Industriefunkuhren

hopf
Elektronik   GmbH

Technical Manual

NTP/SINEC H1 LAN Board

Model 7274 and 7274RC

for housing versions
1U / 3U / DIN-Rail

ENGLISH

Version: 04.00 – 25.04.2018

	SET	**IMAGE**	**FIRMWARE**
Valid for	Version: **04.xx**	Version: **04.xx**	Version: **03.xx**

Version Numbers (Firmware / Description)

THE TERM **SET** DEFINES THE FIXED RELATIONSHIP BETWEEN THE IMAGE VERSION AND THE ASSOCIATED 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 DESIGNATE THE SHARED FUNCTIONAL IDENTITY BETWEEN DEVICE, SOFTWARE AND TECHNICAL DESCRIPTION.

THE VERSION NUMBER OF THE IMAGE AND THE H8 SOFTWARE CAN BE READ IN THE WEBGUI OF BOARD 7274/7274RC (SEE *CHAPTER 6.3.6.1 Device Information* AND *CHAPTER 6.3.6.2 HARDWARE INFORMATION)*.

THE TWO DIGITS AFTER THE DOT IN THE VERSION NUMBER DESIGNATE CORRECTIONS TO THE FIRMWARE AND/OR DESCRIPTION WHICH HAVE NO EFFECT ON FUNCTIONALITY.

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: info@hopf.com

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 compliance with these regulations.

If these are not complied with, then no claims may be made under the terms of the warranty. No liability will be assumed for any ensuing damage.

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.

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

Contents   Page

1 Board Description 7274 and 7274RC

The LAN Boards 7274 and 7274RC are **Network Time Server** (*abbreviation* NTS) for the use in the modular *hopf* Systems 7001RC, 7001, 6844, 6844RC and 6855 and also in the non modular DIN Rail Systems such as GPS Module 6875.

> **i**
>
> Generally, the NTP/SINEC H1 LAN boards 7274 and 7274RC provide functions and fields of applications completely backward compatible to the boards 7272 and 7272RC.
>
> The boards 7274 and 7274RC can be used as direct replacements for already supplied boards 7272 or rather 7272RC. The successor boards provide all functions, adjustment options and protocols as offered by the boards 7272 and 7272RC.
>
> The successor boards are suitable for extensions of *hopf* Clock Systems, already operating boards 7272 or rather 7272RC (mixed operation) without problems.

The boards 7274 and 7274RC are equipped with two Ethernet interfaces (ETH0 and ETH1) 10/100/1000 Base-T (autosensing).

> **i**
>
> The boards 7274 and 7274RC supports operation in IPv4 and IPv6 networks.

The boards 7274 and 7274RC can be used by networks for highly accurate synchronisation over **NTP (Network Time Protocol)** which is available worldwide.

The following synchronisations protocols are available:

- NTP (including SNTP)
- SINEC H1 time datagram
- Daytime
- Time
- IEEE 1588 Precision Time Protocol (PTP) (Activation Key required)

The network connection of the LAN boards 7274 and 7274RC can be installed at any desired point on the network. Each board 7274/7274RC is a completely independent NTP Time Server.

Depending on the respective *hopf* system, a number of these LAN Boards can be implemented (even subsequently) in the Base System on a modular basis.

A variety of management and monitoring functions are available (e.g. SNMP traps, E-mail notification, Syslog messages).

Increased security is freely available via optional encryption methods such as symmetric keys, Autokey and access restrictions and the disabling of unused protocols.

Extensive parameters are provided to suit the conditions of individual applications by means of a variety of access / configuration channels.

- Depending on the clock system the accessibility of the LAN boards 7274 or 7274RC can be adjusted in the network via the keyboard of the *hopf* base system or via a *hmc* remote connection.

- The boards are completely configured over Ethernet by means of a web browser:
  - HTTP/HTTPS WebGUI (**G**raphical **U**ser **I**nterface)
  - Or text-based menus over Telnet and SSH

- Various protocols (e.g. IPv4, http, https, Telnet etc.) are available for the Ethernet connection.

