

Technical Manual

Network Time Client with 2 LAN Interfaces

Model 7279(RC)

ENGLISH

Version: 04.01 - 29.11.2018

SETIMAGE (8030)FIRMWARE (8030)Valid forVersion: 04.xxVersion: 02.xx





Version Numbers (Firmware / Description)

The term **SET** defines the fixed connection between the image version and the related H8 firmware version.

THE FIRST TWO DIGITS OF THE TECHNICAL DESCRIPTION VERSION NUMBER, THE **SET** VERSION AND THE IMAGE VERSION **MUST BE THE SAME**! THEY DESCRIBE THE SHARED FUNCTIONAL IDENTITY BETWEEN DEVICE, SOFTWARE AND TECHNICAL DESCRIPTION.

THE VERSION NUMBER OF THE IMAGE AND THE H8 SOFTWARE CAN BE FOUND IN THE WEBGUI OF THIS DEVICE (SEE **CHAPTER 5.3.7.1 DEVICE INFORMATION AND CHAPTER 5.3.7.2 HARDWARE INFORMATION**).

THE TWO VERSION NUMBER'S DIGITS AFTER THE DOT DESCRIBE CORRECTIONS RE-GARDING THE FIRMWARE AND/OR DESCRIPTION WHICH HAVE NO EFFECT ON FUNC-TIONALITY.

Downloading Technical Manuals

All current manuals of our products are available free of charge via our homepage on the Internet.

Homepage: http://www.hopf.com

E-mail: <u>info@hopf.com</u>

Symbols and Characters



Operational Reliability Disregard may cause damages to persons or material.



Functionality Disregard may impact function of system/device.



Information Notes and Information.





Safety regulations

The safety regulations and observance of the technical data serve to ensure trouble-free operation of the device and protection of persons and material. It is therefore of utmost importance to observe and comply with these regulations.

If not complied with, then no claims may be made under the terms of the warranty. No liability will be assumed for any consequential damages.

<u>F</u>

Safety of the device

This device has been manufactured in accordance with the latest technological standards and approved safety regulations

The device should only be put into operation by trained and qualified staff. Care must be taken that all cable connections are laid and fixed in position correctly. The device should only be operated with the voltage supply indicated on the identification label.

The device should only be operated by qualified staff or employees who have received specific instruction.

If a device must be opened for repair, this should only be carried out by employees with appropriate qualifications or by *hopf* Elektronik GmbH.

Before a device is opened or a fuse is changed, all power supplies must be disconnected.

If there are reasons to believe that the operational safety can no longer be guaranteed, the device must be taken out of service and labelled accordingly.

The safety may be impaired when the device does not operate properly or if it is obviously damaged.

CE-Conformity



This device fulfils the requirements of the EU directive 2014/30/EU "Electromagnetic Compatibility" and 2014/35/EU "Low Voltage Equipment".

Therefore, the device bears the CE identification marking (CE = Communautés Européennes = European communities)

The CE indicates to the controlling bodies that the product complies with the requirements of the EU directive - especially with regard to protection of health and safety for the operator and the user - and may be released for sale within the common markets.



Contents

Page

5 / 125

1 Descrip	otion of the Board	7
1.1 Fron	t Panel	9
1.1.1 B	oard 7279 and 7279RC for 3U / 19" Racks	9
1.1.2 F	Interior and Demoval of the Deard 7270(DC)	9
1.2 Insta	tianol Quartiew of the Front Danal Elements	10
1.3 Fund 131 R	eset Button	10
1.3.2 S	tatus LEDs (TC / ERROR /Operation)	10
1.3.3 U	SB-Port (Host)	11
1.3.4 L	AN Interface ETH0/ETH1	11
1.3.4.1	MAC-Address for ETH0/ETH1	11
2 Function	on Principle	12
3 Board	Behaviour	13
3.1 Boot	Phase	13
3.2 Reg	Ilating Phase	13
3.2.1 N	TP Adjustment Phase (NTP/Stratum/Accuracy)	13
3.2.2 P	TP Adjustment Phase	13
3.3 Rese	et Button	13
3.4 Firm	ware Update	14
3.5 Activ	ation of Functions by Activation Keys	16
4 Commi	ssioning	17
4.1 Gen	eral Procedure	17
4.2 Swite	ching on the Operating Voltage	18
4.3 Esta	blish the Network Connection via Web Browser	18
4.4 Netv	ork Configuration for ETH0 via LAN through <i>hmc</i>	18
5 HTTP V	VebGUI – Web Browser Configuration Interface	22
5 HTTP V 5.1 Quid	VebGUI – Web Browser Configuration Interface	22 22
5 HTTP V 5.1 Quic 5.1.1 R	VebGUI – Web Browser Configuration Interface k Configuration equirements	22 22 22
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps	22 22 22 22
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen	VebGUI – Web Browser Configuration Interface	22 22 22 22 23
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L	VebGUI – Web Browser Configuration Interface	22 22 22 22 23 23 24
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 F	VebGUI – Web Browser Configuration Interface	22 22 22 23 23 24 25 26
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E	VebGUI – Web Browser Configuration Interface	 22 22 22 23 24 25 26 27
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G	VebGUI – Web Browser Configuration Interface	22 22 22 23 24 25 26 27 27
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 C 5.3.2 T	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab	22 22 22 23 24 25 26 27 27 29
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2.1	VebGUI – Web Browser Configuration Interface	22 22 22 23 24 25 26 27 27 29 29
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2.1 5.3.2.2	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface inter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Davlight Saving Time)	22 22 22 23 24 25 26 27 27 29 30 31
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 Z 5.3.2 3 5.3.2 4	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncON / SyncOFF Timer	22 22 22 23 24 25 26 27 27 29 30 31 32
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2.2 5.3.2.3 5.3.2.4 5.3.2.5	VebGUI – Web Browser Configuration Interface	22 22 22 23 24 25 26 27 27 29 29 30 31 32 33
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2.1 5.3.2.1 5.3.2.3 5.3.2.4 5.3.2.6 5.3.2.6	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) Sync Source Errors Sync Status OC	22 22 22 23 24 25 26 27 29 29 30 31 32 33 34 25
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.3 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) Sync Source Errors Sync Status OC ETWORK Tab Host / Name Service	22 22 22 23 24 25 26 27 29 20 31 32 33 34 35 35
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.3 E 5.3 Desc 5.3.1 C 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.3 S	VebGUI – Web Browser Configuration Interface	22 22 22 23 24 25 26 27 27 29 30 31 22 33 34 35 35 37
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2.1 5.3.2.2 5.3.2.4 5.3.2.6 5.3.3 N 5.3.3 N 5.3.3 1 5.3.3 2 5.3.3 N	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncON / SyncOFF Timer Sync Source Errors Sync Status OC ETWORK Tab Host / Name Service Network Interface ETH0/ETH1 Network Interface Bonding/Teaming (Activation Key necessary)	22 22 22 23 24 25 26 27 27 29 30 31 32 33 34 35 37 41
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.3 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S 5.3.5 S	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface niter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) Sync ON / SyncOFF Timer Sync Source Errors Sync Status OC ETWORK Tab Host / Name Service Network Interface ETH0/ETH1 Network Interface PRP (Activation Key necessary) Network Interface PRP (Activation Key necessary) Routing (Activation Key necessary)	22 222 222 23 24 25 26 27 29 20 31 32 33 34 35 37 41 46
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 C 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.3 N 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 S 5.3.5 S	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncON / SyncOFF Timer Sync Source Errors Sync Status OC ETWORK Tab Host / Name Service Network Interface Bonding/Teaming (Activation Key necessary) Network Interface PRP (Activation Key necessary) Network Interface PRP (Activation Key necessary) Routing File	22 222 222 232 24 25 26 27 29 29 30 31 32 33 34 35 37 41 46 950
5 HTTP V 5.1 Quid 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.3 N 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 S 5.3.3 G 5.3.3 T	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface net or Changing Data cription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date. Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncON / SyncOFF Timer Sync Status OC ETWORK Tab Host / Name Service Network Interface ETH0/ETH1 Network Interface Bonding/Teaming (Activation Key necessary) Network Interface PRP (Activation Key necessary) Routing (Activation Key necessary) Routing File Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)	22 222 222 232 24 25 26 27 29 29 30 31 32 33 34 35 35 37 41 46 951
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 T 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 S 5.3.5 S	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data .rription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncoN / SyncOFF Timer Sync Source Errors Sync Status OC ETWORK Tab Host / Name Service Network Interface ETH0/ETH1 Network Interface PRP (Activation Key necessary) Network Interface PRP (Activation Key necessary) Routing (Activation Key necessary) Routing File Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.) TP Tab Suptom Info	22 22 22 23 24 25 26 27 29 30 31 32 33 34 46 9 501 51 4 50 51 4 50 51 4 50 51 4 50 51 51 51 51 51 51 51 51 51 51 51 51 51
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.3 E 5.3 Desc 5.3.1 C 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.2 S 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 S	VebGUI – Web Browser Configuration Interface equirements. onfiguration Steps. eral – Introduction. OGIN and LOGOUT as User avigation via the Web Interface net or Changing Data rription of the Tabs ENERAL Tab ime/Date Tab Set Time/Date Time Zone Offset Configuration of Summer Time (Daylight Saving Time) SyncON / SyncOFF Timer Sync Source Errors. Sync Source Errors. Sync Status OC ETWORK Tab. Host / Name Service. Network Interface ETH0/ETH1 Network Interface PRP (Activation Key necessary) Network Interface PRP (Activation Key necessary) Routing (Activation Key necessary) Routing File. Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.). TP Tab System Info Kernel Info	22 22 22 23 24 25 27 29 23 31 23 34 35 35 37 14 64 9 51 54 55
5 HTTP V 5.1 Quic 5.1.1 R 5.1.2 C 5.2 Gen 5.2.1 L 5.2.2 N 5.2.3 E 5.3 Desc 5.3.1 G 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 T 5.3.2 S 5.3.2 T 5.3.2 S 5.3.2 S 5.3.3 N 5.3.3 N 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 S 5.3.3 N 5.3.3 N	VebGUI – Web Browser Configuration Interface k Configuration equirements onfiguration Steps eral – Introduction OGIN and LOGOUT as User avigation via the Web Interface nter or Changing Data	22 222 222 232 242 252 272 292 301 322 333 342 3537 46 495 51 54 5555

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.4.5	Extended Configuration	57
5.3.4.6	Restart NTP	60
5.3.4.7	Access Restrictions / Configuring the NTP Service Restrictions	60
5.3.4.8	Symmetric Key	65
5.3.4.9	Autokey / Public Key Cryptography	66
5.3.5 P	TP Tab	67
5.3.5.1	PTP Configuration	68
5.3.5.2	PTP IEEE C37.238 Power Profile Settings	69
5.3.5.3	PTP Status	71
5.3.6 A	_ARM Tab	72
5.3.6.1	Syslog Configuration (Activation Key necessary)	
5.3.6.2	E-mail Configuration (Activation Key necessary)	
5.3.6.3	SNMP Configuration / TRAP Configuration (Activation Key necessary)	
5.3.6.4	Alarm Messages (Activation Key necessary)	
5.3.7 D		
5.3.7.1	Device Information	
0.3.7.Z	Halowale Information	
5.3.7.3	Residing Factory-Settings (Factory Delauits)	
5375	Image I Indate & H8 Firmware I Indate	
5376	Unload Certificate (SSI -Server-Certificate)	80
5377	Customized Security Banner	
5.3.7.8	Product Activation	
5.3.7.9	Diagnostics Function	
5.3.7.10) Passwords Master / Device	83
5.3.7.1	1 Downloading SNMP MIB / Configuration Files	84
5.3.8 O	UTPUT Tab	85
5.3.8.1	DCF77	85
5.3.8.2	Serial Interface	87
6 SSH an		105
	d Telnet Basic Configuration	1117
7 Technic	d Telnet Basic Configuration	105
7 Technic	d Telnet Basic Configuration	
7 Technic 8 Factory	d Telnet Basic Configuration al Data Defaults	105 106 108
7 Technic 8 Factory 8.1 Netw	d Telnet Basic Configuration al Data Defaults ork	105 106 108
7 Technic 8 Factory 8.1 Netw 8.2 NTP	d Telnet Basic Configuration al Data Defaults ork	105 106 108
7 Technic 8 Factory 8.1 Netw 8.2 NTP	d Telnet Basic Configuration al Data Defaults ork	105 106 108 108
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP	d Telnet Basic Configuration al Data Defaults ork	103 106 108 108 109 109 109
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF	d Telnet Basic Configuration al Data Defaults ork	103 106 108 108 109 109 110
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI	d Telnet Basic Configuration al Data Defaults ork CE	103 106 108 108 109 109 110 110
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF	d Telnet Basic Configuration al Data Defaults ork RM CE	105 106 108 109 109 110 110 110
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria	d Telnet Basic Configuration al Data Defaults ork RM CE 77 - 01 Unterface - 01	105 106 108 109 109 110 110 110 110 110
7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria	d Telnet Basic Configuration al Data Defaults ork RM CE 77 - 01 I Interface - 01	103 106 108 108 109 109 109 109 109 110 110 110 110 110
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 	d Telnet Basic Configuration eal Data Defaults ork RM CE 77 - 01 I Interface - 01 ry and Abbreviations	103 106 108 109 109 109 110 110 110 110 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 	d Telnet Basic Configuration eal Data Defaults ork RM CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology	105 106 108 109 109 110 110 110 110 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 	d Telnet Basic Configuration eal Data Defaults ork RM CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology Codes (NTP-specific)	105 106 108 109 109 110 110 110 110 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2.1 Ti 	d Telnet Basic Configuration eal Data Defaults ork RM CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology Codes (NTP-specific) me-specific expressions	105 106 108 109 109 109 110 110 110 111 111 111 112
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2.1 Ti 9.3 Abbr 	d Telnet Basic Configuration eal Data Defaults ork RM CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology Codes (NTP-specific) me-specific expressions	105 106 108 109 109 109 110 110 110 111 111 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2.1 Ti 9.3 Abbr 0.4 Definition 	d Telnet Basic Configuration	105 106 108 109 109 109 110 110 110 111 111 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2.1 Ti 9.3 Abbre 9.4 Defin 	d Telnet Basic Configuration	105 106 108 109 109 109 110 110 110 111 111 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.4 Defin 9.4 D 	d Telnet Basic Configuration	105 106 108 109 109 109 110 110 110 110 111 111 111 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.4 Defin 9.4.1 D 9.4.2 N 	d Telnet Basic Configuration al Data Defaults ork RM CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology Codes (NTP-specific)	105 106 108 109 109 109 109 109 109 109 109 109 100 110 110 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.4 Defin 9.4 Defin 9.4.1 D 9.4.2 N 9.4.3 S 	d Telnet Basic Configuration cal Data Defaults ork M CE 77 - 01 I Interface - 01 y and Abbreviations specific Terminology Codes (NTP-specific) me-specific expressions eviations HCP (Dynamic Host Configuration Protocol) TP (Network Time Protocol) MMP (Simple Network Management Protocol)	105 106 108 109 109 109 109 109 109 109 109 109 109 109 110 110 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.4 Defin 9.4 Defin 9.4.1 D 9.4.2 N 9.4.3 SI 9.4.4 To 	d Telnet Basic Configuration cal Data Defaults	105 106 108 109 109 109 109 109 109 109 109 109 110 110 111 114 115 115
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2 Tally 9.2 Tally 9.2 Tally 9.4 Defin 9.4 Defin 9.4.1 D 9.4.2 N 9.4.3 SI 9.4.4 To 9.5 Accu 	d Telnet Basic Configuration cal Data Defaults ork CE 	105 106 108 109 109 109 109 109 109 109 109 109 109 109 110 110 111
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.2.1 Ti 9.3 Abbro 9.4 Defin 9.4.1 D 9.4.2 N 9.4.3 SI 9.4.4 To 9.5 Accu 	d Telnet Basic Configuration cal Data	105 106 108 109 109 109 110 110 110 110 110 111 1
 7 Technic 8 Factory 8.1 Netw 8.2 NTP 8.3 PTP 8.4 ALAF 8.5 DEVI 8.6 DCF 8.7 Seria 9 Glossar 9.1 NTP- 9.2 Tally 9.4 Tolly 9.5 Accu 	d Telnet Basic Configuration cal Data	105 106 108 109 109 109 109 109 110 110 110 110 111 1



1 Description of the Board

The Board 7279(RC) is a **Network Time Client** (*abbreviation* NTC) for the integration into the modular *hopf* Clock Systems 7001RC, 7001, 6844, 6844RC and 6855.

The board is equipped with two Ethernet interfaces (ETH0/ETH1) 10/100/1000 Base-T (auto-sensing).

The Board 7279(RC) is synchronized with the **UTC time** by the worldwide used time **NTP** (Network Time Protocol) via one or more NTP Time Servers. The board can either be synchronized by a **NTP Timer Server** but also by a **SNTP Time Server**, if needed. However, this usually results in a considerably limited accuracy of the time information.

For high-precision network synchronization, the Board 7279(RC) can synchronize with the **PTP time protocol according to IEEE Std 1588** [™] **-2008**. For this, however, the corresponding network topology must be guaranteed.

The time basis of the board synchronized via network is converted into a format that allows the synchronization of further *hopf* devices and components.

The **status** of the board is indicated via three LEDs in the front panel. This allows an easy identification of the current operation status or any fault.

The Board 7279(RC) offers a **broad range of functions**. Some of the practice-oriented functionalities are for example:

Complete parameterisation via protected WebGUI access

All required settings for operation can be executed via a password protected WebGUI, also giving an overview of the status of the Board 7279(RC).

• Automatic handling of the leap second

Should a leap second in the UTC time be announced by the Time Server, this is recognized by the Board 7279(RC) and the leap second will automatically be inserted into the time information.

• Superior Security

A superior security is guaranteed via available coding procedures such as symmetric keys, autokey and access restrictions and deactivation of non-used protocols.

Management and Monitoring Functions

Different functions are available for this purpose (e.g. SNMP, SNMP-Traps, E-mail notification, Syslog-messages including MIB II and private Enterprise MIB).

A few other basic functions of the Board 7279(RC):

- Easy operation via **WebGUI**
- Status LEDs on the front panel
- Completely maintenance-free system

Software supplied:

• *hmc* (*hopf* Management Console) Software



Overview of the functions of the Board 7279(RC):

Two Ethernet Interfaces

- Auto negotiate
- 10 Mbps half-/full duplex
- 100 Mbps half-/full duplex
- 1 Gbps full duplex

Time Protocols

- RFC-5905 NTPv4 Server
 - o NTP Broadcast Mode
 - NTP Multicast Mode
 - NTP Client for additional NTP Servers (redundancy)
 - o SNTP Server
 - NTP Symmetric Key Encryption
 - o NTP Autokey Encryption
 - NTP Access Restrictions
- Precision Time Protocol (PTP) according to IEEE Std 1588[™]-2008 (Activation Key necessary)
 - IEEE standard profile for using IEEE 1588[™] Precision Time Protocol in Power System applications (Power Profile) according to IEEE Std C37.238[™]-2011

Network Configuration (Activation Key necessary)

- Routing
- Bonding (NIC Teaming) Link aggregation according to IEEE 802.1ad
- VLAN support according to IEEE 802.1q
- PRP (Parallel Redundancy Protocol) according to IEC62439-3

System Management (Activation Key necessary)

- E-mail notification
- Syslog messages to external syslog server
- SNMPv2c/v3, SNMP Traps (MIB II, Private Enterprise MIB)

Configuration Channel

- HTTP WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool (*hmc* Network-Configuration-Assistant)

Additional Features

- Firmware Update via TCP/IP
- Failsafe
- Watchdog circuit
- Customizable security banner
- NTP local time support



1.1 Front Panel





1.1.2 Front Panel of Board 7279 for 1U / 19" Racks (Slim Line)

Board 7274/1U - 1U (Slim Line)





1.2 Installation and Removal of the Board 7279(RC)

The board is supplied with power via an internal plug-in connection that also provides the output of the time information based on NTP and the system reset if any.

For service and repair purposes the module can be removed from the device.



Board 7279 (without RC) does not support HOT-PLUG

In case an installation or removal of the board should be necessary the device in which the module is integrated must be disconnected from power.

1.3 Functional Overview of the Front Panel Elements

This chapter describes the individual front panel elements and their functions.

1.3.1 Reset Button



The Reset Button is accessible with a thin object through the small drilling in the front panel next to the "Reset" inscription" (see *Chapter 3.3 Reset Button*).

1.3.2 Status LEDs (TC / ERROR /Operation)



TC-LED (Green)	Time service of the Board 7279(RC)	
On	Standard, running	
Off	Not or partially not running	
ERROR-LED (Red)	Description	
Off	Standard case , Board 7279(RC) is working.	
3Hz flashing	Fail-safe basic parameterization is not available (emergency operation mode)	
On	Primary CPU of Board 7279(RC) does not show any activity.	
Operation-LED (Green)	Description	
On	Standard case, Board 7279(RC) is working	
1Hz flashing	Board 7279(RC) is booting the operating system.	
3Hz flashing	A firmware update (image) of Board 7279(RC) is being implemented.	
Off	Board 7279(RC) is not ready for operation.	



11 / 125

1.3.3 USB-Port (Host)



In case of specific problems the USB connection can be used for a system recovery after consulting the *hopf* Support.

1.3.4 LAN Interface ETH0/ETH1



LNK LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit / 1 GBit Ethernet detected
[
SPD LED (Yellow)	Description
Off	No LAN connection to a network
On	LAN connection available
Flashes	Network activity (transmission / recep- tion)
Pin No.	Assignment
1	TX_DA+
2	TX DA-

1	TX_DA+
2	TX_DA-
3	RX_DB+
4	BI_DC+
5	BI_DC-
6	RX_DB-
7	BI_DD+
8	BI_DD-

1.3.4.1 MAC-Address for ETH0/ETH1

Each LAN interface is clearly identifiable on the Ethernet via a unique MAC Address (hardware address).

The MAC addresses given for the LAN interfaces can be read in the WebGUI of the appropriate board or can be evaluated via the *hmc* Network Configuration Assistant.

The MAC address for ETH1 is set hexadecimally plus 1 to the MAC address of ETH0.

Example:

- MAC address ETH0 = 00:03:C7:12:34:59
- MAC address ETH1 = 00:03:C7:12:34:5A

The MAC address is uniquely assigned for each LAN interface by the company *hopf* Elektronik GmbH.



