
enablev4=0
enablev6=1

[eth]
dns=
enablev6=0
ipv4addr=192.168.0.25
ipv4gateway=
ipv4mask=255.255.255.0
ipv6addr=2001::
ipv6prefixlen=56

[feeda]
switchbackontemperature=
switchbackontemperatureen=
switchbackonvoltage=
switchbackonvoltageen=
switchoffcurrent=
switchoffcurrenten=
switchofftemperature=
switchofftemperatureen=
switchoffvoltage=
switchoffvoltageen=

[fuse1]
label=Server-1
stateafterreset=
stateafterreseten=0
switchbackonovertemperature=
switchbackonovertemperatureen=
switchbackonovervoltage=
switchbackonovervoltageen=
switchoffcurrent=
switchoffcurrenten=
switchoffovertemperature=
switchoffovertemperatureen=
switchoffovervoltage=
switchoffovervoltageen=
switchofftime=
switchofftimeen=
switchontime=
switchontimeen=

[http]
allowfuseswitch=1
allowlogaccess=1
allowsettingswrite=1
authonly=1
httpsonly=1
language=de
login=eta
password=***

[misc]
systemcontact=
systemlocation=
systemname=Control Plex Rack

[ntp]
dst=1
enable=1
server=ptbtime1.ptb.de
timezone=1

[rack]
enablefeedmonitoringafterreset=0

[snmp]
allowfuseswitch=1
allowsettingswrite=0
authentication=MD5
community=private
enable=1
enabletraps=1
encryption=AES
encryptionkey=
login=eta
password=***
traptarget=

SSH
password=*****
```

Notes