The Board 7274(RC) currently has unlockable features that are described in *chapter 2.5 Activation of Functions (Activation Key)*:

- 7515RC Mains Frequency Data
- Network Interface Bonding/Teaming
- IEC 62439-3 Parallel Redundancy Protocol (PRP)
- IEEE 802.1Q Tagged VLAN
- IEEE 1588 Precision Time Protocol (PTP)

Overview of the functions of the network Time Server 7274(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
  - 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
- PPS Time Source
- SINEC H1 time datagram
- RFC-867 DAYTIME Server
- RFC-868 TIME Server
- Precision Time Protocol (PTP) according to IEEE Std 1588™-2008 **(Activation Key necessary)**
  - IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications (Power Profile) according to IEEE Std C37.238™-2011

Network Configuration
- DHCP
- Routing
- Bonding (NIC Teaming) Link aggregation according to IEEE 802.1ad (Activation Key necessary)
- VLAN support according to IEEE 802.1q (Activation Key necessary)
- PRP (Parallel Redundancy Protocol) according to IEC62439-3 (Activation Key necessary)

System Management (Activation Key necessary)
- E-mail notification
- Syslog messages to external syslog server
- SNMPv2c / SNMPv3, SNMP Traps (MIB-II, Private Enterprise MIB)

Configuration Channel
- HTTP/HTTPS WebGUI (browser-based)
- Telnet
- SSH
- External LAN configuration tool (*hmc* **- Network-Configuration-Assistant**)
- *hopf* 7001RC system *hmc*, keypad and display – Board 7274RC only
- *hopf* 7001 system keypad and display – Board 7274 only
- *hopf* 68xx system (3U/Slim Line) keypad and display – Board 7274 only
- *hmc* Remote connection (for basic systems with remote function)

Additionally at Board 7274RC
- Hot-plug functionality
- NTP accuracy message for status and error messages in system 7001RC

Additional Features
- Firmware Update via TCP/IP
- Fail-safe
- Watchdog circuit
- Power management
- System management
- Customized security banner

1.1 Differences between the Boards 7274 and 7274RC

The board 7274RC is identical in function to the board 7274 but designed for the use in System 7001RC. For this purpose the board 7274RC additionally provides "Hot-Plug" and appropriate internal interface functionality for the operation in a *hopf* 7001RC Base System.

> ⚠️ The boards 7274 and 7274RC should only be operated in the suitable Base Systems.
>
> The board 7274RC only works in a System 7001RC.

> ℹ️ As the boards 7274 and 7274RC are identical in their most important functions, the designation **7274(RC)** is used in this manual unless there is no different function of the boards.
>
> In case a function is only provided by one of the two boards just the designation of the appropriate board is used.