The factory set MAC address for the Board 7279(RC) is stated on a sticker directly placed on the board.



hopf Elektronik GmbH MAC addresses begin with **00:03:C7**:xx:xx:xx.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



2 Function Principle

This chapter describes the functional principle of the Board 7279(RC) and the internal relations between the individual function groups.

The Board 7279(RC) is a multi-processor system.

The structure allows the following mode of operation:

The NTP/PTP service on the board is synchronized by a NTP/PTP Server via the network. With this time information the internal time basis of the board is synchronized with high precision. The time is then transformed into outputs with time information allowing further processing in the respective clock system.





3 Board Behaviour

This chapter describes the behaviour of the board in special operational phases and conditions.

3.1 Boot Phase

The boot process of the Board 7279(RC) starts after switching on the system or a reset.

During the boot process the Board 7279(RC) boots its operation system and is therefore not available via LAN.

The end of the boot process is reached when the LED test of the Status-LEDs in the front panel has been finished.



Boot phase takes approx. 35 seconds by using static IP-addresses for ETH0 and ETH1. Boot phase can be extended, depending on the network configuration in use (e.g. DHCP).

3.2 Regulating Phase

After the boot phase, the NTP or PTP service is started automatically depending on the configuration of the board.

After starting the NTP/PTP service, the board will take about 5-10 minutes, depending on the accuracy and availability of the time servers configured in the card, to regulate the internal clock.

3.2.1 NTP Adjustment Phase (NTP/Stratum/Accuracy)

NTP is a regulation process. When the NTP service is activated, it automatically starts in the boot phase. After starting, the board will take about 5-10 minutes, depending on the accuracy and accessibility of the configured NTP server in the board.

After a successful adoption of time by the NTP Server the module usually takes on a Stratum value one plus than the respective NTP Server (e.g. Server = Stratum 1 \Rightarrow Stratum of the Board 7279(RC) = 2).

For an output of time via the module the NTP service needs to be regulated to an accuracy value = HIGH. The duration of the regulation process depends on factors such as accessibility and accuracy of the respective NTP Server (System Peer).

3.2.2 PTP Adjustment Phase

When the PTP service is activated it automatically starts in the boot phase. After starting the board will take about 5-10 minutes, depending on the accuracy and accessibility of the PTP-Grandmasters.

For an output of time via the board the PTP service needs to be regulated to an accuracy value = HIGH. The duration of the regulation process depends on factors such as accessibility and accuracy of the respective PTP Grandmaster.

3.3 Reset Button

The Board 7279(RC) can be reset by the Reset-(Default) Button behind the front panel of the board. The Reset-(Default) Button is accessible with a thin object through the small drilling in the front panel.



After a FACTORY DEFAULT, the settings of Board 7279 (RC) must be checked (see *Chapter* 5.3.7.3 Restoring Factory-Settings (Factory Defaults).)

The button triggers different functions depending on how long it is pressed:

Duration	Function
< 1 sec.	No action
1 - 9 sec.	After releasing a hardware reset on the board will be initiated
>= 10 sec.	After releasing a FACTORY DEFAULT followed by a REBOOT will be initiated after approx. 10 seconds

3.4 Firmware Update

The Board 7279(RC) is a multi-processor system. For this reason a firmware update always consists of a so called Software SET. This software set includes two (2) program releases, defined by the SET version.

Board 7279(RC):

1x Image Update	upgrade_8030gen_rel_vXXXX.img
1x H8 Update	H8_8030NTC_vXXXX_128.mot



An update is a critical process. The device must not be turned off during the update and the network connection to the device may not be interrupted.



All programs of a SET need to be uploaded to ensure a defined operating status.



The information about program releases assigned to a SET version can be found in the release notes of the software SETs of the Board 7279(RC).

The general process of a software update of Board 7279(RC) is described below:



For selection of the correct update set please ensure the correct identification code <u>7279(RC)</u>.

7279(RC) can be found:

- on the label on the housing cover "7279(RC)"
- in WebGUI at the web-banner "7279(RC)"



The firmware update 7279(RC) has to be carried out as a SET.

The software package contained in the file package hopf7279 _GPS_SET_vXXXX.zip has to be unpacked. The following steps have to be executed in the following sequence:

- 1. Image Update
- 2. H8 Firmware Update

Image Update

- 1. Log in as Master in WebGUI of the board.
- 2. Select in **Device** tab the menu item **Image Update**.
- 3. Select the file with the file **.img** via the selection window (Example: **upgrade_8030gen_rel_vXXXX.img**).
- 4. The selected file is shown in the selection window.
- 5. The update process is started with the button **Upload now**.
- 6. In WebGUI the successful file transfer and writing to the board is indicated.
- 7. In WebGUI the successful update is indicated after 2-3 minutes with the request to release a reboot of the board.
- 8. After activation and successful reboot of the board the image update process is finished.

H8 Firmware Update

- 1. Log in as Master in WebGUI of the board.
- 2. Select in the **Device** tab the menu item **H8 Firmware Update**.
- Select the file with the extension .mot via the selection window (Example: H8_7279_vXXXX_128.mot).
- 4. The selected file is shown in the selection window.
- 5. The update process is started with the button **Upload now**.
- 6. In WebGUI the successful file transfer to the board is indicated.
- 7. Now the update of the board automatically starts after a few seconds.
- 8. After successful update the board automatically reboots.
- 9. After approx. 2 minutes the H8 update process is finished and the board is again accessible via WebGUI.



3.5 Activation of Functions by Activation Keys

Currently the Board 7279(RC) offers some functions that require an "Activation Key".

These functions are only available after entering a valid activation key related to the serial number of the Board 7279(RC) (not the serial number of the overall system). The serial number can be found in the WebGUI via Device / Serial Number: 8030xxxxxx.

The activation of such function(s) can be done by default and also later on-site by the user if required.



Activation keys can be entered and displayed in the tab "Device" under the menu item "Product Activation".

Please find an overview of the above mentioned functions here:

IEEE 1588 Precision Time Protocol (PTP)

By activating this function, the PTP time datagram can be parameterized and enabled via the LAN interface for synchronization.

<u>Network interface Bonding/Teaming</u>

By activating this function, the LAN interfaces ETH0 and ETH1 can be bundled to a logical network interface. This feature plays a key role in redundantly structured networks to increase fail-safety of the NTP time service.

IEEE 802.1QTagged VLAN

By activating this function network interfaces can be configured with additional VLANs (Virtual Bridged Local Area Networks) according to IEEE 802.1q.

<u>Static Routing Tables</u>

This function is suitable for configuring static routes based on special network configuration requirements in the Board 7279(RC).

• IEC 62439-3 Parallel Redundancy Protocol (PRP)

The PRP functionality enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface using the Parallel Redundancy Protocol (PRP).

<u>Alarming and Management features</u>

This function enables to use **SNMP** (<u>SNMPv2c, SNMPv3</u>), <u>Syslog and Email notifi-</u> <u>cation</u> to monitor the system status. Together with the assets provided in the MIB II by default, the *hopf* Private Enterprise MIB is also made available. By using the *hopf* Private Enterprise MIB numerous product-specific assets for realizing extended management and control functions are available.



The settings for activation keys (e.g. an entered activation key) are neither modified nor influenced by the functions FACTORY DEFAULTS.



4 Commissioning

This chapter describes commissioning of the Board 7279(RC).

4.1 General Procedure

Overview of the general commissioning procedure:

- Finish the installation process completely
- Switch on the device
- Wait until the booting phase is finished (see Chapter 3.1 Boot Phase)
- Use the SEARCH function of the *hmc* Software (Network Configuration Assistant) in order to access the Board 7279(RC) and set the basis LAN parameters (e.g. DHCP). Afterwards connect to the WebGUI of the Board 7279(RC) via Web browser

OR

connect directly with the factory default IP-address (ETH0 = 192.168.0.1 or ETH1 = DHCP) to the WebGUI via a Web browser

- Log in as "master"
- Change default passwords for "master" and "device" In the DEVICE tab
- Set all required LAN parameters (e.g. entry of DNS server) in NETWORK tab if necessary
- Check current settings in **NTP tab** and modify according to individual needs as necessary (e.g. entry of the NTP Time Server used for synchronization)
- Parameterize optional functions e.g. SNMP if necessary
- If all base settings are carried out correctly and the NTP Time Server supplies the time information with the appropriate accuracy, the **GENERAL** tab should look like this after approx. 30 min. (usually considerably faster):

				© 2005-201	7 rdcs.eu	
General Time/Date	Network	NTP	РТР	Alarm	Device	Output
evice Time		Time Client Statu	5	Annoi	uncements	
DATE TIME) STD	SYNCHRONIZ	ZATION	LEA	P SECOND inactive	STD ⇔ DST
JTC 13.02.2018 09:10:30	0	ACCURACY				
ogin				NTP S	ystem Info	
Jsername				sys 192	тем реек 2.168.180.	103
Password				STA 0.0	BILITY 13 ppm	
Login				STR	атим 2	
Jser is not logged in.				LAM 3.0	IBDA 67 ms	



4.2 Switching on the Operating Voltage

The Board 7279(RC) has no own switch for the power supply. The board is activated by switching on the device in which it is integrated.

4.3 Establish the Network Connection via Web Browser



Ensure that the network parameters of the Board 7279(RC) are configured in accordance with the local network before connecting the device to the network.



Connecting a network to an incorrectly configured Board 7279(RC) (e.g. duplicate IP address) may cause interference on the network.



The Board 7279(RC) is supplied with:

-address
192.168.0.1
255.255.255.0
not set

ETH1 with DHCP



In case you do not know if Board 7279(RC) with its Factory Default setting causes problems in the network, the basis network parameterization should be executed via a "Peer to Peer" network connection.



Request the required network parameters from your network administrator if those are unknown.

The network connection is made via a LAN cable and RJ45 plug (recommended cable type: CAT5 or better).

4.4 Network Configuration for ETH0 via LAN through *hmc*

After connecting the system to the power supply and creating the physical network connection with the LAN interface of Board 7279(RC), the device can be searched on the network via the hmc (hopf Management Console). Consequently the basic LAN parameters (IP address, netmask and gateway or DHCP) may be adjusted in order to allow accessibility of the Board 7279(RC) for other systems on the network.



For locating and identifying Board 7279(RC) via the SEARCH Function of the *hmc* - Network Configuration Assistant it is required that both the *hmc*-computer and Board 7279(RC) are in the same SUB Net.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



The basic LAN parameters can be set via the *hmc* integrated **Network Configuration Assistant**.

File Device	s Tools Help
0 × 0	🕥 View DCF77 Record
	Network Configuration Assistant
-	NTP Analysis
	View GPS Record

After a successful start of the *hmc* Network Configuration Assistant and completed search of the *hopf* LAN devices, the configuration of the basic LAN parameters can be done.

The Board 7279(RC) is stated as 7279(RC) in the Device List.

Several Boards 7279(RC) (or other product variants) can be distinguished by their **Hardware Address** (MAC Address).



The factory set MAC address for the Board 7279(RC) is stated on a sticker laterally positioned on the device.

HMC Network Configuration Assist	ant	
Device List	Configuration	
7279RC	Device Type 7279RC Firmware Version	Host Name hopf7279RC Network Configuration Type
	04.00	Static IP Address 👻
	Hardware Address	IP Address
	00:03:C7:01:94:7E	192.168.180.135
	Serial Number	Netmask
	8030019007	255.255.252.0
	Bonding enabled	Gateway 192.168.180.1
		Apply
· · · · · ·	Set Device Password	Reset To Factory Defaults
Rescan Network	Set Master Password	
		Exit



For extended configuration of Board 7279(RC) through a browser via WebGUI the following basic LAN-parameters are required:

- Host Name
- Network Configuration Type
- IP Address
- Netmask
- Gateway

⇒ e.g. hopf7279

 \Rightarrow e.g. Static IP Address or DHCP

- ⇔ e.g. 192.168.0.4
- ⇔ e.g. 255.255.255.0
- ⇒ e.g. 0.0.0.0

The hostname must meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.' . No distinction is made between capital letters and lowercase letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.



The network parameters being assigned should be pre-determined with the network administrator in order to avoid problems on the network (e.g. duplicate IP address).

IP Address (IPv4)

An IP address is a 32 bit value divided into four 8 bit numbers. The standard presentation is 4 decimal numbers (in the range 0...255) separated from each other by dots (dotted quad notation).

Example: 192.002.001.123

The IP address consists of a leading network ID followed by the host ID. Four common network classes were defined in order to cover different requirements. Depending on the network class, the last one, two or three bytes define the host while the rest define the network (network ID) in each case.

In the following text the "x" stands for the host part of the IP address.

Class A Networks

IP addresses 001.xxx.xxx to 127.xxx.xxx

There is a maximum of 127 different networks in this class. This allows the possibility to connect a very high number of devices (max. 16.777.216)

Example: 100.000.000.001, (Network 100, Host 000.000.001)

Class B Networks

hopf Elektronik GmbH

IP addresses 128.000.xxx.xxx to 191.255.xxx.xxx

Each of these networks can consist of up to 65534 devices.

Example: 172.001.003.002 (Network 172.001, Host 003.002)



Class C Networks

IP addresses 192.000.000.xx to 223.255.255.xxx

These network addresses are the most commonly used. Up to 254 devices can be connected.

Class D Networks

The addresses from 224.xxx.xxx - 239.xxx.xxx are used as multicast addresses.

Class E Networks

The addresses from 240.xxx.xxx.xxx - 254.xxx.xxx are designated as "Class E" and are reserved.

Gateway Address

The gateway or router address is required in order to be able to communicate with other network segments. The standard gateway must be set to the router address which connects these segments. This address must be within the local network.

After entering the above mentioned LAN parameters, they need to be transferred to the Board 7279(RC) via the **Apply** button. Afterwards the entry of the **Device Password** is requested:

Device Pas	ssword	
l		
ОК	Cancel	

The Board 7279(RC) is supplied with the default device password $\langle device \rangle$ on delivery. After entry click on the OK button to confirm.

The LAN parameters thus set are directly adopted (without reboot) by the Board 7279(RC) and are immediately active.



5 HTTP WebGUI – Web Browser Configuration Interface



For correct displaying and the correct function of the WebGUI, JavaScript and Cookies must be activated in the browser.

5.1 Quick Configuration

This chapter gives a brief description of the basic operation of the WebGUI installed on the board.

5.1.1 Requirements

- Board 7279(RC) must be ready for operation
- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Board 7279(RC)

5.1.2 Configuration Steps

- Create the connection to the Time Client with a web browser
- Login as a 'master' user (default password <master> is set by delivery)
- Switch to "Network" tab if available and enter the DNS Server (required for NTP and the alarm messages depending of network)
- Save the configuration
- Switch to "Device" tab and restart Network Time Client via "Reboot Device"
- NTP Service is now available with the standard settings
- NTP specified settings can be done in the "NTP" tab (e.g. entry of the NTP Time Server used for synchronization).
- Alarm messages via Syslog/SNMP/Email can be configured in "Alarm" tab only if this function is enabled by an activation key



The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.



5.2 General – Introduction

The Board 7279(RC) should be accessible to a web browser if it has been set up correctly. Enter the IP address - as set up in the Board 7279(RC) earlier - or the DNS name on the address line <<u>http://xxx.xxx.xxx</u>> and the following screen should appear.

When using IPv6, it is mandatory to enclose the IPv6 address with [], for example: http://[2001:0db8:85a3:08d3::0370:7344]/



General Time/Date	Network	NTP	РТР	Alarm	Device	Output	
evice Time		Time Client Stat	us	Annou	ncements		
DATE TIME LOC 13.02.2018 11:45:36 JTC 13.02.2018 10:45:36	5 STD	SYNCHRONI ON ACCURACY HIGH	ZATION		P SECOND nactive	STD ⇔ DST	
Jsername Password Login Jser is not logged in.				NTPS SYS 192 STA 0.0 STR LAM 2.3	ystem Info TEM PEER 168.180.1 BILITY 09 ppm ATUM 2 BDA 35 ms	.03	



The WebGUI was developed for multi-user read access, but not for multiuser write access. It is the responsibility of the user to pay attention to this issue.



24 / 125

5.2.1 LOGIN and LOGOUT as User

All of the board's data can be read without being logged on as a special user. However, the configuration and modification of settings and data can only be carried out by an authorised user! Two types of user are defined:

- "master" user (default password on delivery: <master>)
- "device" user (default password on delivery: <device>)



Due to security reasons the password should be changed after the first login.



The password must be between 6 and 20 characters long, contain at least one uppercase letter, one lowercase letter and one digit!



Differentiation is made between **capital letters and lower-case** characters in the password. Alphanumeric characters and the following symbols can be used: []()*-_!\$% & / = ?

The following screen should be visible after logging in as a "master" user:

General Time/Date	Network	NTP	РТР	Alarm	Device	Output	
Device Time		Time Client Stat	tus	Annou	incements		
DATE TIME LOC 13.02.2018 11:48:00 9 UTC 13.02.2018 10:48:00	STD	SYNCHRON	IZATION		P SECOND nactive	STD ⇔ DST	
ogin User master is logged in since 10:47:58 UTC.				NTP Sys SYST 192.	stem Info EM PEER 168.180.10	3	
Logout				STAB 0.00	ILITY 9 ppm		
				STRA	тим		
					BDA 8 mg		

Click on the Logout button to log out.

The WebGUI is equipped with a session management. If the user does not conduct a logout, the logout is automatically made after 10 minutes of inactivity (idle time).

After successful login, depending on the access level (device or master user), changes can be made to the configuration and saved.

Users logged in as "master" have all access rights to the Board 7279(RC).

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



Users logged in as "device" do not have access to:

- Trigger reboot
- Trigger factory defaults
- Carry out image update
- Carry out H8 firmware update
- Upload Certificate
- Change master password
- Diagnostics
- Download configuration files

5.2.2 Navigation via the Web Interface

The WebGUI is divided into functional tabs. Click on one of these tabs to navigate through the board. The selected tab is identified by a darker background colour - see the following image (General in this case).

	opf	24 23 22 21 28 19 NETWORK T	IME CLIENT	7279RC	07 06 05 04 0				
ER	Ktronik — GmbH			/// •		© 2005-201	17 rdcs.eu		
	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output	V Z

User login is not required in order to navigate through the board configuration options.



JavaScript and Cookies should be enabled in the browser in order to guarantee the correct operation of the web interface.

E		24 23 22 21 NETWO
	General	Time/Da
	Host Settings	
	Host/Nameserv Network Interfa ETH0 Network Interfa Bonding/Teamin Network Interfa PRP Routing Routing File	

All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.



5.2.3 Enter or Changing Data

It is necessary to be logged on as one of the users described above in order to enter or change data.

All changeable data is saved in Board 7279(RC). For these data transfer of values is divided into two steps.

For a permanent saving the modified value <u>must</u> first be accepted with **Apply** from the board and then be stored with **Save**. Otherwise the modifications get lost after a reboot of the board or switching the system off.

	General	Time/Date	Network	NTP	PTP	Alarm	Device	Output	V Z D
_									
-	Host Settings		Host/Nameservice						
	Host/Nameserv	ice	Hostname hopf7279RC		Г				
	ETHO		Use Manual DNS Entries		_				
	ETH1	ice	enabled V						
	<u>Network Interfa</u> Bonding/Teami	ng	DNS Server 1 IPv4/IPv6	Address					
	<u>Network Interfa</u> <u>PRP</u>	ice	DNS Server 2 IPv4/IPv6	Address	7				
	Routing Routing File								
	Routing File		DNS Server 3 IPv4/IPv6	Address	7				
ſ	Protocols				_				

After an entry made with **Apply**, the configured field is marked with a star '*'. This means that a value has been entered or changed but not yet been stored in the flash memory.



Meaning of the symbols from left to right:

No.	Symbol	Description
1	Apply	Acceptance of changes and entered data
2	Reload	Restoring the saved data
3	Save	Fail-save storage of the data in the flash configuration

If the data should only be tested, it is sufficient to accept the changes with Apply.



Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.

However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data permanently with **Save**.



For adopting changes and entering values only the respective buttons in the WebGUI can be used.



5.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Time/Date
- Network
- NTP
- PTP
- Alarm
- Device

5.3.1 GENERAL Tab

This is the first tab which is displayed when using the web interface. This shows the current time and the synchronization status of Board 7279(RC). Furthermore logging in via this tab is possible (enter username and password), which is necessary to configure the Board 7279(RC) via WebGUI.

				© 2005-201	7 rdcs.eu		
General Time/Date	Network	NTP	PTP	Alarm	Device	Output	₹
Device Time		Time Client Status	;	Annou	incements		
DATE TIME		SYNCHRONIZ	ATION				
	CTD				PSECOND	510 0 051	
LOC 13.02.2018 11:45:36	SID			I I I	nactive	Inactive	
UTC 13.02.2018 10:45:36							
ogin				NTP S	ystem Info		
				SYS	TEM PEER		
Username				192	.168.180.10	03	
				STA	BILITY		
				0.0	09 ppm		
Password					••		
Password				STR	ATUM		
Login				STR.	АТUМ 2		
Login				STR.	ATUM 2 IBDA		

<u>Login</u>

The Login box is used in accordance with Chapter 5.2.1 LOGIN and LOGOUT as User

Device Time

This sector displays the current time and date of Board 7279(RC), used for the output of time information. This time corresponds with the UTC time (UTC) received by NTP and the resulting local time (LOC). The local time is created by the parameters configured under the tab Time/Date (see *Chapter 5.3.2 Time/Date Tab*). In addition to the local time the daylight saving time (DST) / and standard time (STD) is indicated.



Time Client Status

SYNCHRONIZATION

Indicates the synchronization status of the internal time output. This value describes whether connected components/devices can use the time information of Board 7279(RC) for their own synchronization.

- **ON:** The time information put out by board 7279(RC) can be used by connected components/devices for their own synchronization.
- **OFF:** The time information put out by board 7279(RC) <u>cannot</u> be used by connected components/devices for their own synchronization.

ACCURACY

The indication **ACCURACY** (accuracy of NTP/PTP) can include the possible values LOW - MEDIUM - HIGH. The meaning of those values is explained in *Chapter 9.5 Accuracy & NTP/PTP Basic* Principles.



By default, the accuracy must be at least HIGH so that the module supplies time information for synchronization. This value can be set by the user if required.

Announcements

LEAP SECOND

announcement for inserting a leap second

Inactive: No announcement exists

Active: There is an announcement. A leap second is inserted on the next hour.