1.2 Overview of Assembly of Boards 7274(RC)
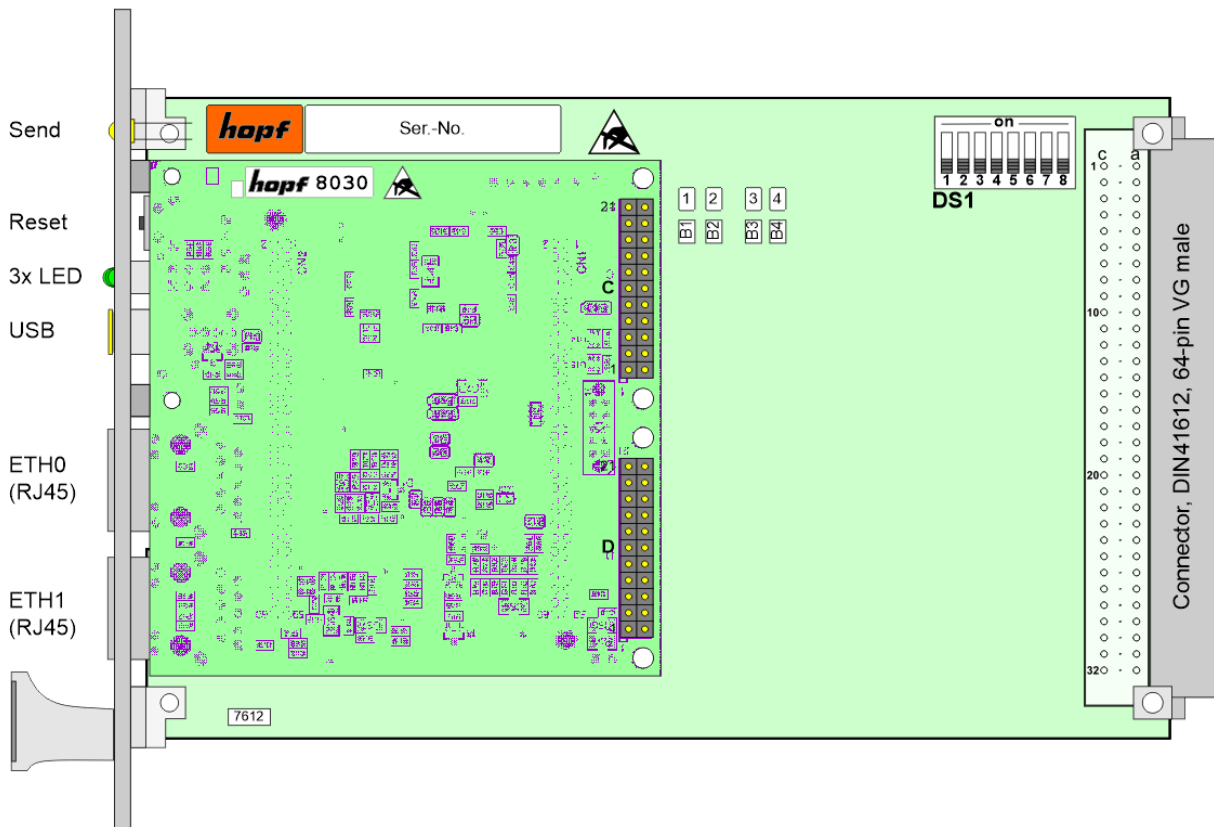
1.2.1 DIP Switch DS1

Depending on the type of board (7274 or 7274RC) the DIP switch DS1 is differently assigned.

1.2.1.1 Functions of the DIP Switch DS1 for Board 7274

The Base System in which the board is to be operated is set via DIP switch DS1. The board number in the Base System is also set here.

DIP Switch DS1	Function
8	Selection of the Base System 68xx or 7001 (see *Chapter 3.3 + 3.4*)
7	No function at present
6	Transmissions point of SINEC H1 time datagram (see *Chapter 6.3.2.8.3*)
5	
4	Board number in System 7001 / 68xx (see *Chapter 3.3.1 + 3.4.1*)
3	
2	
1	

1.2.1.2 Functions of the DIP Switch DS1 for Board 7274RC

Via DIP switch DS1 the board number in the Base System is set primary.

DIP Switch DS1	Function
8	No function at present
7	**Accuracy of the NTP** message 7274RC is used in the system 7001RC for the generation of status and error messages (see *Chapter 3.5.2*)
6	Transmissions point of SINEC H1 time datagram (see *Chapter 6.3.2.8.3*)
5	
4	Board number in System 7001RC (see *Chapter 3.5.1*)
3	
2	
1	

1.2.2 MAC Address for ETH0 and 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 WebGUI of the appropriate board or be evaluated via the **hmc Network Configuration Assistant.**

The MAC address for ETH1 is incremented hexadecimal by 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.

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

1.3   Front Panels of Boards for the Different Housing Versions

1.3.1   Overview of Functions of the Front Panel Elements

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

1.3.1.1 SEND LED (not at DIN-Rail)

SEND LED (yellow)	Description
Flashing / flickering	**Normal case** – indicates access to the internal system bus. Board 7274(RC) is correctly integrated into the respective System.
Off	Board 7274(RC) is not ready for operation.
On	Fault on Board 7274(RC).

> **i** As the DIN Rail Systems have no internal system bus, there is no SEND LED in the DIN Rail Systems available.

1.3.1.2 Reset Button (and Default Button)

The reset button is activated by means of a thin object through the hole in the front panel next to the "Reset" inscription (see **Chapter 2.3 Reset- (Default) Button**).

1.3.1.3 NTP Status LEDs (NTP/Stratum/Accuracy)
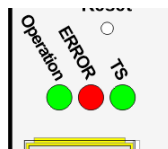
TS-LED (Green)	Time service of the Board 7274(RC)
On	**Standard**, running
Off	Not running
ERROR-LED (Red)	**Description**
Off	**Standard case**, Board 7274(RC) is working.
3Hz flashing	Fail-safe basic parameterization is not available (emergency operation mode)
On	Primary CPU of Board 7274(RC) does not show any activity.
Operation-LED (Green)	**Description**
On	**Standard case**, Board 7274(RC) is working
1Hz flashing	Board 7274(RC) is booting the operating system.
3Hz flashing	A firmware update (image) of Board 7274(RC) is going to be implemented.
Off	Board 7274(RC) is **not** ready for operation.