STD ⇔ DST

Announcement for adjustment for daylight saving time / standard time

Inactive: No announcement exists

Active: There is an announcement. An adjustment for daylight saving time / standard time is made with the upcoming hour change.

NTP System Info (with activated NTP)

SYSTEM PEER

Indicates the currently used NTP Time Server for the synchronisation.

STABILITY

Indicates the current NTP stability value of Board 7279(RC) in ppm.

STRATUM

Indicates the current NTP stratum value of Board 7279(RC) in the value range of 1-16.



By default, the stratum value of the Board 7279(RC) is always one lower than the stratum of the SYSTEM PEER.

The Board 7279(RC) can only be synchronized on a SYSTEM PEER that it is at least **STRATUM 14 or better.**

LAMBDA

Indicates the current calculated NTP-LAMBDA value of Board 7279(RC) in milliseconds.



PTP System Info (with activated PTP)

PTP Grandmaster Identity

Displays the PTP Grandmaster currently used for synchronization.

PTP State

Indicates the synchronization state of the PTP service.

Master Offset

Displays the offset detected by board 7279(RC) to the PTP Grandmaster.

5.3.2 Time/Date Tab

Board 7279 (RC) basically works with the time base UTC. The configuration of difference time (**Time Zone Offset to UTC**) is required for calculating the local standard time (winter time).

5.3.2.1 Set Time/Date

Set the UTC time with date. Setting time and date with this function is not required if Board 7279 (RC) is already connected to a Network Time Server (NTP or PTP). This function can be used if no Network Time Server is available when commissioning the board 7279 (RC).

After input, these values are checked directly for plausibility by pressing the **Apply** button. Then time and date are set.



The UTC time must always be set. The local time is internally calculated from the difference time (Time Zone Offset) and the data of the summer / winter time changeover.

General	Time/Date	Netw	vork N	ТР	РТР	Alarm	Device	Output
Local Time Setting Set Time/Date Time Zone Offs Daylight Saving SyncON / SyncO	et Time DFF	Set UTC Time, Year (YYYY)	/Date Month (MM) Minute (mm)	Day (dd)	ss)			
Sync Status Sync Source Err Sync Status OC	rors							

- Year Enter the current UTC year (2000-2099)
- Month Enter the current UTC month (01-12)
- **Day** Enter the current UTC day (01-31)
- **Hour** Enter the current UTC hour (00-23)
- Minute Enter the current UTC minute (00-59)
- Second Enter the current UTC second (00-59)



The input must be complete and in the specified format.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.2.2 Time Zone Offset

Setting of the difference time (Time Zone Offset) from UTC to the local standard time (winter time).



The difference time to be entered <u>always</u> relates to **the local standard time (winter time)** even though the commissioning or rather the input of the difference time takes place during daylight saving time.

General Time/Date	Network	NTP	РТР	Alarm	Device	Output
Local Time Settings	Time Zone Offset to UT	C				
Set Time/Date Time Zone Offset	Offset Hours					
<u>Daylight Saving Time</u> <u>SyncON / SyncOFF</u>	Offset Minutes					
Sync Status	Direction east (+) V					
Sync Source Errors Sync Status OC						

- Offset Hours Time Zone Offset input of the full hour (0-13)
- Offset Minutes Time Zone Offset input of minutes (0-59)

Example:

Time Offset for Germany	\Rightarrow East, 1 hour and 0 minutes (+ 01:00)
Time Offset for Peru	\Rightarrow West, 5 hours and 0 minutes (- 05:00)

Direction relating to Prime Meridian - Direction of the Difference Time

Entering the direction the local time deviates from world time:

'East'	corresponds to east,
'West'	corresponds to west of the Prime-Meridian (Greenwich)



5.3.2.3 Configuration of Summer Time (Daylight Saving Time)

This input is used to define the point of time at which the changeover to Daylight Saving Time or winter time occurs during the course of the year. The hour, day of the week, week of the month and month at which the Daylight Saving Time begins and ends are determined.

So the exact times are automatically calculated for the current year.

	1	After the automati	turn of the cally recal	year th culated	ie chan d, witho	geover ti ut any us	imes for su ser interve	Immer/wintont	er time are
	General	Time/Dat	e Netw	ork	NTP	РТР	Alarm	Device	Output
Loc Se Tir Da	al Time Settings et Time/Date me Zone Offset aylight Saving T	ime	DST Activation Daylight Savin enabled V	ng Time					
Syr Syr	rncON / SyncOF	<u>5</u>	DST Begin Week last V	Day sunday	Mi V m	onth narch V	Hour Mir 2 0	ute	
	<u>Inc Status UC</u>		DST End Week	Day sunday	M. V 0	onth ctober V	Hour Min 3 0	ute	

- DST Activation (enabled/disabled) Changeover times for summer/winter time
- DST Begin Changeover time for standard time to Daylight Saving Time
- DST End Changeover time for Daylight Saving Time to standard time

The individual items mean the following:

Week	How often the changeover should be pro- cessed per day of the week in the month	First- 1st weekSecond- 2nd weekThird- 3th weekFourth- 4th weekLast- last week
Day	The day of the week when the changeover should be processed	Sunday, Monday … Saturday
Month	the month when the changeover should be processed	January, February December
Hour Minute	The time in hour and minute when the changeover should be processed	00h 23h 00min 59min

These data are entered on the basis of the local time.



5.3.2.4 SyncON / SyncOFF Timer

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
	Local Time Setting Set Time/Date Time Zone Offs Daylight Saving	gs et 1 Time	SyncON / SyncOFF Tin SyncON timer (0-30 n 0	ner nin)	Current Synco 0	DN timer value		
[SyncON / Synco	<u>OFF</u>	SyncOFF timer (2-144	10 min) nc Timer values	Current Synco	OFF timer value		
	<u>Sync Source Er</u> <u>Sync Status OC</u>	rors						

SyncON Timer

The SyncON Timer is used to delay the sync status "SYNC" by the configured time, despite synchronization with a Network Time Server.

This function will be activated when adjustment processes should be terminated as defined before reaching the sync status "SYNC".

This function is not required for this device and should always be set to 0.

SyncOFF Timer

This value is used to provide reception failure bypassing for an error-message free operation even under poor reception conditions.

In the event of a reception failure of the Sync Source (here PTP Grandmaster), the decrease of the Sync Source to '**QUARTZ**' status is delayed by the set value. The system continues to run in synchronization status on the internally regulated, highly accurate quartz base during this period with sync status '**SYOF**'.

This timer is of special significance when certain system outputs are linked to a specific system status.

The Timer can be set from 2min. to 1440min.

Current Timer values

In case of an active Timer the appropriate value of the timer is displayed here.



5.3.2.5 Sync Source Errors

This tab displays the current failure status.

	General	Time/Date		Network	NTP	РТР	Alarm	Device	Output
	Local Time Setting Set Time/Date Time Zone Offs: Daylight Saving SyncON / SyncO	gs et 1 Time DFF	Sync	Source Errors tware Errors OK Gene OK Missir OK Missir	ral Module erro ng data for Tin ng or incomple	or (PCID) ne Zone Offse ite data for da	t ylight saving tir	ne (DST)	
ſ	Sync Status		Har	dware Errors					
	Sync Source Er	rors		OK Adjus	tment of inter	nal quartz fre	quency error		
	<u>Sync Status OC</u>			OK FRAM	error				
	Error values are refreshed automatically every 5 seconds.								

This page is updated automatically every 5 seconds.

Overview Software Errors

- General Module error (PCID) If this error occurs even after a power reset, the device is damaged.
- Missing data for Time Zone Offset Difference time (Time Zone Offset) must initially be entered by the user. Otherwise no synchronization will take place.
- Missing or incomplete data for daylight saving time (DST)
 The switchover times for summer/winter time must be initially set / disabled by the user. Otherwise no synchronization will take place.

Übersicht Hardware Errors

Adjustment of internal quartz frequency error

Problems with the internal quartz regulation have occurred. So the specified accuracy of the Sync Source cannot be guaranteed anymore.

• FRAM error

If this error occurs even after a voltage reset, the support team of company *hopf* needs to be contacted for further steps.

5.3.2.6 Sync Status OC

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
Local Time Setting Set Time/Date Time Zone Offset Daylight Saving 1 SyncoN / Synco	t Time FF	Sync Status OC Opto coupler switch SYOF - Time synchro SYOF - Time synchro QUON - Time crystal QUEX - Time crystal QUEX - Time crystal	es off if statu: onized + Crysta onized + SyncO nized (simulatio + SyncON time (after synchroni after reset or se	s is lower tha frequency is a FF timer is run n mode) er is running zation break / c et manually	n djusted ning clock has synchro	nized before)	
Sync Status Sync Source Erro Sync Status OC	DIS	INVA - Time invalid					

The output of the status optical coupler can be configured by using this function.

The Sync states are listed in this selection window in rising quality from the bottom to the top (**SYNC** = optimal condition).

Behaviour of Optical Coupler:

- Selected status achieved or better Optical coupler switched through •
- Selected status not achieved •
- Optical coupler blocked

Value range

Optical Coupler Status	SYNC	Time synchronized + Quartz regulation started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (without actual GPS reception)
	QUON	Quartz/Crystal time + SyncON running
	QUEX	Quartz/Crystal time (in freewheel after synchronization failure ⇔ Board was already synchronized)
	QUSE	Quartz/Crystal time after reset or manual setting
	INVA	Invalid time



5.3.3 NETWORK Tab

All the links within the tab on the left hand side lead to corresponding detailed setting options.

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
	General Host Settings Host/Nameservi Network Interfa Network Interfa Bonding/Teamin Network Interfa PRP Routing Bouting File	Time/Date	Network	NTP es v6 Address	9T9	Alarm	Device	Output
[Protocols		NS Server 3 IPv4/IP	v6 Address				



Changing Network Parameters

Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.

However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data permanently by pressing **Save**.

5.3.3.1 Host / Name Service

Setting for the unique network identification.

5.3.3.1.1 Hostname

Depending on the system the hostname default is either "**hopf7279**" or "**hopf7279RC**". This name should also be adapted in the respective network infrastructure.

In case of doubt, you might not change the standard value or you might ask your network administrator.



The **hostname** <u>must</u> meet the following conditions:

- The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.' . There should be no distinction between capital letters and lower-case letters.
- The character '.' may only appear as a separator between labels in domain names.
- The sign '-' must not appear as first or last character of a label.



For a correct operation a hostname is required. The field for the hostname **<u>must not</u>** be left blank.



5.3.3.1.2 Use Manual DNS Entries

With this setting you can select if the manually entered DNS servers of Board 7279(RC) (DNS servers 1 to 3) should be used.

If "enabled" is selected here, the entries in DNS Server 1 to 3 are used.

If "disabled" is selected, the entries in DNS Server 1 to 3 are ignored.



If a DHCP server is used to distribute the network configuration and if this also distributes the DNS servers used in the network, you should set Manual DNS Entries disabled at Use.

5.3.3.1.3 DNS Server 1 to 3

The IP address (IPv4 or IPv6) of the DNS server should be entered if you wish to use complete Hostnames (hostname.domainname) or work with reverse lookup.

Contact your network administrator for details of the DNS server if not known.

If no DNS server is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

5.3.3.1.4 Use Manual Gateway Entries

With this setting, you can select if the manually entered gateways of Board 7279(RC) (Default Gateway IPv4 and Default Gateway IPv6) should be used.

If "enabled" is selected here, the entries in Default Gateway IPv4 and Default Gateway IPv6 are used.

If "disabled" is selected, the entries in Default Gateway IPv4 and Default Gateway IPv6 are ignored.



If a DHCP server is used to distribute the network configuration and if this also distributes the address of the default gateway used in the network, you should set Manual Gateway Entries disabled at Use.

5.3.3.1.5 Default Gateway IPv4

If the IPv4 default gateway is not known, it must be requested from the network administrator. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.

5.3.3.1.6 Default Gateway IPv6

If the IPv6 default gateway is not known, it must be requested from the network administrator. If no standard gateway is available (special case), enter :: in the input field or leave the field blank.


5.3.3.2 Network Interface ETH0/ETH1

Configuration of the Ethernet interface ETH0/ETH1 of Board 7279(RC)



ETH1 must not be located in the same sub net as ETH0!

5.3.3.2.1 Default Hardware Address (MAC)

The factory default MAC address can only be read and cannot be changed by the user. It is assigned only once by *hopf* Elektronik GmbH for each Ethernet interface.

For further information about the MAC address refer to *Chapter 1.3.4.1 MAC-Address for ETH0/ETH1* for Board 7279(RC).



hopf Elektronik GmbH MAC addresses begin with **00:03:C7**:xx:xx:xx.



5.3.3.2.2 Customer Hardware Address (MAC)

The MAC address assigned from *hopf* can be changed to any user-defined MAC address. The board identifies itself with the user-defined MAC address to the network. The default hardware address shown in WebGUI remains unchanged.



Double assignment of MAC addresses on the Ethernet referring to customers MAC addresses should be avoided.

If the MAC address is not known, please contact your network administrator.

The use of customers MAC address needs to be activated by the function **Use Custom Hard**ware Address (MAC) with enable and subsequently save it with Apply and Save.

Afterwards the customers MAC address has to be entered in hexadecimal form with a colon to separate as described in the below example, e.g. **00:03:c7:55:55:02**



The MAC address assigned by *hopf* can be activated at any time by disabling this function.



There are no MAC multicast addresses allowed!

Finally, the Board 7279(RC) has to be restarted via "Device - Reboot Device" (see *Chapter* **5.3.7.4 Reboot Device**.

5.3.3.2.3 DHCP

If DHCP should be used, activate this function with enabled.

5.3.3.2.4 IPv4 Address

If DHCP is not used, the IPv4 address needs to be entered here. Contact your network administrator for details of the used IPv4 address if not known.

5.3.3.2.5 IPv4 Network Mask

If DHCP is not used, the network mask needs to be entered here. Contact your network administrator for details of the used network mask if not known.

5.3.3.2.6 Operation Mode

Operation mode



The network device usually adjusts the data stream and duplex mode to the device to which it is connected (e.g. HUB, SWITCH) automatically. If the network device requires a certain speed or duplex mode, this can be configured via the web interface. The value should only be changed in special cases. The automatic setting is normally used.





In individual cases an enabled "Auto negotiate" might lead to problems between the network components and the adjustment process fails.

In such cases it is recommended to set the network speed of Board 7279(RC) <u>and</u> the connected network components manually to the same value.

5.3.3.2.7 Maximum Transmission Unit (MTU)

The Maximum Transmission Unit describes the maximum size of a data packet of a protocol of the network layer (layer 3 of OSI model), measured in octets which can be transferred into the frame of a net of the security layer (layer 2 of OSI model) without fragmentation.

Board 7279(RC) is going to be delivered with default setting 1356.

5.3.3.2.8 IPv6

The Board 7279(RC) can also be operated in an IPv6 network.

To enable IPv6, Use IPv6 Settings must be set to enable.

IPv6 addresses are 128 bits long and they are recorded in eight 4-character hexadecimal blocks. For example: **2001:0db8:0000:08d3:1319:8a2e:0370:7344**

Leading zeroes in a 4-character hexadecimal block can be omitted. For the above example, this results in the notation: **2001:db8:0:8d3:1319:8a2e:370:7344**

In addition, **once** per IPv6 address a consecutive sequence of blocks containing all zeroes may be omitted. But this must be recorded with two consecutive colons. For the above example, this gives the notation: **2001:db8::8d3:1319:8a2e:370:7344**

Another example: 2001:0:0:0:1319:8a2e:0:7344 may be represented

- as 2001::1319:8a2e:0:7344
- or 2001:0:0:1319:8a2e::7344

5.3.3.2.9 DHCP-IPv6

If DHCP should be used, this function is activated with **enabled**.

5.3.3.2.10 IPv6 Address

If DHCP is not used, enter the IPv6 address here. If the IPv6 address to be used is unknown, it must be requested by the network administrator.

5.3.3.2.11 IPv6 Subnet Prefix Lengh

If no DHCP is used, the length of the network address must be entered here. If the length of the network address is not known, it must be requested by the network administrator.



5.3.3.2.12 VLAN (Activation Key necessary)

A VLAN (Virtual Local Area Network) is a logical sub-network within a network switch or a whole physical network. VLANs are used to separate the logical network infrastructure from the physical wiring, thus to virtualize the Local Area Network. The technology of VLAN is standardized by IEEE Standard 802.1q. Network applications like Board 7279(RC), implementing the standard IEEE 802.1q, are able to allocate individual network interfaces to specific VLANs. To transfer data packets of several VLANs via a single network interface the data packets are marked with a related VLAN ID. This method is called VLAN-Tagging. The network application at the other end of the line (e.g. network switch, router etc.) can allocate the data packet to the correct VLAN by checking the marking / tag.

VLAN			
Activation Status disabled V			
VLAN Interfaces			
Add Remove			
ID Label Remark	DHCP	IPv4-Address	IPv4-Network Mask

WebGUI with activated VLAN

To be able to configure VLANs the activation status must be set to "enabled" first. Afterwards up to 32 different VLANs per network interface can be configured by clicking the button "Add".

An explicit VLAN ID must be configured for each VLAN interface.

The boxes "Label" and "Remark" can be filled out with a designation or a comment to easily keep the configured VLANs apart.

Determination of the IP-address for the configured VLAN interface can either be done automatically via DHCP or by filling out the boxes "IP-Address" and "Network Mask".

VLAN					
Activatio enabled	n Status V				
VLAN Ir	iterfaces				
Add	Remove				
ID	Label	Remark	DHCP	IP-Address	Network Mask
□ 10	DEV	Development	disabled 🗸	192.168.180.30	255.255.255.0

i

To ensure the correct function the network appliance must be connected with Board 7279(RC) via the network interface. Furthermore, it must be ensured that the network appliance is accurately configured with the same VLANs.



VLAN ID one (1) and two (2) are reserved and are therefore not permitted!

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.3.3 Network Interface Bonding/Teaming (Activation Key necessary)

The function Network Interface Bonding/Teaming (also known as NIC Bonding, NIC Teaming, Link Bundling, EtherChannel) enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface.

General III	ne/Date Network NTP I	PTP Alarm Device	Output
General		n Aun Device	output
Host Settings	Bonding/Teaming IPv4 Settings	Bonding/Teaming IPv6 Settings	
Host/Nameservice Network Interface ETH0 Network Interface Bonding/Teaming Network Interface PRP Routing Routing File	NIC Bonding/Teaming active disabled ✓ DHCP disabled ✓ IPv4-Address IPv4-Network Mask Operation mode Auto negotiate ✓ Maximum Tangenicipe Unit (MTU)	Use IPv6 Settings disabled \checkmark DHCP-IPv6 disabled \checkmark IPv6-Address IPv6 Subnet Prefix Length	
rrotocols Management	Advanced Settings Bonding Policy Round-Robin MII Link Monitoring Interval (ms) 100	Link Down Delay (ms) 0 0	ay (ms)
	LACP Rate (only valid for IEEE 802.3ad poli Slow (every 30 seconds) ✓ Primary Device (only valid for Active-Backu None ✓	icy) Jp and TLB policy)	
	WARNING: changing these values can modifications only if you really know w changing the bonding configuration.	cause serious network problems. Perfor hat you are doing! A reboot is recomme	m ended after
	VLAN Activation Status disabled V VLAN Interfaces		

This function is used for the distribution of load as well as to increase fail-safety in computer networks.



Making settings without profound knowledge of Bonding/Teaming can lead to serious network problems!

An incorrect configuration can lead to a loss of the network connection so that the Ethernet access to Board 7279(RC) is going to be refused. In this case settings must be set back to default!



If function Bonding has been activated, parameters for ETH0 and ETH1 cannot be changed any more. The parameters are not displayed in the host setting menu as long as Bonding will be deactivated.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.3.1 Basic Configuration

Determination of the basic network configuration with activated function Bonding/Teaming.

Bonding/Teaming IPv4 Settings	
NIC Bonding/Teaming active	
DHCP disabled ∨	
IPv4-Address	
IPv4-Network Mask	
Operation mode	
Maximum Transmission Unit (MTU)	1

NIC Bonding/Teaming active

Activation of function NIC Bonding/Teaming

DHCP

Activation of DHCP of the "Bonding interface".



A change of the IPv4 address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.

IPv4 address

Input of IPv4 address of the "Bonding interface".

If you do not know the IPv4 address, please contact your network administrator.



A change of the IPv4 address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.

IPv4 Network Mask

Input of the IPv4 network mask of the "Bonding interface".



A change of the IPv4 address or activating of DHCP do have an immediate effect after confirming the settings – the connection to the web interface must be adapted and renewed.



5.3.3.2 IPv6 Network Configuration

Defining the IPv6 network configuration with the Bonding / Teaming function activated.

Bonding/Teaming IPv6 Settings	
Use IPv6 Settings	
disabled 🗸	
DHCP-IPv6	
disabled V	
IPv6-Address	
That Calment Destination at	
IPv6 Subnet Prefix Length	

Use IPv6 Settings

Activation of IPv6 function.

DHCP-IPv6

Activation of IPv6 DHCP for the "bonding interface".

IPv6 address

Input of the IPv6 address for the "bonding interface". If the IPv6 address is not known, it must be requested from the network administrator.

IPv6 Subnet Prefix Length

Input of the IPv6 network length for the "bonding interface".



5.3.3.3.3 Advanced Settings

Bonding Policy Round-Robin MII Link Monitoring Interval (ms) Link Down Delay (ms) Link Up Delay (ms) 100 0 0 LACP Rate (only valid for IEEE 802.3ad policy) 0 0 Slow (every 30 seconds) V Primary Device (only valid for Active-Backup and TLB policy) None V WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	Advanced Settings		
MII Link Monitoring Interval (ms) Link Down Delay (ms) Link Up Delay (ms) 100 0 0 LACP Rate (only valid for IEEE 802.3ad policy) 0 Slow (every 30 seconds) ✓ Primary Device (only valid for Active-Backup and TLB policy) None ✓ WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	Bonding Policy Round-Robin		
100 0 0 LACP Rate (only valid for IEEE 802.3ad policy) Slow (every 30 seconds) ♥ Primary Device (only valid for Active-Backup and TLB policy) None ♥ WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	MII Link Monitoring Interval (ms)	Link Down Delay (ms)	Link Up Delay (ms)
LACP Rate (only valid for IEEE 802.3ad policy) Slow (every 30 seconds) ♥ Primary Device (only valid for Active-Backup and TLB policy) None ♥ WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	100	0	0
Primary Device (only valid for Active-Backup and TLB policy) None WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	LACP Rate (only valid for IEEE 802.3ad polic Slow (every 30 seconds) ✓	-v)	
WARNING: changing these values can cause serious network problems. Perform modifications only if you really know what you are doing! A reboot is recommended after	Primary Device (only valid for Active-Backup None V	p and TLB policy)	
changing the bonding configuration.	WARNING: changing these values can c modifications only if you really know wh changing the bonding configuration.	ause serious network probl nat you are doing! A reboot	ems. Perform is recommended after

Bonding Policy

• Round-Robin:

In this case the network interfaces, starting with ETH0, are transmitting sequentially whereby a distribution of load and a higher tolerance for errors are achieved. In that mode the network interfaces must be connected to the same network switch.