1.3.1.4 USB Female Connector (Host)
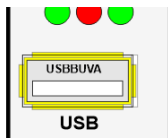
The USB connection can be used for certain problems and after consulting the *hopf* support for a System recovery.

1.3.1.5 LAN Interface ETH0/ETH1
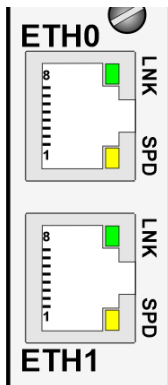
LNK LED (Green)	Description
Off	10 MBit Ethernet detected
On	100 MBit / 1 GBit Ethernet detected

SPD LED (Yellow)	Description
Off	No LAN connection to a network
On	LAN connection available
Flashes	Network activity at ETH0 (transmission / reception)

Pin No.	Assignment
1	TX_DA+
2	TX_DA-
3	RX_DB+
4	BI_DC+
5	BI_DC-
6	RX_DB-
7	BI_DD+
8	BI_DD-

1.3.2   Front Panel of Boards 7274 and 7274RC for 3U / 19" Racks

Board 7274
3U/4HP
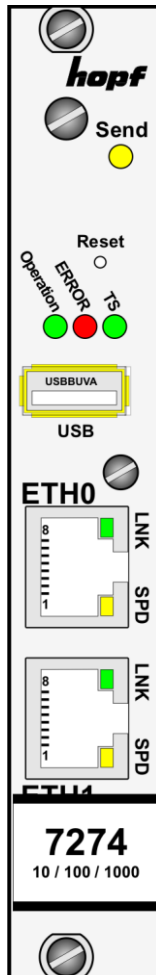
Board 7274RC
3U/4HP
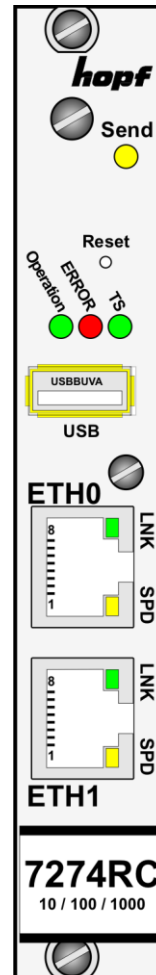
1.3.3   Front Panel of Board 7274 for 1U / 19" Racks (Slim Line)

Board 7274/1U
1U (Slim Line)
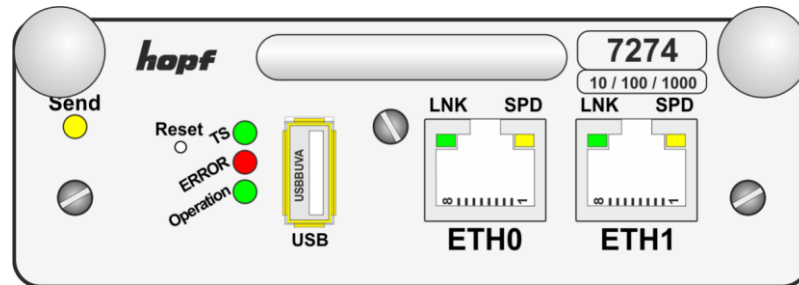
1.3.4   Front Panel of Board 7274 for DIN Rail Mounting

Board 7274DIN-Rail
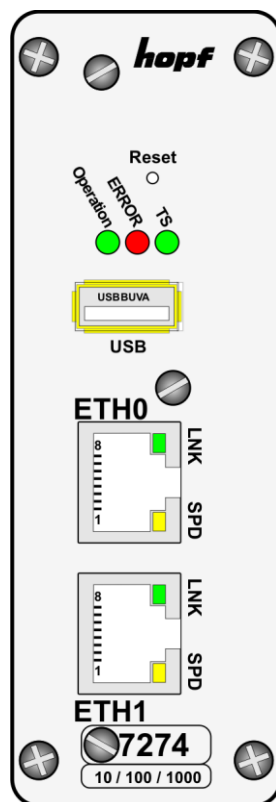
The board 7274DIN-Rail is non-modular pluggable. A replacement of board can only be done in the factory at company **hopf**.

2 System Behaviour of the Board 7274(RC)

In this chapter the behaviour of the boards in special operation phases is described.

2.1 Boot Process

The boot process of the board starts after turning on the Clock System the board is operated in or rather after a reset of the board.

During the boot process the board booting its operation system and is therefore not available via LAN.

2.2 NTP Regulating Phase (Stratum/Accuracy)

NTP is a regulation process. After start of the NTP services (automatically processed during booting) the board requires a certain period of time (usually 5-10 minutes) until NTP is set to the high accuracy of the Base System and reaches the optimized operation condition of **STRATUM = 1** and **ACCURACY = High**.

The decisive factors here are accuracy of the synchronization source and the appropriate synchronization condition of the clock System.

2.3 Reset- (Default) Button

The Board 7274(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.

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

Duration	Function
< 1 sec.	No action
1 - 9 sec.	After releasing a system wide **hardware reset** is triggered
>= 10 sec.	After releasing a **FACTORY DEFAULT** followed by a **REBOOT** is triggered after approx. 10 seconds

2.4 Firmware Update

The Board 7274(RC) is a multi processor system. For this reason a firmware update always consists of a so called Software SET including two (2) programs versions for the image and H8 programs defined by the Set-Version which both needed to be loaded into the board.

Board 7274(RC) (WebGUI: Device):

1x Image Update	upgrade_8030gen_rel_vXXXX.img
1x H8 Update	H8_8030_vXXXX_128.mot

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

All programs of a SET needed to be loaded to ensure a defined operation condition.

The assignment of program versions of a SET-Version may be taken from the Release-Notes of the software sets of Board 7274(RC) in cases of doubt.

2.4.1 Firmware Update Board 7274(RC) (WebGUI: Device)

The general process of a software update of Board 7274(RC) is described below:

For selection of the correct update set the identifier of Board 7274(RC) has to be observed obligatory.

Board 7274(RC) can be recognized:
- By the label on the front panel
- In WebGUI at the Web-banner "**7274(RC)**"

The firmware update 7274(RC) has to be performed as a SET.

The software package contained in the file package hopf7274_SET_vXXXX.zip has to be unpacked. The following steps have to be executed in the following sequence:

1. **Image Update 8030 (7274)**
2. **H8 Firmware Update 8030 (7274)**

Image Update 7274(RC)

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
   (Exapmle: **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 Module 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 7274(RC)

1. Log in as Master in WebGUI of the board.

2. Select in the **Device** tab the menu item **H8 Firmware Update**.

3. Select the file with the file extension **.mot for Board 7274(RC)** via the selection window (Example: **H8_8030_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 Module 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.

2.5   Activation of Functions (Activation Key)

The Board 7274(RC) offers several functions that require an "Activation Key".

These functions are only available after entering a valid activation key depending on the serial number of the particular Board 7274(RC), (not depending on the serial number of the entire clock system). The serial number can be found in the WebGUI via
Device / Serial Number: 8030xxxxxx.

The required function(s) can be activated at time of delivery as well as subsequently on site by the user.

Please find an overview of the above mentioned functions here:

- **Network Interface Bonding/Teaming**
  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.

- **IEC 62439-3 Parallel Redundancy Protocol (PRP)**
  The PRP functionality enables to bundle the physical network interfaces ETH0 and ETH1 to a logical network interface using the Parallel Redundancy Protocol (PRP).

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

- **IEEE 1588 Precision Time Protocol (PTP)**
  By activating this function Precision Time Protocol (PTP) according to IEEE Std 1588™-2008 can be configured.

- **7515RC Mains Frequency Data**
  This option allows the distribution of network time and network frequency over Ethernet from a 7515RC network frequency board located in the System 7001RC.

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

3 Implementing Board 7274(RC) in a modular *hopf* 19" Base System

Operation

An ESD conform handling and operation of the board has to be ensured!

Otherwise there is the danger that the board might get damaged through ESD (electrostatic discharge).
Damages to the board caused by improper handling are not covered by factory guaranty.

Electrical Properties

The function board 7274 **does not** support **Hot Plug**.