• Active Backup:

Only one of two network interfaces is sending and receiving. If an error occurs, the other network interface assumes responsibility for the process. The network interfaces do not have to be connected to the same network switch. From the outside the MAC address of the association is only visible on one network interface to avoid a mix-up. This mode supports tolerance for errors.

• Balance XOR:

Source and target are permanently assigned with one another via the MAC address of the network interfaces ETH0 and ETH1. The network interfaces must be connected to the same network switch. This mode supports distribution of load and tolerance for errors.

• Broadcast:

In this mode the computer sends its data via all available network interfaces which enables the use of several network switches. This fact leads to a high tolerance for errors, but this mode does not enable distribution of load.

• IEEE 802.3ad Dynamic Link Aggregation:

The network interfaces ETH0 and ETH1 are going to be bundled (Trunking) in this mode. It is mandatory that the network interfaces are configured with the same transmission rate and duplex setting. Bundling is made dynamically via the Link Aggregation Control Protocol (LACP). This mode supports distribution of load as well as tolerance for errors.



The network switch on which the network interfaces ETH0 and ETH1 of Board 7279(RC) are connected also needs to be configured correctly! A wrong configuration can lead to a loss of availability of Board!



• Adaptive Transmit Load Balancing (TLB):

Outbound data traffic is split on both network interfaces ETH0 and ETH1 in accordance with the current load, depending on the interface speed adjusted. The network interfaces do not have to be connected on the same network switch. This mode supports distribution of load and tolerance for errors.

MII link monitoring interval (ms)

Indicates the interval in milliseconds for observing the MII-connection. A value of zero deactivates monitoring. The default value is 100ms.

link down delay (ms)

Determines the delay time in milliseconds to deactivate a connection after a link error is detected. This value needs to be a multiple of the MII link monitoring interval.

link up delay (ms)

Determines the delay time in milliseconds to enable a conjunction after a connection is detected. This value needs to be a multiple of the MII link monitoring interval.

LACP rate (only available for IEEE 802.3ad directive)

Indicates the link partner's request frequency to transfer LACP packets in IEEE 802.3ad mode.

Primary Device (only valid for active backup and TLB directive)

If this asset is configured and the network interface is active, the adjusted network interface is going to be used. Only if the network interface is inactive, mode is changed to the second network interface.



5.3.3.4 Network Interface PRP (Activation Key necessary)

The PRP (Parallel Redundancy Protocol) functionality is specified in standard IEC 62439-3:2011 and enables to bundle the physical network interfaces ETH0 and ETH1 to one logical network interface. Each network interface is connected to an independent LAN (Local Area Network). If one of the two LANs has got a failure, usage of PRP ensures that the network connection between the PRP terminal devices is going to be maintained via the second, independent LAN. PRP standard was developed for very high demanding and critical applications in the field of automation of substations.

The following illustration shows an example of a PRP network:



PRP-suitable applications are known as DAN (Dual Attached Node) and are going to be connected to the independent networks "LAN A" and "LAN B". The advantage of PRP is that costefficient and common network switches can be used which do not have to support the PRP standard. Applications which do not need to be redundantly available and which do not have to support PRP can be connected without problems in one of the two LANs - they are then called SAN (Single Attached Node). If it is necessary to redundantly connect non-PRP-supporting applications to the PRP network, a so-called RedBox (Redundancy Box) can be used.

Board 7279(RC) supports PRP as DAN and can therefore directly be integrated into a PRP network without using a RedBox.



General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
Host Settings		PRP IPv4 Settings			PRP IPv6 Setting	5]
Host/Nameservid Network Interfac ETH0 Network Interfac ETH1 Network Interfac Bonding/Teamin Network Interfac PRP Routing Routing File		NIC PRP active disabled V DHCP disabled V IPv4-Address IPv4-Network Mask			Use IPv6 Setting disabled V DHCP-IPv6 disabled V IPv6-Address IPv6 Subnet Pref	s Îix Length	
Protocols Management		Maximum Transmissi	on Unit (MTU)				

To use PRP the following settings must be carried out:

NIC PRP active

Activation of the PRP functionality

DHCP

Activation of DHCP for the "PRP interface".



A change of the IPv4 address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.

IPv4 address

Input of the IPv4 address for the "PRP interface". If unknown the IPv4 address needs to be obtained by the network administrator.



A change of the IPv4 address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.

IPv4 Network Mask

Input of the IPv4 network mask for the "PRP interface".



A change of the IPv4 address or activation of DHCP will have an immediate effect after applying the settings - the connection to the web interface must be adapted and renewed.



Maximum Transmission Unit (MTU)

Input of the MTU to be used for the "PRP interface".

The network interface ETH0 of Board 7279(RC) needs to be connected to PRP network "LAN A", network interface ETH1 needs to be connected to PRP network "LAN B"!



Changing of the MTU default setting with value 1466 should not be necessary by default.

If settings are done without profound knowledge of PRP, severe network problems can occur.

An incorrect configuration can lead to a loss of the network connection which refuses the Ethernet access to Board 7279(RC).

In that case the settings of Board 7279(RC) need to be set to "factory default"!



If the functionality PRP was activated, parameters for ETH0 and ETH1 can no longer be adapted. The parameters will not be displayed in the host settings menu as long as PRP is going to be deactivated.

5.3.3.4.1 IPv6-Netzwerkkonfiguration

Defining the IPv6 network configuration for the PRP interface.

Use IPv6 Settings

Activation of IPv6 function

DHCP IPv6

Activation of IPv6 DHCP for the "PRP interface ".

IPv6 address

Input of the IPv6 address for the "PRP interface". If the IPv6 address is not known, it must be requested from the network administrator.

IPv6 Subnet Prefix Length

Input of the IPv6 network length for the "PRP interface".



5.3.3.5 Routing (Activation Key necessary)

Additional static routes can be configured if the board is not only used in the local sub net and if connection cannot be established via the configured standard gateway.

The gateway / gateway host needs to be in the local sub-network range of the board in order to use the static routes.



The parameterization of this feature is a critical process as an incorrect configuration may lead to considerable problems on the network!

WebGUI with Routing activated

ost Settings	Current System Rout	ing Table			
Host/Nameservice	Network/Host	Network Mask	Gateway	Network Inter	face
Network Interface	default	0.0.0	192.168.180.1	eth0	
<u>ETHO</u> <u>Network Interface</u> ETH1	192.168.180.0	255.255.252.0	0.0.0.0	eth0	
Network Interface					
Bonding/Teaming	User Defined Routes				
<u>vetwork Interrace</u> PRP					
Routing	disabled V				
Routing File	diodolog -				
	Network Routes				
rotocols	Add Remove				
<u>Management</u>	Network/Host	Netv	/ork Mask	Gateway	
	1				

The image above shows every configured route of the base system routing table as well as the user's defined static routes.



The board cannot be used as a router!

By selecting **Use Route File** you can set up whether the under **User Defined Routes** set routing configuration should be used, or if routing configuration should take place by using a routing file.



If IPv6 routes are required, the routes must be made using the settings in *Chapter 5.3.3.5 Routing (Activation Key necessary)*



5.3.3.6 Routing File

In order to activate this function, Use Route File must be set to enabled on the Routing Page (see Chapter 5.3.3.5 Routing (Activation Key necessary)).

	General	Time/Date	Netwo	ork NTP	РТР	Alar	m Device	Output	
	Host Settings Host/Nameserv Network Interfit ETH0 Network Interfit Bonding/Teami Network Interfit PRP Routing	ice ace ace ng ace	Routing File Update file: Upload nov Download Rout	v ting File e to download	Du	rchsuchen			
	Routing File		Current System	Routing Table					
ſ	Protocols		Network/Host		Net	vork Mask	Gateway	N	letwork interface
ŀ	FIOLOCOIS		default		0.0	0.0	192.168.180.1	e	eth0
	<u>Management</u>		192.168.180.	0	255	.255.252.0	0.0.0.0	e	eth0
			0000000000000	000000000000000000000000000000000000000	000000180		000000000000000000000000000000000000000	00000000000000000000000000000000000000	0
			fe800000000	000000203c7fffe0	01947e 80		000000000000000000000000000000000000000	000000000000000000000000000000000000000	0
			fe800000000	000000000000000000000000000000000000000	0000000 40		000000000000000000000000000000000000000	0000000000000000000 e	eth0
			ff0000000000	000000000000000000000000000000000000000	0000000 08		000000000000000000000000000000000000000	000000000000000000 e	eth0
			00000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000		000000000000000000000000000000000000000	000000000000000000000000000000000000000	0

The routing file also makes it possible to configure IPv6 routes.

Via the selection window under **Update file** and the button **Upload now** a new routing file can be uploaded. While uploading the file is checked whether it is error-free; only then it is used.

If a routing file has already been uploaded, the uploaded routing file can be downloaded under **Download Routing File.**

Routing File Syntax

Each line of the routing file must be either a valid routing line or a comment line.

A comment line starts with a hash sign (#) and can contain any text behind it.

A routing line has the format [destination address] [tab] [length of the destination mask in bits] [tab] [gateway address for the specified destination].

Should the host 192.168.20.11 be reached by using the gateway 192.168.0.2, then the routing file must look like this:

192.168.20.11 32 192.168.0.2

Example of a Routing File:

```
# Host 192.168.20.11 via Gateway 192.168.0.2
192.168.20.11 32 192.168.0.2
#Net 192.168.180.0 Netmask 255.255.255.0 via Gateway 192.168.0.2
192.168.180.0 24 192.168.0.2
#Net 2001:0db8:0:f102:: Subnet Prefix Length 64 via Gateway 2001:0db8:0:f101::1
2001:0db8:0:f102:: 64
                           2000::1
```

Current System Routing Table

This table shows all active IPv4 and IPv6 routes that are active in the Board 7279(RC).

For IPv6 routes, the colons of the destination and gateway addresses are not displayed, and the Network Mask column displays the length in hexadecimal.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01

hopf Elektronik GmbH

50 / 125



5.3.3.7 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)

Protocols that are not required should be disabled for security reasons. A correctly configured board is always accessible via the web interface.

Changes to the availability of a protocol (enable/disable) take effect immediately.





These service settings are valid globally! "Disabled" Services are not externally accessible and are not made externally available by the board!



General Time/Date	Network	NTP	РТР	Alarm	Device	Output
Host Settings Host/Nameservice Network Interface ETH0 Network Interface Bonding/Teaming Network Interface PRP Routing Routing File Protocols Management	Management Proto HTTP enabled ✓ HTTPS disabled ✓ SSH enabled ✓ TELNET disabled ✓ SNMP disabled ✓	Network Interfa Both V Network Interfa Both V Network Interfa Both V Network Interfa Both V	ace ace ace ace	SNMP System Location System Contact System Contact SNMPv2 Read O public SNMPv2 Read W secret SNMPv3 Access Readonly SNMPv3 Access Readonly SNMPv3 Authen MD5 SNMPv3 Authen SNMPv3 Authen SNMPv3 Privacy DES SNMPv3 Privacy	nly Community //rite Community //rite Community // Name 	• •

WebGUI with Alarming activated

Using SNMP and SNMP- traps the protocol SNMP should be enabled.



5.3.3.7.1 SNMPv2c / SNMPv3 (Activation Key required)

Both protocols SNMPv2c and SNMPv3 are supported and can be configured and enabled independently from each other.

System Location and System Contact are global settings and are valid for both protocols (SNMPv2c / SNMPv3).

In order to disable SNMPv2c both fields **SNMP Read Only Community** and **SNMP Read Write Community** must remain empty.

SNMPv2c	SNMPv2c enabled	SNMPv2c disabled
Read Only Community:	set (e.g. public)	empty
Read/Write Community:	set (e.g. secret)	empty

In order to enable SNMPv3 the following fields must be set:

SNMPv3	Description
Security Name:	SNMPv3 is enabled (identical to the username)
Access Rights:	Equivalent to the Read/Write Communities in SNMPv2c
Authentication Protocol:	Authentication (MD5 or SHA Hash)
Privacy Protocol:	Encryption (DES or AES Algorithm)

There are three security levels in SNMPv3 that can be adjusted by the removal of the passphrases:

SNMPv3	noAuthNoPriv	authNoPriv	authPriv
Authentication Passphrase:	empty	set	set
Privacy Passphrase:	empty	empty	set



Right now only one user is supported.



5.3.4 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Board 7279(RC).

If you are not familiar with the subject of NTP you can find a short description in the Glossary. More details are also available at <u>http://www.ntp.org/</u>.

Depending on the receiving conditions and under unfavourable circumstances it may take several hours until long-term accuracy is obtained (normally 5-10 minutes). During this time the NTP algorithm adjusts the internal accuracy parameters.



After all changes relating to NTP a restart of the NTP service must be performed (see *Chapter 5.3.4.6 Restart NTP*).



Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

5.3.4.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the Board 7279(RC) are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Board 7279(RC), the status to the leap second, and the current system peer are also found here.

The NTP version used adjusts the leap second correctly.

In case the used NTP Server (System PEER) works with Stratum 1 the NTP Client reaches max. Stratum 2.

(General	Time/Date	Network	NTP РТР	Alarm	Device	Output
	General NTP Info System Info Kernel Info Peers Basic Configuratio Server Configuratio	Time/Date	Network ystem Info System Peer 192.168.180.103 kefID 192.168.180.103 .eap Indicator 10 warning Stratum	NTP PTP	Alarm	Device	Output
	Extended Configuration Restart NTP		2 Root Delay 0.000366 s Root Dispersion 0.003693 s				
	Access Restricti Symmetric Key Autokey	ions S	nter 0.000000 s Stability 0.007706 ppm				



5.3.4.2 Kernel Info

The "Kernel Info" overview shows the current error values. Both values are internally updated every second.

General	Time/Date	Network	NTP PTI	Alarm	Device	Output
NTP Info System Info Kernel Info Peers Basic Configuratio	Ke M 0. Es 0.	rnel Info ax. Error .077550 s stimated Error .000017 s				

This screenshot shows a maximum kernel clock error of 77,550 msec (milliseconds). The estimated error value is $17 \ \mu$ s (microseconds).

The values indicated here are based on the calculation of the NTP service and have no significance for the accuracy of the Sync Source.

5.3.4.3 Peers

The "Peers summary" is used to track the performance of the configured NTP server/driver and the NTP algorithm itself.

The information displayed is identical with the information available via NTPQ or NTPDC programs.

Each NTP server/driver that has been set up in the NTP server configuration is displayed in the peer information.

The connection status is displayed in the reachability column (not reachable, bad, medium, and reachable).

General	Time/Date	e (Network	NTP	РТР	Alarm	Device	Output
 NTP Info System Info Kernel Info Peers		Peers	Peer LOCAL(0)	Stratum 15	Reachability not reachable	Delay 0.000000	Offset 0.000000	Dispersion 15.937500
		*	192.168.180.103	1	reachable	0.000370	0.000009	0.001960

In the upper picture, the second line shows the external NTP server used for synchronization.

A short explanation and definition of the displayed values can be found in *Chapter 9.5 Accuracy & NTP/PTP Basic* Principles.

The character in the first column on the left presents the current status of the NTP association in the NTP selection algorithm. A list and description of possible characters can be found in the Glossary (see *Chapter 9.2 Tally Codes (NTP-specific)*).

5.3.4.4 Server Configuration

The basic settings for NTP base functionality are displayed when the "Server Configuration" link is selected.

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output	<50
NT S K P	P Info ystem Info ernel Info eers		Broadcast/Multicast Broadcast/Multicast disabled V Multicast Client Addu	Mode					
Ba: Si Cu Ru	sic Configuration erver Configur xtended onfiguration estart NTP	ation	NTP servers Configured NTP se	rvers					
	curity ccess Restricti ymmetric Keys utokey	<u>ons</u>	Server Identif	ìer).103			Authentication	Key ID	Peer

5.3.4.4.1 Broadcast / Multicast

This section is used to configure the Board 7279(RC) as a broadcast or multicast server.

The broadcast mode in NTPv3 and NTPv4 is limited to clients on the same sub-network and Ethernets which support broadcast technology.

This technology does not generally extend beyond the first hop (network node - such as router or gateway).

The broadcast mode is provided for configurations which are designed to facilitate one or more servers and as many clients as possible in a sub-network. The server continuously generates broadcast messages at defined intervals, corresponding to 16 seconds (minpoll 4) for Board 7279(RC). Care should be taken to ensure that the correct broadcast address is used for the sub-network, usually xxx.xxx.255 (e.g. 192.168.1.255). If the broadcast address is not known, this can be requested from the network administrator.

This section can also be used to configure the Board 7279(RC) as a multicast server. The configuration of a multicast server is similar to that of a broadcast server. However, a multicast group address (class D) is used instead of the broadcast address.

An explanation of multicast technology goes beyond the scope of this document.

In principle, a host or router sends a message to an IPv4 multicast group address and expects all hosts and routers to receive this message. In doing so, there is no limit to the number of senders and receivers and a sender may also be a receiver and vice-versa. The IANA has assigned the multicast group address IPv4 224.0.1.1 to the NTP, however this should only be used if the multicast range can be safely limited in order to protect neighbouring networks. As a basic principle, administratively manageable IPv4 group addresses should be used as described in RFC-2365 or GLOP group addresses as described in RFC-2770.



5.3.4.4.2 NTP SERVERS for Synchronisation

Server Name

In this field the NTP Server, used for the synchronisation of Board 7279(RC), should be registered. Adding further NTP servers provides the option to implement a safety system for the time service. However, this influences the accuracy and stability of the board.

Detailed information on this subject can be found in the NTP documentation (<u>http://www.ntp.org/</u>).

Authentication / Key ID

Broadcast packets can be protected by authentication for security reasons.

If a security method is selected here, this must be configured ADDITIONALLY in the security settings of the NTP tab. A key must be defined if the "Symmetric Key" is selected.

5.3.4.5 Extended Configuration

The synchronisation behaviour of Board 7279(RC) can be adjusted following the link " **Extended Configuration**". This function allows by reference to the associated system properties Board 7279(RC) to use NTP Server for synchronization and thus for the output of time information for the synchronization of connected devices and components with inaccurate NTP server. Reasons for inaccurate NTP server could be e.g. poor network performance, poor own accuracy or bad availability resulting in an insufficiently accurate synchronization of the module with the standard settings.

This function should be disabled by default.



When using this function the specified accuracy of Board 7279(RC) and thus the accuracy of devices and components synchronized by the module may be worsened.



When using this function the specified data of NTP accuracy stated in the technical data of Board 7279(RC) are not valid anymore.



General	Time/Date	Network		РТР	Alarm	Device	Output
NTP Info System Info Kernel Info Peers Basic Configuration Server Configuration Extended Configuration Restart NTP	on ration	imitation of Liability IN NO EVENT WIL ELEKTRONIK GMB INCIDENTAL, SPE WHATSOEVER REI SETTINGS OFFER CONFIGURATION, BUSINESS INTER EVEN IF RDCS INI GMBH IS/ARE EXI EXCLUSION AND W WHETHER BASED THEORIES.	L BOTH RDCS THE LIABLE CIAL, EXEMPL LATED TO OR A ED IN THE CUR , INCLUDING, RUPTION, LOS FORMATIONST PRESSLY ADVI WAIVER OF LI ON CONTRACT	INFORMA TO ANY PA ARY OR C ARISING F RENT COL WITHOUT T SAVING ECHNOLO SED OF TI ABILITY A F, WARRA	TIONSTECHNO ARTY FOR ANY ONSEQUENTIA "ROM THE USE NFIGURATION LIMITATION, S OR LOSS OF GIE GMBH AN HE POSSIBILT APPLIES TO AL NTY, TORT, OR	DLOGIE GMBH / DIRECT, INDII L DAMAGES 01 OF THE NON-S SECTION EXTI ANY LOST PRC PROGRAMS OF D/OR HOPF EL TY OF SUCH DA L CAUSES OF A L ANY OTHER L	AND HOPF RECT, F ANY TYPE STANDARD SINDED OFITS, R OTHER DATA, EKTRONIK IMAGES. THIS ICTION, EGAL
Security Access Restricti Symmetric Key Autokey	ons S	Customized Settings for Override default limit disabled \checkmark Lambda (λ) = 20 HIGH)	or Synchronization values for synchron] ms (1 - 999,	n onization default: 20), minimum acc	uracy = HIGH	✓ (default:

These functions are only unlocked with the declaration of consent "I agree" of the disclaimer "Limitation of Liability".



Safety Guidelines

These functions should only be used by qualified users. *hopf* is not liable for any damage caused by these.

Security Access Restrictions	Customized Settings for Synchronization
Symmetric Keys Autokey	Override default limit values for synchronization disabled -
	Lambda (λ) = 20 ms (1 - 999, default: 20), minimum accuracy = HIGH ▼ (default: HIGH) LOW MEDIUM HIGH

Override default limit values for synchronization

For standard operation this function is disabled and should only be used by qualified users.

Lambda (λ)

For observance of specified accuracy of Board 7279(RC), it uses only accurate NTP server for synchronisation which have an accuracy value for lambda better 20ms.

In case it is required that Board 7279(RC) should be synchronized on a more inaccurate NTP server the threshold accuracy value for lambda can be adjusted by this function.

The actually calculated lambda value is shown in the General tab.



Therefore, the function "**Override default limit values for synchronisation**" needs to be activated and to configure the required accuracy value for lambda (1-999ms).



When using this function the specified accuracy of Board 7279(RC) and thus the accuracy of devices and components synchronized by the module may be worsened.

Minimum Accuracy

Only with the accuracy status **accuracy = high** Board 7279(RC) synchronizes.

This function can be used for NTP server not being able to synchronize Board 7279(RC) with the required accuracy. It allows the adjustment of the accuracy value (**accuracy = high** / **medium** / **low**) and the accuracy of the connected devices and components for the synchronization.



Modification of values does not cause an immediate effect when clicking on the apply symbol. In addition the NTP service <u>must</u> be restarted (see *Chapter 5.3.4.6 Restart NTP*).

5.3.4.5.1 Definition Accuracy (Low / Medium / High)

Calculation

LAMBDA = ((root delay / 2) + Rootdispersion) * 1000

LOW =

LAMBDA > Accuracy-value or No system peer available or Stratum = 16 or Internal NTP clock = not sync or Clock hardware fault = ERROR

MEDIUM =

LAMBDA < Accuracy-value and System_Peer_Offset >= 0,001s or LAMBDA < Accuracy-value and Stability > 2,0

HIGH =

LAMBDA < Accuracy-value and Stability < 0,2 or LAMBDA < Accuracy-value and Stability <= 2,0 and System Peer Offset < 0,001s



5.3.4.6 Restart NTP

The following screen appears after clicking on the Restart NTP function:

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
NTP Info System Info Kernel Info Peers Basic Configuratio Server Configuration Extended Configuration Restart NTP	n n ration	start NTP VARNING! estarting NTP wi ake tens of minut ccuracy again. Do TP? Restart now	ll decrease ac es until NTP r o you really w	curacy. It eaches hig ant to res	can gh tart		

Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Board 7279(RC). As can be seen from the warning message, the currently reachable stability and accuracy are lost due to this restart.

After a restart of the NTP service it takes a few minutes until the NTP service on Board 7279(RC) is adjusted on an available NTP Server again.

5.3.4.7 Access Restrictions / Configuring the NTP Service Restrictions

One of the extended configuration options for NTP is the "Access Restrictions" (NTP access restrictions).

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output		V 20
ſ	NTP Info		Access Restrictions							
	<u>System Info</u>		Default restriction	ignore	kod nogu		DOCOMUNE	noteon noteurt	varcian	
	<u>Kernel Info</u> <u>Peers</u>		default nomodify							
L			Restrictions							
ĺ	Basic Configuration	n	Add Remove							
	Server Configur	ation	IPv4/IPv6 Address	Netmas	sk ignore	kod noquery	nopeer noser	rver notrap notru	st version	
	Extended Configuration									
	Restart NTP									
ĥ	Security									
	Access Restricti	ons								
	<u>Symmetric Key</u> <u>Autokey</u>	<u>5</u>								

Restrictions are used in order to control access to the System's NTP service and these are regrettably the most misunderstood options of the NTP configuration.

If you are not familiar with these options, a detailed explanation can be found at <u>http://www.ntp.org/</u>.



IP addresses should be used when configuring the restrictions – no Hostnames!



The following steps show how restrictions can be configured - should these not be required it is sufficient to retain the standard settings.

The standard restrictions tell the NTP service how to handle packets of hosts (including remote time servers) and sub-network which otherwise have no special restrictions.

The NTP configuration can simplify the selection of the correct standard restrictions while making the required security available.

Before beginning the configuration the points **5.3.4.7.1** to **5.3.4.7.4** must be checked by the user:

5.3.4.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful In- spection Firewall?					
No	Proceed to Chapter 5.3.4.7.2 Blocking Unauthorised Access				
Yes	No restrictions are required in this case. Proceed further to <i>Chapter 5.3.4.7.4 Internal Client Protection / Local Network</i> <i>Threat Level</i>				

5.3.4.7.2 Blocking Unauthorised Access

Is it really Service is	Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?					
No	Proceed to Chapter 5.3.4.7.3 Allowing Client Requests					
Yes	In this case the following restrictions are to be used: ignore in the default restrictions					
	separate lines for each authorised server, client or sub-network. See <i>Chapter</i> 5.3.4.7.5 Addition of Exceptions to Standard					



5.3.4.7.3 Allowing Client Requests

Are client the time in module, o	Are clients to be allowed to see the server status information when they receive the time information from the NTP service (even if this is information about the module, operating system and NTPD version)?					
	In this case select from the following standard restrictions: See <i>Chapter 5.3.4.7.6 Access Control Options</i>					
	kod 🗸					
No	notrap					
	nopeer					
	noquery.					
	In this case select from the following standard restrictions: See <i>Chapter 5.3.4.7.6 Access Control</i> Options:					
	kod					
Yes	notrap					
163	nopeer					
	If a standard restriction is selected in this area, exceptions can be declared in separate lines for each authorised server, client or sub-network. See <i>Chapter 5.3.4.7.5 Addition of Exceptions to Standard</i> .					

5.3.4.7.4 Internal Client Protection / Local Network Threat Level

How much protection from internal network clients is required?						
	The following restrictions can be enabled if greater security settings than installed authentication are required in order to protect the NTP service f the clients see <i>Chapter 5.3.4.7.6 Access Control Options.</i>					
Yes	kod notrap nopeer	$\overline{\checkmark}$				



5.3.4.7.5 Addition of Exceptions to Standard Restrictions

After the standard restrictions have been set once, certain exceptions may be necessary for special hosts/sub-networks in order to allow remote time servers and client hosts/sub-networks to contact the NTP service.

These standard restrictions are to be added in the form of restriction lines.

Access Restrictions					
Default restriction ignore kod noquery default nomodify 🔽 🔽	nopeer	noserver	notrap I	notrust	version
Restrictions Add Remove					
IP-Address Netmask	ignore kod	noquery nope	er noserve	r notrap no	otrust version
192.168.233.199 255.255.224.0					



An unrestricted access of the Board 7279(RC) to its own NTP service is always allowed, irrespective of whether standard restrictions are ignored or not. This is necessary in order to be able to display NTP data on the web interface.

Add restriction exception: (for each remote time server)

Restrictions:	Press ADD	
	Enter the IP address	s of the remote time server.
	Enable restrictions:	e.g.
	notrap / nopeer / n	oquery 🗸
Allow unrestricted acce	ss to a special host ((e.g. System administrator's workstation):
Restrictions:	Press ADD	
	IP address 192.168	.1.101
	Do not enable any	restrictions
Allow a sub-network to	receive time server a	nd query server statistics:
Restrictions:	Press ADD	
	IP address 192.168	.1.0
	Network mask	255.255.255.0
	notrap / nopeer	\checkmark

The occurrence of exceptions also works for IPv6 addresses. To do this, the IPv6 address must be added in the **IPv4/IPv6 address**, and the **Netmask** column must be set to the length of the IPv6 netmask.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.4.7.6 Access Control Options

The official documentation concerning the current implementation of the restriction instructions can be found on the "Access Control Options" page at <u>http://www.ntp.org/</u>.

Numerous access control options are used. The most important of these are described in detail here.

nomodify – "Do not allow this host/sub-network to modify the NTPD settings unless it has the correct key."



Default Settings:

Always active. Can't be modified by the user.

As standard, NTP requires authentication with a symmetric key in order to carry out modifications with NTPDC. If a symmetric key is not configured for the NTP service, or if this is kept in a safe place, it is not necessary to use the nomodify option unless the authentication procedure appears to be unsafe.

noserver – "Do not transmit time to this host/sub-network." This option is used if a host/sub-network is only allowed access to the NTP service in order to monitor or remotely configure the service.

notrust -- "Ignore all NTP packets which are not encrypted."

This option tells the NTP service that all NTP packets which are not encrypted should be ignored (it should be noted that this is a change from ntp-4.1.x). The notrust option MUST NOT be used unless NTP Crypto (e.g. symmetric key or Autokey) has been correctly configured on both sides of the NTP connection (e.g. NTP service and remote time server, NTP service and client).

noquery – "Do not allow this host/sub-network to request the NTP service status." The ntpd status request function, provided by ntpd/ntpdc, declassifies certain information over the running ntpd Base System (e.g. operating system version, ntpd version) which under certain circumstances ought not to be made known to others. It must be decided whether it is more important to hide this information or to give clients the possibility of seeing synchronization information over ntpd.

ignore - "In this case ALL packets are refused, including ntpq and ntpdc requests".

kod – "A kiss-o'-death (KoD) packet is transmitted if this option is enabled in the case of an access error."

KoD packets are limited. They cannot be transmitted more frequently than once per second. Any KoD packet which occurs within one second from the last packet is removed.

notrap – "Denies support for the mode 6 control message trap service in order to synchronise hosts."

The trap service is a sub-system of the ntpq control message protocols. This service logs remote events in programmes.

version - "Denies packets which do not correspond to the current NTP version."



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see *Chapter 5.3.4.6 Restart NTP*).

5.3.4.8 Symmetric Key

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
NTP Info System Info Kernel Info Peers Basic Configuration Server Configuration Extended Configuration Restart NTP	on s	ymmetric Keys Control Key Symmetric Keys Add Remove Key ID	MD5 Key				
Security Access Restrict Symmetric Key Autokey	ions S						

5.3.4.8.1 Why Authentication?

Most NTP users do not require authentication as the protocol contains several filters (for bad time).

Despite this, however, the use of authentication is common. There are certain reasons for this:

- Time should only be used from safe sources
- An attacker broadcasts false time signals
- An attacker poses as another time server

5.3.4.8.2 How is Authentication used in the NTP Service?

Client and server can execute an authentication whereby a code word is used on the client side and a restriction on the server side.

NTP uses keys to implement the authentication. These keys are used when data are exchanged between two machines.

In principle both sides must know this key. The key can generally be found in the "*.*/etc/ntp.keys" directory. It is unencrypted and hidden from public view. This means that the key has to be distributed on a safe route to all communication partners. The key can be downloaded for distribution under "Downloads / Configuration Files" on the DEVICE tab. It is necessary to be logged in as "Master" in order to access this.

The keyword key of a client's ntp.conf determines the key that is used to communicate with the designated server (e.g. the **hopf** NTP Time Server 8030NTS/GPS). The key must be reliable if time is to be synchronised. Authentication causes a delay. This delay is automatically taken into account and adjusted in the current versions.

5.3.4.8.3 How is a key created?

A key is a sequence of up to 31 ASCII characters. Some characters with special significance cannot be used (alphanumeric characters and the following symbols can be used:[]()*-_! % & I = ?).

A new line can be inserted by pressing the $\boxed{\text{ADD}}$ key. The key which is stored in the key file is entered on this line. The key ID is used to identify the key and is in the range from 1 – 65534. This means that 65534 different keys can be defined.



Duplicate key ID's are not allowed. Having now explained the principles of keys, it should be possible to use a key in practically the same way as a password.

The value of the request key field is used as the password for the ntpdc tool while the value of the control key field is used as the password for the ntpq tool.

More information is available at http://www.ntp.org/.

5.3.4.8.4 How does authentication work?

The basic authentication is a digital signature and no data encryption (if there are any differences between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.

The receiver (which has the same key) carries out the same calculation and compares the results. Authentication has been successful if the results agree.

5.3.4.9 Autokey / Public Key Cryptography

NTPv4 offers a new Autokey scheme based on public key cryptography.

As a basic principle, **public key cryptography** is safer than **symmetric key cryptography** as protection is based on a private value which is generated by each host and is never visible.

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
	NTP Info System Info Kernel Info Peers		Autokey Configuration Autokey Enabled disabled V Autokey Password					
	Basic Configuration	n ration	Key Generation Generate Server Key Generate now					
[Security Access Restricti Symmetric Key Autokey	ions S	Upload Group Key		Durc	hsuchen		

In order to enable Autokey v2 authentication, the "Autokey Enabled" option must be set to "enabled" and a password specified (may not be blank).

A new server key and certificate can be generated by pressing the "Generate now" button.



Generate now

This should be carried out regularly as these keys are only valid for one year.

If the Board 7279(RC) is to form part of an NTP trust group, a group key can be defined and uploaded with the "Upload now" button.

Detailed information about the NTP Autokey scheme can be found in the NTP documentation (<u>http://www.ntp.org/</u>).



Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see *Chapter 5.3.4.6 Restart NTP*).



5.3.5 PTP Tab

This Tab shows information and adjustment possibilities of the PTP service of the Board 7279(RC).

PTP functionality is provided by a PTP-Demon running on the embedded Linux of the Board 7279(RC).

Depending on the receiving conditions and under unfavourable circumstances it may take several hours until long-term accuracy is obtained (normally 5-10 minutes).

The PTP-Demon is implemented according to standard IEEE 1588-2008. More detailed description of the adjustable value in the PTP tab and their effects on the PTP-Demon can be found in this standard.

PTP Onfiguration PTP Configuration PTP Enable	PTP Alarm Device Output	РТР	NTP	Network	Time/Date	General	
PTP Advanced Settings PTP Status Info: Enabling PTP turns NTP off PTP Interface ETH0 ∨ PTP Domain 0 PTP Priority 1 128 PTP Priority 2 128 PTP Priority 1 128 PTP Priority 2 128 PTP Profile IEEE C37.238 Power Profile ∨ Recommended Network Settings for PTP: Network interface operation mode: 100 Mbps / half duplex or 100 Mbps / full	PTP Alarm Device Output for PTP: e: pps / full	for PTP: le: bps / full	Profile V vork Settings peration mod olex or 100 M	Network	Time/Date	General PTP PTP Configurati PTP Advanced S PTP Status	



5.3.5.1 PTP Configuration

The "PTP Configuration" window provides basic settings of the PTP service.

General	Network	NTP	РТР	Alarm	Device	GPS Sync Source	Output	<
PTP PTP Configurati PTP IEEE C37.2 Power Profile S PTP Advanced 3 PTP Leap Secor	on 38 ettings 5ettings Id File	PTP Configura PTP Enable enabled V PTP Interface PRP0 V PTP Domain 0 PTP Priority 1 128 PTP Priority 2 128 PTP Profile IEEE C37.233 Recommend	tion 8 Power Profile ✓ ed Network Set]				
		Network inte 100 Mbps / I duplex	erface operation half duplex or 10	mode: D0 Mbps / ful	1			

PTP Enable

This option activates or deactivates the PTP service.

Remark: Changes in the "Network Interface ..." settings in the "NETWORK" tab, can lead to the deactivation of "PTP Enable".

Note: Enabling PTP automatically disables NTP. Then NTP only can be reactivated by disabling PTP.

PTP Interface

This option sets the network interface that is used by the PTP service.

The content of the drop down depends on the settings in the "NETWORK" tab.

If "NIC Bonding / Teaming active" is active, only "BOND0" can be chosen.

If "NIC PRP active" is active, only "PRP0" can be chosen.

If "NIC Bonding / Teaming active" and "NIC PRP active" are inactive, "ETH0" or "ETH1" can be chosen.

PTP Domain

This option controls the PTP domain.

• Value-range: 0 to 255



PTP Priority 1

This option controls the PTP priority 1.

• Value-range: 0 to 255

PTP Priority 2

This option controls the PTP priority 2.

• Value-range: 0 to 255

PTP Profile

This option supports the selection of predefined profiles. Either "None" or "IEEE C37.238 Power Profile" can be selected.

If "IEEE C37.238 Power Profile" is selected, all settings in the "PTP Advanced Settings" window are set according to the standard IEEE C37.238 and all the settings in that window cannot be modified.

If "None" is selected, the settings in the "PTP Advanced Settings" window can be modified.

5.3.5.2 PTP IEEE C37.238 Power Profile Settings

The "PTP IEEE C37.238 Power Profile Settings" window supplies settings for the IEEE C37.238 standard. They only affect the PTP service if the "IEEE C37.238 Power Profile" profile is selected in the "PTP Configuration" window.

General	Time/Date	Network	NTP	РТР	 Alarm	Device	Output
PTP PTP Configurati PTP Advanced S PTP Status	2n Siettings F E C P F C C P C C C P C C C P C C C P C C C P C C C P C C C P C C C C C P C	TP Advanced Settings Settings can not be C37.238 Power Profi TP Transport Sthernet / P2P TP sync interval (2^x) TP pdelay request int TP announce interval	changed if IE ile is activated : sec) erval (2^x sec) (2^x sec) (sec)*	EE d1		<u> </u>	

PTP Transport

This setting determines the network protocol that is used by the PTP service. Possible choices: " Ethernet / P2P", "Ethernet / E2E" und "IPv4 / E2E "



PTP sync interval (2^x sec)

This setting determines the sending interval of SYNC messages of the PTP service.

The sending interval is calculated in the following way:

- x ... selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -7 to 6

The sending interval can be chosen between 0.0078125 seconds up to 64 seconds.

PTP pdelay request interval (2[^] sec)

This setting determines the sending interval of Path Delay or Delay messages of the PTP service.

The sending interval is calculated in the following way:

- x ... selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -7 to 6

The sending interval can be chosen between 0.0078125 seconds up to 64 seconds.

PTP announce interval (2^x sec)

This setting determines the sending interval of Announce messages of the PTP service.

The sending interval is calculated in the following way:

- x ... selected value in the WebGUI
- Sending interval = 2^x
- Value-range: -4 to 6

The sending interval can be chosen between 0. 0625 seconds up to 64 seconds.

PTP announce timeout

This setting determines how many seconds the PTP service stays in the LISTENING state.

• Value-range: 2 to 255

The value entered corresponds to the seconds that the PTP service spends in the LISTENING state.



5.3.5.3 PTP Status

The status of the PTP service can be queried in this window.

To query status information, select the appropriate value from the PTP Status Query Type drop-down box and then press the Get PTP Status button.

The displayed information is identical to the retrievable information by means of the PTP program PMC.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
PTP PTP Configurati PTP Advanced S PTP Status	on Settings C C C C C C C C C C C C C C C C C C C	P Status IP Status Query Typp LOCK ACCURACY LOCK DESCRIPTIC SURRENT DATA SE DELAY MECHANISN JOMAIÑ SRANDMASTER SE OG ANNOUNCE OG SYNC INTERV OG SYNC INTERV OG SYNC INTERV ORT DATA SET VARENT DATA S	DN ET T T ITERVAL REQ_INTERVA AL T IP RTIES DATA_SET DPERTIES N	NL			



5.3.6 ALARM Tab

All the links within the tabs on the left-hand side lead to corresponding detailed setting options.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
Alarm Configurati	on Sy	slog Configuration]				
Syslog Configura eMail Configura SNMP Configura	ation S ation s	enabled V enabled V erver Identifier	d]			
Alarm Messages Alarm Message:	2 P	Iarm Level nfo v Iease note: Feature acilities are used for vithout a valid activ	e is not activa r diagnostic p ation key.	ated! Syslog ourposes only			

5.3.6.1 Syslog Configuration (Activation Key necessary)

It is necessary to enter the name or IPv4 or IPv6 address of a Syslog server in order to store every configured alarm situation which occurs on the Board in a Syslog. If everything is configured correctly and enabled (dependent on the Syslog level), every message is transmitted to the Syslog server and stored in the Syslog file there.

Syslog uses Port 514.

Co-logging on the Board itself is not possible as the flash memory is not of sufficient size.

It should be noted that the standard Syslog mechanism is used for this functionality. This is not the same as the Windows System Event mechanism!

General	Time	Network	NTP	Alarm	Device	Output	V Z D
Alarm Configurati Syslog Configur eMail Configura SNMP Configura	on ration tion ation	Syslog Configur Syslog Logging enabled V Server Name 192.168.100.	Enabled				
Alarm Messages	5	Alarm Level none info warning error alarm					

The alarm level designates the priority level of the messages to be transmitted and the level from which transmission has to take place (see *Chapter 5.3.6.4 Alarm Messages (Activation Key necessary)*).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01


5.3.6.2 E-mail Configuration (Activation Key necessary)

E-mail notification is one of the important features of this device which offers technical personnel the opportunity to monitor and/or control the IT environment.

It is possible to configure various, independent E-mail addresses which each have different alarm levels.

Depending on the configured level, an E-mail is sent to the respective receiver after an error has occurred.

A valid E-mail server (SMTP server) must be entered for the purpose of correct configuration.

Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

The Alarm Level designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 5.3.6.4 Alarm Messages (Activation Key necessary)**).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



5.3.6.3 SNMP Configuration / TRAP Configuration (Activation Key necessary)

It is possible to use an SNMP agent (with MIB) or to configure SNMP traps in order to monitor the Board over SNMP.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
Alarm Configurati Syslog Configura eMail Configura SNMP Configura Alarm Messages Alarm Message	on	SNMP Configuration SNMP Traps Enabled enabled Alarm Level info SNMP Traps Add Remove Host Name 122 168 100 55		Port Number	Community		
		Info: You have to ac	tivate SNMP nent menu to	service o use this feat	ure!		

SNMP traps are sent to the configured hosts over the network. It should be noted that these are based on UDP and therefore it is not certain that they will reach the configured host!

Several hosts can be configured. However, all have the same alarm level.

The private *hopf* enterprise MIB is also available over the web (see *Chapter 5.3.7.11 Down- loading SNMP MIB / Configuration Files*).

The "Alarm Level" designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 5.3.6.4 Alarm Messages (Activation Key necessary)**).

Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm



SNMP protocol must be enabled in order to use SNMP (see *Chapter* 5.3.3.7 *Management (Management-Protocols – HTTP, SNMP, SNMP, Traps, etc.)*).



5.3.6.4 Alarm Messages (Activation Key necessary)

Every message shown in the image can be configured with the displayed alarm levels. If level NONE is selected this means that this message is completely ignored.

	General	Time/Da	ate	Network	NTP	РТР	Alarm	Device	Output	
ſ	Alarm Configurati	ion	Ala	arm Messages						
Syslog Configuration eMail Configuration SNMP Configuration				essage ccuracy changed ynchronization sta		Alarm Level info V info V				
	Alarm Messages	s	N N Fi	TP System peer ha TP Stratum has ch irmware update ha	info ♥ info ♥ warning ♥					
				eapsecond has bee eboot by User has hanges made in th	n announced been initiateo e configuratio	- will take pla d on have been	ace with the next saved to flash dis	hour change	info none info warning error alarm	
			D n D	aylight saving time ext hour change aylight saving time	e change has e indicator ha	been announ s changed	ced - will take pla	ce with the	info V	
			D	aylight saving time	none V					

A corresponding action is carried out if an event occurs, depending on the messages, their configured levels and the configured notification levels of the E-mails.



Modified settings are failsafe stored after **Apply** and **Save** only.



5.3.7 DEVICE Tab

All the links within the tabs on the left-hand side lead to corresponding detailed setting options.

This tab provides the basic information about the module hardware and software/firmware. Password administration and the update services for the device are also made accessible via this website. The complete download zone is also a component of this site.

5.3.7.1 Device Information

All information is available exclusively in write-protected and read-only form. Information about the Board type, serial number and current software versions is provided to the user for service and enquiry purposes.