A change of boards **mandatorily** requires turn-off of System. Otherwise the System or the function boards might get damaged.

System Requirments

The boards 7274 und 7274RC are **function boards for the system bus.** Thus the systems in which these boards should be operated needed to provide appropriate slots.

Non-Modular Systems

DIN Rail Systems are **non-modular Systems**. The user cannot change or extend boards to these systems.

Board Number

Each LAN Board is assigned a definite board number via DIP switch in order to be uniquely identified in a *hopf* Base System.

Configuration

The basic LAN parameters (IP address etc.) to access the Board 7274(RC) in the network are set via the Base System or via the **Network Configuration Assistant** integrated in the *hmc*.
Afterwards the complete parameterization of the board is made by means of a web browser via WebGUI of the board.

Power Supply

The functions boards 7274 and 7274RC (except DIN Rail) are exclusively supported with operating voltage via the internal system bus.

3.1 Handling of Board / ESD Protection

An ESD conform handling and operation of the board has to be ensured!

Otherwise there is the danger that the board might get damaged through ESD (electrostatic discharge).
Damages to the board caused by improper handling are not covered by the factory guaranty.

3.2 General - Setting the Board Number for the Use in Base System

The boards must be coded to a System Board number in order to enable the various LAN Boards to be administered and configured in the Base System.

Under no circumstances may two LAN with the same board number be integrated into one Base System. This leads to unspecified faults on these two boards!

The coding of the board number is effected on Board 7274(RC) via DIP switch bank (**DS1**).

3.3 *hopf* Base Systems 6844, 6844RC, and 6855 – Only Board 7274

The operation of the board in Base System 7001 and the Base Systems 6844, 6844RC and 6855 can be selected via switch **8** of the DIP switch bank **DS1.**

Only a correct setting of switch 8 onto DIP switch bank DS1 allows a proper operation of the board 7274 in the according Base System.

DS1 / SW8	*hopf* Base System Selection
off	Base System 7001
on	Base System 68xx

3.3.1 Setting the Board Number for Base Systems 68xx

A maximum of 2 LAN Boards of different types (also different types - e.g. boards 7273 and board 7274) can be configured in the System 68xx. The Board number is set via the DIP switch bank (**DS1 / SW1-5**) for unique identification in the Base System.

The LAN board with the board number 1 is parameterised in the menu of the Base System under menu LAN 1 and the LAN board with the number 2 under menu LAN 2.

SW5	SW4	SW3	SW2	SW1	Board Number:	WebGUI
off	off	off	off	off	Board No. 1	Board No. 0
off	off	off	off	on	Board No. 2	Board No. 1

Only Board Numbers 1 and 2 are allowed in System 68xx.
System 68xx is unable to configure board numbers which are set outside this range.

ATTENTION: Deviating presentation of the board number in WebGUI
Board numbers displayed in WebGUI (Board No. X) start with the number 0 instead of number 1. That means e.g. LAN Board 1 is designated with board number 0 in WebGUI.

3.4 *hopf* Base System 7001 – Only Board 7274

The parameterization for the operation of the board in Base System 7001 or in the Base Systems 6844, 6844RC and 6855 is made via the switch **8** of the DIP switch bank **DS1.**

> ⚠ Board 7274 will only operate properly if the setting is correct.

DS1 / SW8	*hopf* Base System Selection
off	Base System 7001
on	Base System 68xx

3.4.1 Setting the Board Number for Base System 7001

A maximum of 8 LAN Boards of different types (also different types - e.g. boards 7273 and board 7274) can be configured in System 7001. The board number is set via the DIP switch bank (**DS1 / SW1-5**) for unique identification in the Base System.

The LAN boards are parameterised in the Base System menu under LAN 1-8 according to their board numbers (e.g. LAN board with the number 1 is parameterized in menu LAN 1).

SW5	SW4	SW3	SW2	SW1	System Board No.:	WebGUI
off	off	off	off	off	Board No. 1	Board No. 0
off	off	off	off	on	Board No. 2	Board No. 1
off	off	off	on	off	Board No. 3	Board No. 2
off	off	off	on	on	Board No. 4	Board No. 3
off	off	on	off	off	Board No. 5	Board No. 4
off	off	on	off	on	Board No. 6	Board No. 5
off	off	on	on	off	Board No. 7	Board No. 6
off	off	on	on	on	Board No. 8	Board No. 7

> ⚠ **In System 7001 only board numbers 1 – 8 are allowed.**
> System 7001 is unable to configure board numbers which are set outside this range.