General	Time/Date	Network	NTP	РТР	Alarm	Device Output
Device	De	vice Info				
Device Info Hardware Info Factory Defaults Reboot Device Hardware Reset	D 7 0	evice Type 279RC evice Uptime days 21 hours 36 arial Number	minutes			
Image Update H8 Firmware Upd Upload Certificate Customized Secu	ate II 2 0 rity I	030019007 mage Version 4.00 (P2)				
Banner Product Activation Diagnostics		nage Program Date 7.01.2018				

5.3.7.2 Hardware Information

Read-only access is provided here in the same way as for device information.

The user requires this information in the case of service requests, e.g. MACH version, hard-ware status etc.

	General	Time/Dat	e Netwo	rk	NTP	РТР		Alarm	Devie	:e	Output	
ſ	Device		Hardware Info	7								
	Device Info Hardware Info Factory Default Reboot Device Hardware Rese Image Update H8 Firmware U Upload Certific Customized Se Banner Product Activat Diagnostics	s t pdate ate curity ion	Serial Number 8030019007 HB Firmware Ve 01.00 (14.02. HB status Normal operat HB uptime 0 days 21 hou MACH Firmware 12 Bridges	rsion 2018) ion rs 37 m Version	ninutes							
	Passwords Master Passwo Device Passwo Downloads SNMP MIB	rd rd	24 Card Layout 0 Special Program 0 Network Interfa 10/100/1000 Product-Config- 01803001900 Current DIP Sw	n MBit Au ID 700000	tosensing 418029999 ings	99010024	0118000	00011100	00100140	2180012		
	Configuration F	iles	1 OFF (2 DFF	3 OFF	4 OFF	5 OFF	6 OFF	7 OFF	8 ON		



5.3.7.3 Restoring Factory-Settings (Factory Defaults)

In some cases it might be wished to restore all settings of the Board 7279(RC) to their factorysettings (factory defaults).

General	Time/Date	Network	NTP	РТР	Alarm	Device Output
Device Info Hardware Info Factory Default: Reboot Device Hardware Resel Image Update H8 Firmware Up Upload Certifica Customized Sec	s Fa V R V r t t t t t t t t t t t t t t t t	ARNING WARNING ESET to factory of alues will be set ebootet immedia o reset to factory Reset now	lefaults is a to default - tely. Are you defaults no	critical acti the device v J sure you w W?	on, all vill be rant	

This function enables the restoring of all settings from the flash memory to their factory default values. This also affects passwords (see *Chapter 8 Factory Defaults*).

The registration is conducted as Master user according to the manual, *Chapter 5.2.1 LOGIN* and LOGOUT as User.

By pressing "Reset now" factory default values are set.

There is NO chance to restore the deleted configuration once this process is triggered.



After a **Factory Default** a complete verification and a possibly new configuration of the Board 7279(RC) are required. Especially the default MASTER and DEVICE passwords and the settings for system synchronization should be reset.

5.3.7.4 Reboot Device

General Tim	e/Date	Network	NTP	PTP	Alarm	Device Output
Device Device Info Hardware Info Factory Defaults Reboot Device Hardware Reset Image Update HB Firmware Update Upload Certificate	Re V R C T	boot Device VARNING! EBOOT is a critic hanges will be log eboot the device Reboot now	al action, al st. Are you s now?	l unsaved sure you wa	nt to	

All settings not saved with "Save" are lost on reset (see Chapter 5.2.3 Enter or Changing Data).

In broad terms, the **NTP service** implemented on the Board is restarted. This leads to a renewed alignment phase with the loss of the stability and accuracy reached up to this point.

Please log in as a "Master" user in accordance with the description in *Chapter 5.2.1 LOGIN* and LOGOUT as User.

Press the "Reset now" button and wait until the restart has been completed.

This procedure can take up to one minute. The website is not automatically updated.



5.3.7.5 Image Update & H8 Firmware Update

Patches and error recovery are provided for the individual boards by means of updates.

Both the embedded image and the H8 firmware can only be downloaded to the Board via the web interface (login as "Master" user required). See also *Chapter 3.4 Firmware Update*.

	The following points should be noted regarding updates:
	 Only experienced users or trained technical personnel should carry out an update after checking all necessary preconditions.
\checkmark	• Important: Faulty updates or update attempts may under certain circumstances require the Board to be returned to the factory for rectification at the owner's expense.
	• Check that the update on hand is suitable for your Board. If in doubt please consult the support of the <i>hopf</i> company.
	 In order to guarantee a correct update, the "New version of saved site" function must be set to "On each access to the site" in the In- ternet browser used.
	• During the update procedure, the device must not be switched off and settings must not be saved to the flash memory !
	• Updates are <u>always</u> executed as software set. I.e. H8 firmware up- date + image update. Unless specifically defined otherwise in the SET, it is absolutely essential to complete the H8 firmware update first, followed by the image update.
	 For the Update please pay attention to the points in Chapter 3.4 Firmware Update.

In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

Correct firmware and image designations are (e.g.):

H8-8030NTC_v0100_128. mot	for the H8 firmware (update takes approx. 1-1.5 minutes)
upgrade_8030_v0200_Release. img	for the embedded image (update takes approx. 7-8 minutes)



The update process is started by pressing the "**Update now**" button. The update is installed if the transfer and checksum test are successful. A success page is displayed and shows the number of bytes that have been transferred and installed.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
Device Info Hardware Info Factory Default Reboot Device Hardware Rese Image Update HB Firmware UJ Upload Certifica Customized Sec Banner	s t pdate curity	18 Firmware Update WARNING! H8 FIRMWARE UP ensure not to swit Device will be rebo Update file: Upload now	DATE is a cr ch off powe potet autom	ritical action er during up hatically afte	. Please oad! r update! hsuchen	Device	output
Product Activat	ion						

A restart of the Board with the new Firmware is done automatically after the H8-Firmware update.

The procedure for the **Image update** differs only in how the board is restarted.

	General	Time/Date	Network	NTP	РТР	Alarm	Device Output
-	General Device Info Hardware Info Factory Default Rebot Device Hardware Reset Image Update H8 Firmware Up Upload Certifica Customized See Banner Product Activati Diannostics	Time/Date	Network mage Update WARNING! IMAGE UPDATE is This action takes Please ensure not update! CAUTION: It is his operation mode o negotiate" during Update file:	NTP a critical ac several minu t o switch o ghly recomm f the networ update ope	PTP tion. utes! ff power dur nended to se rk interfaces ration! Durc	Alarm ing t the to "Auto hsuchen	Device Output
	Diagnostics		Update now				

After the image-update the WebGUI displays a window to confirm the restart (reboot) of the board.



5.3.7.6 Upload Certificate (SSL-Server-Certificate)

It is possible to encrypt the https connections to the 7052RC card with a user-supplied SSL server certificate.

General	Network	Alarm	Device	GPS	System		
	_						
evice		Upload Certificat	e				
Device Info		WARNING!					
<u>Hardware Info</u>		UPLOAD a Certificate is a critical action. Please ensure not to switch off power during upload and					
Factory Defaults							
<u>Reboot Device</u>		reboot after upload!					
<u>Hardware Reset</u>		Update file:					
<u>Image Update</u>				D	urchsuchen		
H8 Firmware Upda	ate						
Upload Certificate			7				
Customized Secur	ity	Upload now					
<u>Banner</u>							
Product Activation							



5.3.7.7 Customized Security Banner

Special security information displayed in the General tab can be entered here by the user.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
General Device Info Hardware Info Factory Default Reboot Device Hardware Resel Image Update H8 Firmware Up	Time/Date	Network stomized Security B ecurity Banner Text (his is a Security Ba General Tab!	NTP anner for Gene max. 2000 cha anner Text for	PTP ral Tab racters)* r special custo	Alarm	Device	Output
Passwords Passwords Master Password Master Password	tte curity ion						~

The security information can be written as 'unformatted' text as well as in HTML format. There are 2000 characters available to write failsafe into the device.

When saving the text, only the following characters are accepted (all other characters are discarded and therefore not displayed on the General page!):

- Capital letters (A...Z)
- Lowercase letters (a...z)
- Numbers (0...9)
- The following special characters: space (" "), exclamation mark ("!"), Comma (","), dot ("."), Colon (":"), question mark ("?")

nik GmbH			/ •		© 2005-201	7 rdcs.eu	
General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
	Time, bute	network			Alum	Device	output

After a successful storage the "Customized Security Banner" with the saved security information is displayed in the General-Tab.

To delete the "Customized Security Banner" the inserted text must be deleted and saved again.



82 / 125

5.3.7.8 Product Activation

For the activation of optional functions, e.g "Network Interface Bonding/Teaming", a special activation key is required for which an order with the *hopf* Elektronik GmbH can be placed. Each activation key is related to a special board with an appropriate serial number and cannot be used for several boards.



For a subsequent order of an activation key the serial number of the device needs to be provided. The serial number can be found under the tab DEVICE – Device info (serial number 8030...).



The settings for activation keys (e.g. an entered activation key) are neither deleted nor restored via the function FACTORY DEFAULTS.

General	Time/Dat	e Netwo	rk NTP	РТР	Alarm	Device	Output	
Device		Overview						
Device Info Hardware Info Factory Default Reboot Device Hardware Rese Image Update H8 Firmware U Upload Certific: Customized Se Banner Product Activat Diagnostics	s t pdate ate curity ion	Feature Static Routing Alarming and Network Inte IEC 62439-3 (PRP) IEEE 802.1Q IEEE 1588 Pr	g Table management feat rface Bonding/Tear Parallel Redundan Tagged VLAN ecision Time Proto	ures ming cy Protocol col (PTP)	StatusActivInactiveN/AInactiveN/AInactiveN/AInactiveN/AInactiveN/A	ration Key		
Passwords Master Password Device Password	rd rd		on Key					
Downloads SNMP MIB Configuration F	iles	Key Reset WARNING The activate want to read again. Perform Ke	! d features won't :tivate this featu :y Reset now	: be available res you will	e anymore after have to enter th	reset. If you le activation key	5	

Overview

Full listing of all optional functions with the current activation status and stored activation key

Activate Feature

Input field to enter a new activation key. After entering the feature is activated by pressing the \square Apply button.

If the activation was successful the new feature is listed in the overview with status "Active" and can be used immediately.

Key Reset

Clears all activation keys and sets all optional features to status "Inactive". All other non-optional features are still available after performing the key reset. If an optional feature is enabled again, the last stored configuration for this feature is restored.

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.7.9 Diagnostics Function

If "status messages" is enabled the output is processed as SYSLOG message. This function should only be used/enabled in case a problem arises and after consulting the *hopf* support.

General	Time/Date	Network	NTP	РТР	Alarm	Device Output
Device	R	eal Time Diagnostics				
<u>Device Info</u> <u>Hardware Info</u> Factory Default	<u>s</u>	disabled 🗸				
Reboot Device						
Hardware Reset	H	ardware Log				
H8 Firmware Up	odate I	Download Hardware Lo	og			
Upload Certifica	ite 🛛	Click here to a	<u>lownload</u>			
Customized Sec Banner Product Activati Diagnostics	ion	Refresh Hardwar	e Log			

5.3.7.10 **Passwords Master / Device**

Differentiation is made between capital letters and lower-case characters in passwords. In principle, all alphanumeric characters and the following symbols are allowed in passwords:

[]()*-_!\$%&/=?

(See also Chapter 5.2.1 LOGIN and LOGOUT as User)
Change Master Password
Current password
New password (min. 6 characters)
Confirm new password
Info: New passwords must contain a upper case character (AZ), a lower case character (az) and a number (09)



A new password must contain at least one capital letter and lowercase letter, a number, and six characters.



5.3.7.11 Downloading SNMP MIB / Configuration Files

The "private *hopf* enterprise MIB" is available via the WebGUI in this area.

	General	Time/Date	Networl	NTP	РТР	Alarm	Device	Output
ſ	Device	(SNMP MIB					
	Device Info		Download hopf72	79/RC MIB				
	Hardware Info			<u>o downioad</u>				
	Factory Default	<u>s</u> [
	Report Device							
	Image Lindate	<u> </u>						
	H8 Firmware U	pdate						
	Upload Certifica	ate						
	Customized Sec	curity						
	Banner							
	Product Activat	ion						
	<u>Diagnostics</u>							
ſ	Passwords							
-	1 43500143							
	Master Passwor	rd l						
	Device Passwor	rd 🛛						
L								
_								
-	Downloads							
	SNMP MIB							
	Configuration F	iles						

In order to be able to download certain configuration files via the web interface it is necessary to be logged on as a "Master" user.

	General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
ſ	Device	ĺ	Configuration Files					
	Device Device Info Hardware Info Factory Default Reboot Device Hardware Rese Image Update H8 Firmware UI Upload Certifica Customized Ser Banner Product Activat Diagnostics Passwords Master Passwor Device Passwor Downloads SNMP MIB Configuration F	s t pdate ate curity ion	Configuration Files Download NTP-Config Click here to de Download NTP-Keyfile Click here to de Click here to de Click here to de Download NTP Group- Click here to de Device Configuration Download Device Configuration Click here to de Refresh Device C	urationfile ownload Key (IFF) ownload iguration download	<u>n</u>			



5.3.8 OUTPUT Tab

This chapter describes the additional output functions of the Board 7279(RC).



Subsequent activation of the Output functionality is **<u>not</u>** possible on site.

5.3.8.1 DCF77

The signal generation for the output of a DCF77 pulse (1Hz) may be configured in this panel.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
DCF77 01 DCF77 - 01 Serial Interface Serial Interface	- 01	DCF77 - 01 Timebase Local ✓ Output if blocked 2Hz-Pulse ✓ Minimum SyncStatu: QUSE - Time crystal TimeOFF timer (0-65: 0 0 0 0 0 0 0 0 0 0 0 0 0	s for Output after reset or sa 535 min.) Ou S1 S2 n	et manually Current 0 tput inverted S3 S4 S	- TimeOFF time 5 56 57	▼ r value S8	
						, .	

5.3.8.1.1 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general, the local time is set as the base. This time leaps forward/back 1 hour every daylightsaving time changeover. The standard or UTC time must be selected as the base if automatic daylight-saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.



5.3.8.1.2 Output if blocked

Using this menu item the interference reaction of the DCF77 pulse can be controlled unless the system status is lower than the reference value.

Fault signal	2 Hz Pulse: If the system status is lower than the reference value, a 2Hz pulse instead of the DCF77 pulse is provided.
	No Signal If the system status is lower than the reference value there is <u>no</u> signal output.



Transmission of a 2Hz pulse in the event of a fault allows the connected devices to monitor for line breakage.

5.3.8.1.3 Minimum Sync.-Status for Output

The signal output can be adjusted only to be generated when the Sync Module has reached a minimum synchronization status. As soon as this minimum synchronization status drops below this value during operation, the signal output stops unless the TimeOFF Timer has been set greater than 0. In this case the output is done for the duration of the TimeOFF Timer despite the minimum synchronization status for the output falls below the set value.

Range of Sync.-Status

The synchronization status is represented from the bottom of the following table up with increasing quality.

Synchronisation Status	SYNC	Time synchronized + quartz control started/running
	SYOF	Time synchronized + SyncOFF running
	SYSI	Time synchronized as simulation mode (with no actual GPS reception)
	QUON	Quartz/crystal time + SyncON running
	QUEX	Quartz/crystal time (in freewheel after synchronization failure
	QUSE	Quartz/crystal time after reset or manually set
	INVA	Invalid time

Value range TimeOFF timer = 0 to 65635min.

5.3.8.1.4 Status of the Signal Output

The status of the output is stated via a display element with the following color and text indications:

GREEN	OUTPUT active	There is a signal output
YELLOW	OUTPUT + TimeOFF active	There is a signal output for the duration of the TimeOFF Timer
RED	OUTPUT blocked	There is no signal output

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.8.1.5 Output inverted

All outputs stated in the system manuals of the according devices are related to the DEFAULT setting: Output not inverted.

If nevertheless the inverting of the output signal has to be configured the "Output inverted" checkbox has to be enabled.

5.3.8.1.6 Special Configuration

If used, the correct settings are described in the additional system manual of the customerspecific device.

Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

5.3.8.2 Serial Interface

The serial data string generation may be configured in this panel.

General	Time/Date	Network	NTP	РТР	Alarm	Device	Output
DCF77		Serial Interface - 01 Serial Interface: Tra	nsmit and Recei	ve (RxD and TxE))		
Serial Interface Serial Interface	<u>- 01</u>	Baudrate 9600 V Parity none V Serial time String hopf Master/Slave-St Timebase	ring V	Databits	5		
		Local V Transmission - Charae with second forerun / Transmission - Point i every minute V	teristics control charact n time S1 S2	er delayed eve S3 S4 S	ry second V	58	
		Special Configuratio	n 🗌 🗌		Generat	or: 8030019007 / V	'01.00



5.3.8.2.1 Serial Interface



Data strings are available by selection to change automatically the serial parameter.

Baud Rate

- 9600 baud
- 1200 baud
- 4800 baud
- 9600 baud
- 19200 baud
- 38400 baud
- 57600 baud
- 115000 baud

Databits

Possible settings are:

- 8 for 8 databits
- 7 for 7 databits

Parity

Possible settings are:

- No Parity
- Even Parity
- Odd Parity

Stopbits

Possible settings are:

- 1 for 1 stopbit
- 2 for 2 stopbits



5.3.8.2.2 Timebase

Timebase	Local Time
	Standard Time
	UTC Time

In general, the local time is set as the base. This time leaps forward/back 1 hour every daylightsaving time changeover. The standard or UTC time must be selected as the base if automatic daylight-saving time changeover shall be suppressed.

When setting standard time (winter time), the time offset to local summer time is minus 1 hour. Standard time runs continuously (without time leap) throughout the whole year.

When setting UTC, the world time (formerly GMT) is used as the time base. This time base also runs continuously (without time leap) throughout the whole year.

5.3.8.2.3 Output scheme

The output scheme for the transmission must be selected here:

- Without second forerun / immediate control character
- With second forerun / immediate control character
- With second forerun / control character every second
- With second forerun / control character delayed every second

5.3.8.2.4 Transmission Time

- Every Second
- Every Minute
- Every Hour
- Remote

5.3.8.2.5 Special Configuration

If used, the correct settings are described in the additional system manual of the customerspecific device.

Otherwise for S1-S8 the DEFAULT-setting (all checkboxes disabled) should not be changed due to compatibility reasons.

5.3.8.2.6 Serial time String

The string output for the transmission must be selected here:

- *hopf* Binary String
- hopf Master/Slave-String
- hopf Standard String (6021)
- Trimble Time String (TSIP)
- SINEC H1 Extended
- SAT 1703 Time String
- ABB Melody (CR/LF)
- ABB Melody (LF/CR)
- ABB Freelance



5.3.8.2.6.1 *hopf* Binary String

The *hopf* Binary String can be used to synchronize slave systems with the time data of the master system.

Required:	Transmission Time every second
	 With second forerun / control character every second
	UTC time
	 9600 baud, 8 bit, 1 stop bit, no parity

Example:

```
(STX):TIME:80;0233D88F08;07E0;003C;F4108014*6B(CR)(LF) (ETX)
```

5.3.8.2.6.2 hopf Master/Slave-String

The *hopf* Master/Slave-String can be used to synchronize slave systems with the time data of the master system.

The *hopf* Master/Slave-String transmits:

- the full time information (hour, minute, second)
- the date (day, month, year [2 digits])
- the difference time local to UTC (hour, minute)
- the day of the week
- status information (announcement of DST changeover, announcement of a leap second and the status of reception of the *hopf* Master/Slave-String source)

5.3.8.2.6.2.1 Specified Settings

Required:	The following settings are required for the synchronization of the <i>hopf</i> slave-systems:
	output second forerun
	 ETX on the second change; selectable: data string at the beginning or at the end of the 59. second.
	local time
	 9600 baud, 8 bit, 1 stop bit, no parity



Received data on the serial interface that are not specified in the pertinent data string might disturb and interrupt the cyclic string output. The receiving synchronization interface should be set to "transmitting on request" for Sub-Master (Slave) Systems.



5.3.8.2.6.2.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status	\$30-39, \$41-46
3	day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	difference time tens hour / operational sign	\$30-31, \$38-39
17	difference time unit hour	\$30-39
18	difference time tens minutes	\$30-35
19	difference time unit minutes	\$30-39
20	LF (line feed)	\$0A
21	CR (carriage Return)	\$0D
22	ETX (end of text)	\$03

The difference time (time zone offset) is transmitted in hours and minutes following the year. The transmission is done in BCD. The difference time may be up to $\pm 14.00h$.

The operational sign is shown as the highest bit in the hours.

logic $\mathbf{1}$ = local time before UTC logic $\mathbf{0}$ = local time after UTC

Example:

Data String	Tens Difference Time Nibble	Difference Time
(STX)83123456030196 <u>0</u> 300(LF)(CR)(ETX)	<u>0000</u>	- 03:00h
(STX)83123456030196 <u>1</u> 100(LF)(CR)(ETX)	<u>0001</u>	- 11:00h
(STX)83123456030196 <u>8</u> 230(LF)(CR)(ETX)	<u>1000</u>	+ 02:30h
(STX)83123456030196 <u>9</u> 100(LF)(CR)(ETX)	<u>1001</u>	+ 11:00h

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



5.3.8.2.6.2.3 Status

	b3 b2 b1 b0 Meaning										
Status	х	х	х	0		no an	nouncement hour				
			х	х	1		annou	uncement (DST chang	jeover)		
		х	х	0	х		stand	standard time			
		х	х	1	х		daylig	daylight saving time (DST)			
		х	0	х	х		no announcement leap second				
		х	1	х	х		annou	announcement leap second			
		0	х	х	x		synchronization status code: INVA / QUSE / QUEX / QUON				
		1	х	х	х		synchronization status code: SYOF / SYNC				
Day of the	Week:	0	0	0	1		Monday				
		0	0	1	0		Tuesc	lay			
		0	0	1	1		Wedn	esday			
		0	1	0	0		Thurs	day			
		0	1	0	1		Friday	/			
		0	1	1	0		Sature	day			
		0	1	1	1		Sunda	ау			
Chatria	Onerstin	. Ma	مام		T :			DCT change over	Leen Cecend		
Status			ae		Time			DST changeover	Leap Second		
0 = 0000	0 = 0000 INVA / QUSE / QUEX / QUON				standard time			no announcement	no announcement		
1 = 0001 INVA / QUSE / QUEX / QUON			2	standard time			announcement	no announcement			
2 = 0010 INVA / QUSE / QUEX / QUON				DST			no announcement	no announcement			
3 = 0011 INVA / QUSE / QUEX / QUON				DST			announcement	no announcement			
4 = 0100 INVA / QUSE / OUEX / QUON				standard time			no announcement	announcement			
5 = 0101	INVA / QU QUEX / Q	JSE /	' 		standard time			announcement	announcement		
6 = 0110	INVA / QU QUEX / Q	JSE /	' 		DST			no announcement	announcement		
7 = 0111 INVA / QUSE / QUEX / QUON				DST			announcement	announcement			
8 = 1000 SYOF / SYNC				standard time		me	no announcement	no announcement			
9 = 1001 SYOF / SYNC			stand	ard ti	me	announcement	no announcement				
A = 1010 SYOF / SYNC			DST			no announcement	no announcement				
B = 1011 SYOF / SYNC			DST			announcement	no announcement				
C = 1100	SYOF / S	YNC			stand	ard ti	me	no announcement	announcement		
D = 1101	SYOF / S	YNC			stand	ard ti	me	announcement	announcement		
E = 1110	SYOF / S	YNC			DST			no announcement	announcement		
F = 1111 SYOF / SYNC				DST			announcement	announcement			

DST = daylight saving time

5.3.8.2.6.2.4 Example

(STX)841234561807028230(LF)(CR)(ETX)

- It is Thursday 18.07.2002 12:34:56 o'clock
- synchronization status code: SYNC
- no announcement of a changeover
- The difference time to UTC is +2.30 h



5.3.8.2.6.3 *hopf* Standard String (6021)

Below the *hopf* Standard String is described.

5.3.8.2.6.3.1 Specified Settings

Required: no	
--------------	--

5.3.8.2.6.3.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	LF (line feed)	\$0A
17	CR (carriage return)	\$0D
18	ETX (end of text)	\$03

5.3.8.2.6.3.3 Status

The second and the third ASCII-character contain the status and the day of the week. The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	х	Х	х	0	no announcement hour
	х	Х	х	1	announcement (DST changeover)
	х	Х	0	х	standard time
	х	х	1	х	daylight saving time (DST)
	0	0	х	х	synchronization status code: INVA
	0	1	х	х	synchronization status code: QUSE / QUEX / QUON
	1	0	х	х	synchronization status code: SYOF
	1	1	х	х	synchronization status code: SYNC
Day of the Week:	0	х	х	х	CEST / CET
	1	Х	х	х	UTC - time
	х	0	0	1	Monday
	х	0	1	0	Tuesday
	х	0	1	1	Wednesday
	х	1	0	0	Thursday
	х	1	0	1	Friday
	х	1	1	0	Saturday
	х	1	1	1	Sunday



Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

5.3.8.2.6.3.4 Example

(STX)E4123456180702(LF)(CR)(ETX)

- It is Thursday 18.07.2002 12:34:56 o'clock.
- synchronization status code: SYNC
- daylight saving time
- no announcement of a changeover
- () ASCII-control characters e.g. (STX)

5.3.8.2.6.4 Trimble Time String (TSIP)

The Trimble Time String (TSIP) can be used to synchronize slave systems with the time data of the master system.

Example in Hex description (not ASCII):

10	8F	0 B	00	00	41	0A	49	00	00	00	00	00	13	04	07	E0	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	10	03										



5.3.8.2.6.5 SINEC H1 Extended

Below the data string SINEC H1 Extended is described.

String request

The data string SINEC H1 Extended can also be sent by request. The time of output shall be configured to "send only by request" and the string will be requested with the ASCII character "?".

5.3.8.2.6.5.1 Specified Settings

Required:	no

5.3.8.2.6.5.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	"D" ASCII D	\$44
3	":" colon	\$3A
4	tens day	\$30-33
5	unit day	\$30-39
6	"." point	\$2E
7	tens month	\$30-31
8	unit month	\$30-39
9	"." point	\$2E
10	tens year	\$30-39
11	unit year	\$30-39
12	";" semicolon	\$3B
13	"T" ASCII T	\$54
14	":" colon	\$3A
15	day of the week	\$31-37
16	";" semicolon	\$3B
17	"U" ASCII U	\$55
18	":" colon	\$3A
19	tens hour	\$30-32
20	unit hour	\$30-39
21	"." point	\$2E
22	tens minute	\$30-35
23	unit minutes	\$30-39
24	"." point	\$2E
25	tens second	\$30-36
26	unit second	\$30-39
27	";" semicolon	\$3B
28	"#" or " " (space)	\$23 / \$20
29	"*" or " " (space)	\$2A / \$20
30	"S", "U" or " " (space)	\$53 / \$55 / \$20
31	"!", "A" or " " (space)	\$21 / \$41 / \$20
32	ETX (end of text)	\$03



5.3.8.2.6.5.3 Status

The characters 28-31 in the data string SINEC H1 Extended tell the synchronization status of the device.

The characters mean the following:

character no. 28 = "#" " " (space)	no synchronisation after reset, time invalid "synchronization status code: INVA" synchronisation after reset, clock in crystal operation "synchronization status code: QUSE / QUEX / QUON / SYOF / SYNC"
character no. 29 = "*" " " (space)	time from internal crystal in the clock "synch. status code: INVA / QUSE / QUEX / QUON" time by synchronisation "synchronization status code: SYOF / SYNC"
character no. 30 = "S"	daylight saving time
"U"	UTC
" " (space)	standard time
character no. 31 = "!"	announcement of a DST or standard time changeover
"A"	announcement of a leap second
" " (space)	no announcement

5.3.8.2.6.5.4 Example

(STX)D:18.07.02;T:4;U:12.34.56; _ _ _ (ETX) (_) = Space

- It is Thursday 18.07.02 12:34:56 o'clock •
- The clock is synchronous (synchronization status code: SYNC) •
- standard time (winter time) •
- no announcement of a changeover •



5.3.8.2.6.6 SAT 1703 Time String

All modes can be transmitted with the SAT 1703 Time String (e.g. with forerun or end character at second change).

The SAT 1703 Time String can also be sent on request. The point of transmission shall be set to "transmission on request". The String may be requested with ASCII-character "?".

5.3.8.2.6.6.1 Specified Settings

Required:	no

5.3.8.2.6.6.2 Structure

Character No.	Meaning	Hex-Value			
1	STX (start of text)	\$02			
2	tens day	\$30-33			
3	unit day		\$30-39		
4			\$2E		
5	tens month		\$30-31		
6	unit month		\$30-39		
7	=.		\$2E		
8	tens year		\$30-39		
9	unit year		\$30-39		
10	"/"		\$2F		
11	unit day of the week		\$31-37		
12	"/"		\$2F		
13	tens hours		\$30-32		
14	unit hours	\$30-39			
15	"." ·	\$3A			
16	tens minutes	\$30-35			
17	unit minutes	\$30-39			
18	"."	\$3A			
19	tens seconds	\$30-35			
20	unit seconds		\$30-39		
21	"M" or "M" or "U"		\$4D, \$4D, \$55		
22	"E" or "E" or "T"	(Standard time,	\$45, \$45, \$54		
23	"Z" or "S" or "C"	or UTC)	\$5A, \$53, \$43		
24	" " or "Z" or " "		\$20, \$5A, \$20		
25	" " (\$20 ⇔ synchronous	\$20			
	"*" (\$2A ⇔ not synchron	\$2A			
26	" " (\$20 ⇔ no announce	ement) or	\$20		
	"!" (\$21 ⇔ announceme	\$21			
27	CR (corrigge return)	e changeover)			
21			\$0D		
28			φυΑ ¢02		
29	EIX		ФU3		



5.3.8.2.6.6.3 Status

The characters 21-26 in the SAT 1703 Time String indicate the synchronisation status.

The characters mean the following:

Character no. 21-24 =	"MESZ" "MEZ " "UTC "	Central European Summertime (Daylight Saving Time) Central European Time (standard time / winter time) Coordinated Universal Time
Character no. 25 =	"*"	time from internal crystal in the clock "synchronization status code: INVA / QUSE / QUEX / QUON"
	" " (space)	time by synchronisation "synchronization status code: SYOF / SYNC"
Character no. 26 =	"!" " " (space)	announcement of a DST or standard time changeover no announcement

5.3.8.2.6.6.4 Example

(STX)18.07.02/4/02:34:45UTC_ _ (CR)(LF)(ETX)

- It is Thursday 18.07.02 02:34:45 o'clock UTC
- The clock is synchronous (synchronization status code: SYNC)



5.3.8.2.6.7 ABB Melody (CR/LF)

Below the ABB Melody DataString is described.

5.3.8.2.6.7.1 Specified Settings

Required:	The following settings are required for the synchronization:
	Output every minute
	Output without second forerun
	Output without ETX on the second change
	UTC time
	 9600 baud, 8 bit, 2 stop bit, parity even

5.3.8.2.6.7.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	CR (carriage return)	\$0D
17	LF (line feed)	\$0A
18	ETX (end of text)	\$03



5.3.8.2.6.7.3 Status

The second and the third ASCII-character contain the status and the day of the week. The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	х	Х	х	0	no announcement hour
	х	Х	х	1	announcement (DST changeover)
	х	х	0	х	standard time
	х	Х	1	х	daylight saving time (DST)
	0	0	х	х	synchronization status code: INVA
	0	1	х	х	synchronization status code: QUSE / QUEX / QUON
	1	0	х	х	synchronization status code: SYOF
	1	1	х	х	synchronization status code: SYNC
Day of the Week:	0	х	х	х	CEST / CET
	1	х	х	х	UTC - time
	х	0	0	1	Monday
	х	0	1	0	Tuesday
	х	0	1	1	Wednesday
	х	1	0	0	Thursday
	х	1	0	1	Friday
	х	1	1	0	Saturday
	х	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

5.3.8.2.6.7.4 Example

(STX)CC123456210416(CR)(LF)(ETX)

- It is Thursday 21.04.2016 12:34:56 o'clock.
- synchronization status code: SYNC
- UTC
- no announcement of a changeover
- () ASCII-control characters e.g. (STX)



5.3.8.2.6.8 ABB Melody (LF/CR)

Below the ABB Melody DataString is described.

5.3.8.2.6.8.1 Specified Settings

Required:	The following settings are required for the synchronization:
	Output every minute
	Output without second forerun
	Output without ETX on the second change
	UTC time
	 9600 baud, 8 bit, 2 stop bit, parity even

5.3.8.2.6.8.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday 7=Sunday) for UTC time bit 3 is set to 1 in the day of the week	\$31-37
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	LF (line feed)	\$0A
17	CR (carriage return)	\$0D
18	ETX (end of text)	\$03



5.3.8.2.6.8.3 Status

The second and the third ASCII-character contain the status and the day of the week. The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	Х	Х	х	0	no announcement hour
	Х	х	х	1	announcement (DST changeover)
	Х	х	0	х	standard time
	х	Х	1	х	daylight saving time (DST)
	0	0	х	х	synchronization status code: INVA
	0	1	х	х	synchronization status code: QUSE / QUEX / QUON
	1	0	х	х	synchronization status code: SYOF
	1	1	х	х	synchronization status code: SYNC
Day of the Week:	0	х	х	х	CEST / CET
	1	Х	х	х	UTC - time
	х	0	0	1	Monday
	Х	0	1	0	Tuesday
	х	0	1	1	Wednesday
	х	1	0	0	Thursday
	х	1	0	1	Friday
	х	1	1	0	Saturday
	Х	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

5.3.8.2.6.8.4 Example

(STX)CD123456220416(LF)(CR)(ETX)

- It is Friday 22.04.2016 12:34:56 o'clock.
- synchronization status code: SYNC
- UTC
- no announcement of a changeover
- () ASCII-control characters e.g. (STX)



5.3.8.2.6.9 ABB Freelance

Below the ABB Freelance DataString is described.

5.3.8.2.6.9.1 Specified Settings

Pre-settings	The following settings are required for the synchronization:
at string selection:	Output at minute change
	Output with second forerun
	 Output with ETX on the second change
	UTC time
	 9600 baud, 8 bit, 1 stop bit, no parity



These settings are activated when the freelance string is selected newly, that is: beforehand, another string must have been activated! While the Freelance string is active, the settings can be changed. The changed settings will be kept if a reset is released.

5.3.8.2.6.9.2 Structure

Character No.	Meaning	Hex-Value
1	STX (start of text)	\$02
2	status (internal clock status)	\$30-39, \$41-46
3	day of the week (1=Monday 7=Sunday)	\$31-37
	for UTC time bit 3 is set to 1 in the day of the week	
4	tens hour	\$30-32
5	unit hour	\$30-39
6	tens minute	\$30-35
7	unit minute	\$30-39
8	tens second	\$30-36
9	unit second	\$30-39
10	tens day	\$30-33
11	unit day	\$30-39
12	tens month	\$30-31
13	unit month	\$30-39
14	tens year	\$30-39
15	unit year	\$30-39
16	CR (carriage return)	\$0D
17	LF (line feed)	\$0A
18	ETX (end of text)	\$03



5.3.8.2.6.9.3 Status

The second and the third ASCII-character contain the status and the day of the week. The status is decoded binary.

	b3	b2	b1	b0	Meaning
Status:	Х	Х	х	0	no announcement hour
	Х	Х	х	1	announcement (DST changeover)
	Х	Х	0	х	standard time
	х	Х	1	х	daylight saving time (DST)
	0	0	х	х	synchronization status code: INVA
	0	1	х	х	synchronization status code: QUSE / QUEX / QUON
	1	0	х	х	synchronization status code: SYOF
	1	1	х	х	synchronization status code: SYNC
Day of the Week:	0	Х	х	х	CEST / CET
	1	Х	х	х	UTC - time
	х	0	0	1	Monday
	Х	0	1	0	Tuesday
	Х	0	1	1	Wednesday
	х	1	0	0	Thursday
	х	1	0	1	Friday
	х	1	1	0	Saturday
	Х	1	1	1	Sunday

Status	operation mode	time	announcement SZ-WZ-SZ
0 = 0000	INVA	winter	no announcement
1 = 0001	INVA	winter	announcement
2 = 0010	INVA	summer	no announcement
3 = 0011	INVA	summer	announcement
4 = 0100	QUSE / QUEX / QUON	winter	no announcement
5 = 0101	QUSE / QUEX / QUON	winter	announcement
6 = 0110	QUSE / QUEX / QUON	summer	no announcement
7 = 0111	QUSE / QUEX / QUON	summer	announcement
8 = 1000	SYOF	winter	no announcement
9 = 1001	SYOF	winter	announcement
A = 1010	SYOF	summer	no announcement
B = 1011	SYOF	summer	announcement
C = 1100	SYNC	winter	no announcement
D = 1101	SYNC	winter	announcement
E = 1110	SYNC	summer	no announcement
F = 1111	SYNC	summer	announcement

5.3.8.2.6.9.4 Example

(STX)CC123456210416(CR)(LF)(ETX)

- It is Thursday 21.04.2016 12:34:56 o'clock.
- synchronization status code: SYNC
- UTC
- no announcement of a changeover
- () ASCII-control characters e.g. (STX)



_

×

6 SSH and Telnet Basic Configuration



Only basic configuration is possible via SSH or Telnet. The complete configuration of the device takes place exclusively via the WebGUI.

It is just as easy to use SSH (Port 22) or Telnet (Port 23) as the WebGUI. Both protocols use the same user interface and menu structure.

The user names and passwords are the same as on the WebGUI and are kept in alignment (see *Chapter 5.3.7.10 Passwords Master / Device*).



SSH does not allow blank passwords for safety reasons.



The corresponding protocols should be enabled for the use of Telnet or SSH (see *Chapter 5.3.3.7 Management (Management-Protocols – HTTP, SNMP, SNMP-Traps, etc.)*).

```
🗬 192.168.180.135 - PuTTY
```

```
login as: master
master@192.168.180.135's password:
     N N TTTTTTT CCCCC
     NN N T
                    C
                          C
     N N N
                    С
               Т
     N N N
               Т
                     С
              Т
       NN
                     C
                          C
     Ν
        N
                      CCCCC
     Ν
              Т
     Hopf 8030 Network Time Client (c) 2009
     Press Enter to continue
Main Menu
 1 ... General
 2 ... Network
 3 ... Alarm
 4 ... NTP
 5 ... Device Info
 0 ... Exit
Choose a Number =>
```

The navigation through the menu takes place by entering the respective number associated with the menu option (as can be seen in the above image).



7 Technical Data



The company *hopf* reserves the right to hardware and software alterations at any time.

General	
Operation	via WebGUI
Installation Position	any position
Protection Type of Board	IP00
Dimensions of Module	Multi-layer board 80mm x 60mm
Power Supply	5V DC \pm 5% (via internal plug-in connectors)
MTBF	> 1,250,000h
Weight	Approx. 0.1kg

Temperature Range	
Operation	0° C to +50° C
Storage	-20° C to +75° C
Humidity	max. 90%, non condensing

Power Consumption - internal	
Normal operation	typ. 550 mA (max. 850 mA)
Boot phase	typ. 550 mA (max. 850 mA)

LAN - ETH0/ETH1	
Network connection	Via a LAN cable with RJ45 connector, male (recommended cable type CAT5 or better)
Request per second	Max. 6,250 requests (during operation in GigaBit net- works under optimum network conditions)
Number of connectable Clients	Theoretically unlimited
Network interface ETH0	10/100/1000 Base-T
Ethernet compatibility	Version 2.0 / IEEE 802.3
Isolation voltage (Network- to system side)	1500 Vrms
Boot time:	typ.: 35 seconds - When using static IP addresses for ETH0 and ETH1. De- pending on the network configuration in use (e.g. DHCP) an extension of the boot phase can occur.

CE Conformity		
EMV Directive 2004/108/EC		
EN 55022 : 2006 + A1 : 2007		
EN 61000-3-2 : 2006 + A2 : 2009, EN 61000-3-3 : 2008		
EN 55024 : 1998+A1 : 2001+A2 : 2003		
Low Voltage Directive 2006/95/EC		
EN 60950-1 : 2006		

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



NTP Accuracy	Accuracy Value	
LOW	Lambda > 20 msec	
MEDIUM	Lambda < 20 msec	
HIGH	Lambda < 20 msec AND stability < 0.8 pp	

Time Protocols

- NTPv4 Server
- NTP Broadcast Mode
- NTP Multicast Mode
- NTP Client for additional NTP Servers (Redundancy)
- SNTP Server
- NTP Symmetric Key Encryption
- NTP Autokey Encryption
- NTP Access Restrictions
- IEEE 1588 Precision Time Protocol (PTP)

TCP/IP Network Protocols

- HTTP
- FTP
- Telnet
- SSH
- SNMP
- NTP
- PTP

Configuration

- HTTP WebGUI (Browser Based)
- Telnet
- SSH
- hmc Network Configuration Assistent

Features

- HTTP (status, control)
- SNMPv2c, SNMPv3, SNMP Traps (MIB-II, Private Enterprise MIB)
- E-mail Notification
- Syslog Messages to External Syslog Server
- Update over TCP/IP
- Fail-safe
- Watchdog
- Power Management
- System Management
- IEEE 802.1Q Tagged VLAN
- IEC 62439-3 Parallel Redundancy Protocol (PRP)
- Network Interface Bonding/Teaming



8

Factory Defaults Usually the delivery status of the Board 7279(RC) corresponds with the factory-defaults.

8.1 Network

Host/Name Service	Setting	WebGUI Presentation
Hostname	hopf8030ntc	hopf8030ntc
Use Manual DNS Entries	Enabled	Enabled
DNS Server 1 IPv4/IPv6 Address	Blank	
DNS Server 2 IPv4/IPv6 Address	Blank	
DNS Server 3 IPv4/IPv6 Address	Blank	
Use Manual Gateway Entries	Enabled	Enabled
Default Gateway IPv4-Adresse	Blank	
Default Gateway IPv6-Adresse	Blank	
Network Interface ETH0	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	
DHCP	Disabled	Disabled
IPv4	192.168.0.1	192.168.0.1
IPv4 Netmask	255.255.255.0	255.255.255.0
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
IPv6 settings	Disabled	Disabled
Network Interface ETH1	Setting	WebGUI
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	
DHCP	Enabled	Enabled
IPv4	Blank	
IPv4 Netmask	Blank	
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	Disabled	Disabled
IPv6 settings	Disabled	Disabled
Bonding	Setting	WebGUI
Network Interface Bonding/Teaming	Disabled	Disabled
PRP	Setting	WebGUI
Network Interface PRP	Disabled	Disabled
Routing	Setting	WebGUI
Use Route File	Disabled	Disabled
User Defined Routes	Disabled	Disabled
Management	Setting	WebGUI
НТТР	Enabled	Enabled
HTTPS	Disabled	Disabled
SSH	Enabled	Enabled
TELNET	Disabled	Disabled
SNMP	Disabled	Disabled
System Location	Blank	
System Contact	Blank	
Read Only Community	public	public
Read/Write Community	secret	secret
Security Name	Blank	
Access Rights	Readonly	Readonly
Authentication Protocol	MD5	MD5
Authentication Passphrase	Blank	
Privacy Protocol	DES	DES
Privacy Passphrase	Blank	

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01


8.2 NTP

NTP Server Configuration	Setting	WebGUI
Additional NTP Servers	Blank	
Authentication	Disabled	None
Key ID	Blank	
Peer	Blank	
Broadcast/Multicast Mode	Disabled	Disabled
Multicast Client address	Blank	
NTP Client Configuration	Setting	WebGUI
Lambda	20ms	20ms
Accuracy	HIGH	HIGH
NTP Access Restrictions	Setting	WebGUI
Access Restrictions		Default no modify
NTP Symmetric Keys	Setting	WebGUI
Request Key	Blank	
Control Key	Blank	
Symmetric Keys	Blank	
NTP Autokey	Setting	WebGUI
Autokey	Disabled	Disabled
Password	Blank	

8.3 PTP

PTP Configuration	Setting	WebGUI
PTP Enabled	Disabled	Disabled
PTP Interface	ETH0	ETH0
PTP Domain	0	0
PTP Priority 1	128	128
PTP Priority 2	128	128
PTP Profile	IEEE C37.238 Power Profile	IEEE C37.238 Power Profile
PTP IEEE C37.238 Power Profile Settings	Setting	WebGUI
PTP Grandmaster ID	3	3
Time Zone Name	UTC	UTC
PTP Advanced Settings	Setting	WebGUI
PTP Transport	Ethernet / P2P	Ethernet / P2P
PTP sync interval (2 ^x sec)	1 second	0
PTP delay request interval (2 ^x sec)	1 second	0
PTP announce interval (2 ^x sec)	1 second	0
PTP announce timeout (sec)	2 second	2



8.4 ALARM

Syslog Configuration	Setting	WebGUI
Syslog	Disabled	Disabled
Server Name	Blank	
Alarm Level	Disabled	None
E-mail Configuration	Setting	WebGUI
E-mail Notifications	Disabled	Disabled
SMTP Server	Blank	
Sender Address	Blank	
E-mail Addresses	Blank	
SNMP Traps Configuration	Setting	WebGUI
SNMP Traps	Disabled	Disabled
Alarm Level	Disabled	None
SNMP Trap Receivers	Blank	
Alarm Messages	Setting	WebGUI
Alarms	All disabled	All none

8.5 DEVICE

User Passwords	Setting	WebGUI	
Master Password	master		
Device Password	device		

8.6 DCF77 - 01

Timebase	Local
Output if blocked	2Hz-Pulse
Minimum SyncStatus for Output	QUSE – Time Crystal after reset or set manually
TimeOFF timer (0 - 65535 min.)	0

8.7 Serial Interface - 01

Baudrate	9600
Databits	8
Parity	None
Stopbits	1
Serial Time String	hopf Binary String
Timebase	UTC
Transmission - Characteristics	Without second forerun / immediate control character
Transmission - Point in time	Every second



Glossary and Abbreviations 9

NTP-specific Terminology 9.1

Stability	The average frequency stability of the clock system.
Accuracy	Specifies the accuracy in comparison to other clocks.
Precision of a clock	Specifies how precisely the stability and accuracy of a clock system can be maintained.
Offset	This value represents the time difference between two clocks. It is the offset by which the local time would have to be adjusted in order to keep it congruent with the reference clock.
Clock skew	The frequency difference between two clocks (first derivative of offset over time).
Drift	Real clocks vary in frequency difference (second derivative of offset over time). This variation is known as drift.
Roundtrip delay	Roundtrip delay of an NTP message to the reference and back.
Dispersion	Represents the maximum error of the local clock relative to the reference clock.
Jitter	The estimated time error of the system clock measured as the average exponential value of the time offset.

Tally Codes (NTP-specific) 9.2

space	reject	Rejected peer – either the peer is not reachable or its syn- chronization distance is too great.
x	falsetick	The peer was picked out by the NTP intersection algorithm as a false time supplier.
	excess	The peer was picked out by the NTP sort algorithm as a weak time supplier on the basis of synchronization distance (concerns the first 10 peers).
-	outlyer	The peer was picked out by the NTP clustering algorithm as an outlyer.
+	candidate	The peer was selected as a candidate for the NTP combining algorithm.
#	selected	The peer is of good quality but not among the first six peers selected by the sort algorithm on the basis of synchronization distance.
*	sys.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System.
0	pps.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System. The current synchroni- zation is derived from a PPS (pulse-per-second) signal either indirectly via PPS reference clock driver or directly via kernel interface.



9.2.1 Time-specific expressions

UTC	UTC Time (Universal Time Coordinated) was depending on the Greenwich Mean Time (GMT) definition of the zero meridian. While GMT follows astrological calculations, UTC is based on the stability and accuracy of the Caesium standard. The leap second was defined in order to cover this deviation.
Time Zone	The globe was originally divided into 24 longitudinal seg- ments or time zones. Today, however, there are a number of time zones which in part apply specifically to certain indi- vidual countries only.
	In relation to the time zones, consideration was given to the fact that local daylight and sunlight coincide at different times in the individual time zones.
	The zero meridian runs through the British city of Green- wich.
Time Offset	This is the difference between UTC and the valid standard time of the current time zone. The Time Offset will be commit from the local time zone.
Local Standard Time	Standard Time = UTC + Time Offset
(winter time)	The time offset is defined by the local time zone and the lo- cal political regulations.
Daylight Saving Time	Offset of Daylight Saving Time = + 1h
(summer time)	Daylight Saving Time was introduced to reduce the energy requirement in some countries. In this case one hour is added to the standard time during the summer months.
Local Time	Local Time = Standard Time if exists with summer / winter time changeover
Leap Second	A leap second is a second which is added to the official time (UTC) in order to synchronise this with Greenwich Mean Time when required. Leap seconds are defined internationally by the Interna- tional Earth Rotation and Reference Systems Service (IERS).



9.3 Abbreviations

D, DST	Daylight Saving Time
ETH0	Ethernet Interface 0
ETH1	Ethernet Interface 1
FW	Firmware
GPS	Global Positioning System
HW	Hardware
IF	Interface
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NTP	Network Time Protocol
NE	Network Element
OEM	Original Equipment Manufacturer
OS	Operating System
RFC	Request for Comments
SNMP	Simple Network Management Protocol (handled by more than 60 RFCs)
SNTP	Simple Network Time Protocol
S, STD	Standard Time
ТСР	Transmission Control Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
ToD	Time of Day
UDP	User Datagram Protocol http://de.wikipedia.org/wiki/User_Datagram_Protocol
UTC	Universal Time Coordinated
WAN	Wide Area Network
msec	millisecond (10 ⁻³ seconds)
µsec	microsecond (10 ⁻⁶ seconds)
ppm	parts per million (10 ⁻⁶)



9.4 Definitions

An explanation of the terms used in this document.

9.4.1 DHCP (Dynamic Host Configuration Protocol)

DHCP makes it possible to integrate a new computer into an existing network with no additional configuration. It is only necessary to set the automatic reference of the IP address on the client. Without DHCP, relatively complex settings need to be made. Beside the IP address, further parameters such as network mask, gateway and DNS server have to be entered. A DHCP server can assign these parameters automatically by DHCP when starting a new computer (DHCP client).

DHCP is an extension of the BOOTP protocol. A valid IP address is allocated automatically if a DHCP server is available on the network and DHCP is enabled.



See RFC 2131 Dynamic Host Configuration Protocol for further information.

9.4.2 NTP (Network Time Protocol)

Network Time Protocol (NTP) is a standard for the synchronization of clocks in computer systems via packet-based communication networks. Although it is processed mainly over UDP, it can also be transported by other layer 4 protocols such as TCP. It was specially developed to facilitate reliable timing via networks with variable packet runtime.

NTP uses the Marzullo algorithm (devised by Keith Marzullo of the San Diego University in his dissertation) with a UTC timescale and supports leap seconds from Version 4.0. NTP. It is one of the oldest TCP/IP protocols still in use. It was developed by David Mills of the University of Delaware and published in 1985. The protocol and UNIX implementation continue to be developed under his direction. Version 4 is the up to date version of the protocol. This uses UDP Port 123.

NTPv4 can maintain the local time of a system to an accuracy of some 10 milliseconds via the public Internet. Accuracies of 500 microseconds and better are possible under ideal conditions on local networks.

With a sufficiently stable, local clock generator (oven-stabilised quartz, rubidium oscillator, etc.) and using the kernel PLL (see above), the phase error between reference clock generator and local clock can be reduced to something of the order of a few hundred microseconds. NTP automatically compensates for the drift of the local clock.

NTP can be installed over firewalls and offers a range of security functions.



See RFC 5905 for further information.



9.4.3 SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is a network protocol which was developed by the IETF in order to be able to monitor and control network elements from a central station. This protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the composition of the data packets which can be transmitted and the communication procedure. SNMP was designed in such a way that can be provided by SNMP include:

- Monitoring of network components
- Remote control and configuration of network components
- Fault detection and notification

Due to its simplicity, SNMP has become the standard which is supported by most management programmes. SNMP Versions 1 and 2c hardly offer any safety mechanisms. The safety mechanisms have been significantly expanded in the current Version 3.

Using description files, so-called MIB's (Management Information Base), the management programmes are able to represent the hierarchical structure of the data of any SNMP agent and to request data from them. In addition to the MIB's defined in the RFC's, every software and hardware manufacturer can define his own so-called private MIB's which reflect the special characteristics of his product.

9.4.4 TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP and IP are generally used concurrently and thus the term TCP/IP has become established as the standard for both protocols.

IP is based on network layer 3 (layer 3) in the OSI Layer Model whereas TCP is based on layer 4, the transport layer. In other words, the expression TCP/IP signifies network communication in which the TCP transport mechanism is used to distribute or deliver data over IP networks. As a simple example: Web browsers use TCP/IP to communicate with web servers.

9.5 Accuracy & NTP/PTP Basic Principles



NTP and PTP are network protocols. Transmission delays and errors as well as the loss of data packets can lead to unpredictable accuracy data and time synchronization effects.



NTP and PTP protocols neither defines nor guarantees the accuracy or correctness of the time server.

Thus the QoS (Quality of Service) used for direct synchronization with GPS or serial interface does not apply to synchronization via NTP and PTP.

In simplified terms, during synchronization with NTP accuracies of between 1msec and 1sec can be expected, depending on the accuracies of the servers used. PTP uses a better algorithm to compensate for network delays, so with PTP it is possible to achieve an accuracy of 0.5 µs. Problems in the network can also lead to greater inaccuracies with PTP.



The accuracy of network-based time synchronization is depending on the following criteria:

- Characteristics and accuracy of the time server / time signal used
- Characteristics of the sub-network
- Characteristics and quality of the synchronization client
- The algorithm used

NTP and PTP has a variety of algorithms to equalise the possible characteristics of IP networks. Algorithms also exist to equalise the offset between reference time source and the local clock.

However, under some circumstances it is not possible to provide an algorithmic solution.

For example:

- Time servers which do not deliver <u>any</u> correct time cannot be detected at all. The only
 option available to NTP is to mark these time servers as FALSETICKERS in comparison to other time servers and to disregard them. However, this means that if only 2
 time servers are configured, NTP has no way of determining the correctness of the
 individual times and clearly identifying which time is incorrect.
- 2. Asymmetries in the transmission between NTP servers and NTP clients as well as between PTP Grandmaster and PTP slave can neither be measured nor calculated by NTP/PTP. NTP/PTP works on the assumption that the transmission path to the NTP server/PTP Grandmaster is exactly as long as the return path. The NTP algorithm can only filter out changes on a statistical basis. The use of several servers makes it possible for the combining algorithm to pick up and filter out any such errors. However, there is no possibility of filtering if this asymmetry is present on all or most of the NTP servers (faulty routing etc).
- 3. It goes without saying that the accuracy of the synchronised time cannot be better than the accuracy resolution of the local clock on the NTP server and NTP client resp. PTP Grandmaster and PTP Slave.

With reference to the above mentioned error circumstances, the delivered **time offset** of the NTP/PTP should be considered to be at best the most favourable case and in no way to be a value that takes account of all possible errors.

In order to resolve this problem, NTP delivers the maximum possible error in relation to the offset. This value is designated as the synchronization distance ("LAMBDA") and is the sum of the **Root Dispersion** and half of the **Root Delay** of all NTP servers used. This value describes the worst possible case and thus the maximum error that can be expected.

Finally, please note that the user of the Time Server is responsible for the network conditions between the Time Server and the NTP clients resp. PTP Grandmaster and PTP Slave.

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronization) of 50msec occurs. The synchronised clients will therefore NEVER achieve accuracy values of one millisecond or even microseconds!

The accuracy value in the GENERAL tab of the WebGUI is designed to help the user to estimate the accuracy.



10 List of RFCs

- NTPv4 Protocol and Algorithms Specification (RFC 5905)
- NTPv4 Autokey Specification (RFC 5906)
- PPS API (RFC 2783)
- DHCP (RFC 2131)
- Time Protocol (RFC 868)
- Daytime Protocol (RFC 867)
- HTTP (RFC 2616)
- HTTPS (RFC 2818)
- SSH-2 (RFC 4250-4256, 4335, 4344, 4345, 4419, 4432, 4716, 5656)
- TELNET (RFC 854)
- SNMPv2c (RFC 1213, RFC1901-1908)
- SNMPv3 (RFC 3410)
- SYSLOG (RFC 5424)
- SMTP (RFC 5321)



11 List of Open Source Packages used

Third Party Software

The Board 7279(RC) includes a numerous of software packages subject to other license conditions. In case the use of such a software package might violate the licence conditions immediately after written notice it is ensured that the underlying licence conditions are met again.

If the underlying licence conditions relating to a specific software package require availability of the source code the package is provided electronically (email, download etc.) on requested.

The following table includes all used software packages with the applicable underlying software license conditions:

Package name	Version	Licence	Licence details	Patches
boost	1.60.0		http://www.boost.org/LICENSE_1_0.txt	no
busybox	1.24.1	GPL	v2	no
bzip2	1.0.6	BSD		no
can-utils	f0abaaacb0 a3f620f73dd 6fd716d7da a3c36a8e3	GPL	v2	no
cifs-utils	6.4	GPL	v3	no
dhcpcd	6.10.1	BSD		no
dhcpdump	1.8		 Copyright 2001, 2002 by Edwin Groothuis, edwin@mavetju.org All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IM-PLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABIL-ITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDI-RECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF AD-WISED OF THE POSSIBILITY OF SUICH DAMAGE 	no
dosfstools	3.0.28	GPL	v3	no
eeprog	0.7.6	GPL	v2+	no
ethtool	4.2	GPL	v2	no
exfat	1.2.3	GPL	v2+	no
exfat-utils	1.2.3	GPL	v2+	no

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01



Package name	Version	Licence	Licence details	Patches
freetype	2.6.2	GPL	v2	no
gd	2.1.1	BSD		no
genext2fs	1.4.1	-		no
gzip	1.6	GPL	v2	no
host-autoconf	2.69	GPL	v3	no
host-au- tomake	1.15	GPL	v2	no
host-bison	3.0.4	GPL	v3	no
host-dos2unix	7.3.1	BSD		no
host- e2fsprogs	1.42.13	GPL	v2	no
host-flex	2.5.37		Flex carries the copyright used for BSD software, slightly	no

Flex carries the copyright used for BSD software, slightly no modified because it originated at the Lawrence Berkeley (not Livermore!) Laboratory, which operates under a contract with the Department of Energy:

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007 The Flex Project.

Copyright (c) 1990, 1997 The Regents of the University of California.

All rights reserved.

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITH-OUT ANY EXPRESS OR IMPLIED WARRANTIES, IN-CLUDING, WITHOUT LIMITATION, THE IMPLIED WAR-RANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This basically says "do whatever you please with this software except remove this notice or take advantage of the University's (or the flex authors') name".

Note that the "flex.skl" scanner skeleton carries no copyright notice. You are free to do whatever you please with scanners generated using flex; for them, you are not even bound by the above copyright.

host-gen- ext2fs	1.4.1	GPL	v2	no
host-gettext	0.19.7	GPL	v3	no
host-kmod	22	LGPL	v2.1	no

7279(RC) Network Time Client with 2 LAN Interfaces - V04.01

hopf Elektronik GmbH Nottebohmstr. 41 • D-58511 Lüdenscheid • Tel.: +49 (0)2351 9386-86 • Fax: +49 (0)2351 9386-93 • Internet: http://www.hopf.com • E-Mail: info@hopf.com



Package name	Version	Licence	Licence details	Patches
host-libffi	3.2.1		libffi - Copyright (c) 1996-2014 Anthony Green, Red Hat, Inc and others. See source files for details.	no
			Permission is hereby granted, free of charge, to any per- son obtaining a copy of this software and associated doc- umentation files (the ``Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:	
			The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.	
			THE SOFTWARE IS PROVIDED ``AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, IN- CLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIA- BILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.	
host-libglib2	2.46.2	LGPL	v2	no
host-libtool	2.46	GPL	v2	no
host-libxml2	2.9.3		Copyright (C) 1998-2012 Daniel Veillard All Rights Reserved. Permission is hereby granted, free of charge, to any per- son obtaining a copy of this software and associated doc- umentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, IN- CLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIA- BILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE LISE	no
host-Izo	2.09	GPL	V2	no
host-m4	1.4.17	GPL	v3	no
host-mtd	1.5.2	GPL	v2	no
host-ncurses	5.9		Copyright (c) 1998-2010,2011 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any per-	no
			son obtaining a copy of this software and associated doc- umentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the	



Package name	Version	Licence	Licence details	Patches
			Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:	
			The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.	
			THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, IN- CLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CON- NECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.	
			Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.	
host-omap-u- boot-utils	0.2.1	GPL	v2	no
host-pkgconf	0.9.12		Copyright (c) 2011, 2012, 2013, 2014, 2015 pkgconf au- thors (see AUTHORS). Permission to use, copy, modify, and/or distribute this soft- ware for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permis-	no
			sion notice appear in all copies. This software is provided 'as is' and without any warranty, express or implied. In no event shall the authors be liable for any damages arising from the use of this software.	
host-uboot- tools	2016.01	GPL	v2+	no
host-zlib	1.2.8		Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler	no
			This software is provided 'as-is', without any express or im- plied warranty. In no event will the authors be held liable for any damages arising from the use of this software.	
			Permission is granted to anyone to use this software for any purpose, including commercial applications, and to al- ter it and redistribute it freely, subject to the following re- strictions:	
			 The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledg- ment in the product documentation would be appreci- ated but is not required. 	
			2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.	
			3. This notice may not be removed or altered from any source distribution.	
hwdata	0.267	GPL	v2	no
i2c-tools	3.1.2	GPL	v2	no
igmpproxy	0.1	GPL	v2	no
ipkg	0.99.163	GPL	v2	no
iproute2	4.4.0	GPL	v2	no
iptables	1.6.0	GPL		no



Package name	Version	Licence	Licence details	Patches
iputils	2.4.10	GPL	v2	no
latencytop	0.5	GPL	v2	no
libarchive	3.1.2	BSD		no
libevent	2.0.22	3-clause BSD	http://libevent.org/LICENSE.txt	no
libffi	3.2.1	MIT License		no
libfuse	2.9.5	GPL		no
libglib2	2.46.2	LGPL	v2+	no
libnl	3.2.27	GPL		no
linux	4.1.13- g8dc6617	GPL	v2	yes
linuxptp	1.8	GPL	v2	yes
libpcap	1.7.4	2-clause BSD		no
libpng	1.6.21		http://www.libpng.org/pub/png/src/libpng-LICENSE.txt	no
libselinux	2.1.13			
libsepol	2.1.9	LGPL	v2.1	
libserial	0.6.0rc2	GPL	v3	no
libserialport	0.1.1	GPL	v3	no
libsocketcan	0.0.10	LGPL	v2.1	no
libsysfs	2.1.0	LGPL	v2.1	no
libusb	1.0.19	LGPL	v2	no
libxml2	2.9.3	MIT License		no
libzip	0.11.2	BSD		no
lighttpd	1.4.39	3-clause BSD		no
Im-sensors	3.4.0	LGPL	v2.1	no
Ishw	B.02.17	GPL	v2	no
lua	5.3.2	MIT License		no
Izo	2.09	GPL	v2	no
Izop	1.03	GPL	v2	no
memstat	1.0	MIT License		no
mii-diag	2.11	GPL		no
minicom	2.7	GPL	v2	no
mmc-utils		GPL	v2	no
mtd	1.5.2	GPL	v2	no
nano	2.5.1	GPL		no
nanocom	1.0	GPL		no
ncftp	3.2.5		http://www.ncftp.com/ncftp/doc/LICENSE.txt	no
ncurses	5.9	Permissive free soft- ware licence	Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any per- son obtaining a copy of this software and associated doc- umentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:	no



Package name	Version	Licence	Licence details	Patches
			The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.	
			THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, IN- CLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CON- NECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.	
			Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.	
netsnmp	5.7.3	BSD (mehrere)	http://net-snmp.sourceforge.net/about/license.html	no
netstat-nat	1.4.10	GPL		no
ntp	4.2.8p11	NTP	Copyright (c) University of Delaware 1992-2011	yes (6)
			Permission to use, copy, modify, and distribute this soft- ware and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright no- tice and this permission notice appear in supporting docu- mentation, and that the name University of Delaware not be used in advertising or Publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is pro- vided "as is" without express or implied warranty.	
openssh	7.1p2	BSD		no
openssl	1.0.2g	Dual	http://www.openssl.org/source/license.html	no
opkg	0.3.1	GPL	v2	no
pcre	8.38	BSD		no
popt	1.16	GNU Free Documenta- tion License	V1.3	no
pps-tools	0deb9c7e13 5e9380a6d0 9e9d2e938a 146bb698c8	GPL	v2	no
prp	1.4	Permissive free soft- ware licence	Copyright (c) 2007, Institute of Embedded Systems at Zur- ich University of Applied Sciences (<u>http://ines.zhaw.ch</u>)	yes
			Redistribution and use in source and binary forms, with or without modification, are permitted provided that the fol- lowing conditions are met:	
			- Redistributions of source code must retain the above cop- yright notice, this list of conditions and the following dis- claimer.	
			- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.	
			- Neither the name of the Zurich University of Applied Sci- ences nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.	



Package name	Version	Licence	Licence details	Patches
rsync	3.1.2	GPL		no
setools	3.3.8	GPLv2, LGPLv2.1		no
setserial	2.17	GPL		no
spidev_test	V3.0	GPL	v2	no
sqlite	3100200	Public do- main		no
sshpass	1.05	GPL		no
start-stop- daemon	1.18.4	GPL	v2	no
statserial	1.1	GPL		no
sudo	1.8.15	ISC-style	http://www.sudo.ws/sudo/license.html	no
sysstat	11.2.0	GPL	v2	no
	354b5f3ad7 c723897f40 051fddee49		 served. All rights reserved. Base on code from Copyright (c) 2007, 2008, Johannes Berg johannes@sipsolutions.net Copyright (c) 2007, Andy Lutomirski Copyright (c) 2007, Mike Kershaw Copyright (c) 2008-2009, Luis R. Rodriguez mcgrof@gmail.com Redistribution and use in source and binary forms, with or without modification, are permitted provided that the fol- lowing conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * Neither the name Texas Instruments nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written per- mission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EX- PRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICU- LAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAM- AGES (INCLUDING, BUT NOT LIMITED TO, PROCURE- MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE_DATA_OR PROFITS: OR BUISINESS INTER- 	
			BILITY, OR TORT (INCLUDING NEGLIGENCE OR OTH- ERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSI- BILITY OF SUCH DAMAGE.	
uboot	2010.06	GPI	v2	no
uboot-tools	2016.01	GPI	v2	no



Package name	Version	Licence	Licence details	Patches
usb_modeswit ch	2.2.6	GPL	v2	no
usb_modeswit ch_data	20151101	GPL	v2	no
util-linux	2.27.1	GPL	v2	no
zlib	1.2.8	Permissive free soft- ware licence	http://www.gzip.org/zlib/zlib_license.html	no