> ⚠ **ATTENTION: Deviating presentation of the board number in WebGUI**
> Board numbers displayed in WebGUI (Board No. X) start with the number 0. That means e.g. LAN Board 1 is designated with board number 0 in WebGUI and LAN board 8 with the number 7.

3.5 *hopf* Base System 7001RC – Only Board 7274RC

3.5.1 Setting the Board Number for Base 7001RC

A maximum number of 31 LAN boards (also different types – e.g. board 7273RC and board 7274RC) can be configured in a System 7001RC. The board number is set via the DIP switch bank (**DS1 / SW1-5**) for unique identification in the Base System.

SW5	SW4	SW3	SW2	SW1	System Board No.:
off	off	off	off	off	-
off	off	off	off	on	Board No. 01
off	off	off	on	off	Board No. 02
off	off	off	on	on	Board No. 03
off	off	on	off	off	Board No. 04
off	off	on	off	on	Board No. 05
off	off	on	on	off	Board No. 06
off	off	on	on	on	Board No. 07
off	on	off	off	off	Board No. 08
off	on	off	off	on	Board No. 09
off	on	off	on	off	Board No. 10
off	on	off	on	on	Board No. 11
off	on	on	off	off	Board No. 12
off	on	on	off	on	Board No. 13
off	on	on	on	off	Board No. 14
off	on	on	on	on	Board No. 15
on	off	off	off	off	Board No. 16
on	off	off	off	on	Board No. 17
on	off	off	on	off	Board No. 18
on	off	off	on	on	Board No. 19
on	off	on	off	off	Board No. 20
on	off	on	off	on	Board No. 21
on	off	on	on	off	Board No. 22
on	off	on	on	on	Board No. 23
on	on	off	off	off	Board No. 24
on	on	off	off	on	Board No. 25
on	on	off	on	off	Board No. 26
on	on	off	on	on	Board No. 27
on	on	on	off	off	Board No. 28
on	on	on	off	on	Board No. 29
on	on	on	on	off	Board No. 30
on	on	on	on	on	Board No. 31

> **In System 7001RC only board numbers 1 – 31 are allowed.**
> System 7001RC is unable to configure board numbers which are set outside this range.

3.5.2 NTP Accuracy Notification for Status- and Error Messages in System 7001RC

> **i** The evaluation of NTP Accuracy message is available from version 07.00 of control board 7020RC of the Base System 7001RC.

The evaluation of the **NTP Accuracy Message** for the generation of status and error messages can be allowed / suppressed for the Base System 7001RC by each board 7274RC with DIP switch **DS1 / SW7**.

DS1 / SW7	Function
ON	Evaluation of NTP Status in System 7001RC allowed
OFF	Evaluation of NTP-Status in System 7001RC not allowed

The status messages of the system 7001RC are described in the manual of System 7001RC, chapter status and error messages.

3.6 Creating the Network Connection

> **!** Ensure that the network parameters of the LAN board are configured in accordance with the local network before connecting the LAN board to the network.

> **!** Connecting a network to an incorrectly configured LAN Board (e.g. duplicated IP address) may cause interference in the network.

> **!** The Board 7274/RC) is supplied with:
>
> **ETH0 with static IPv4-address**
> IPv4 address: 192.168.0.1
> IPv4 network mask: 255.255.255.0
> Gateway: not set
>
> **ETH1 with DHCP**

> **i** 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   Network Configuration for ETH0 via LAN Connection through *hmc*

After connecting the system to the power supply and creating the physical network connection to the LAN interface of the Board 7274(RC), the device can be searched for on the network via the *hmc* Software. Then the base LAN parameters (IP address, netmask and gateway or DHCP) may be adjusted in order to allow accessibility of the board for other systems in the network.

> ⚠ The SEACH Function of the *hmc* - **Network Configuration Assistant** **requires** for location and recognition of the wished LAN board(s) the *hmc*-computer is **in the same LAN**.

The basis LAN parameters can be set via the *hmc* integrated **Network Configuration Assistant**.
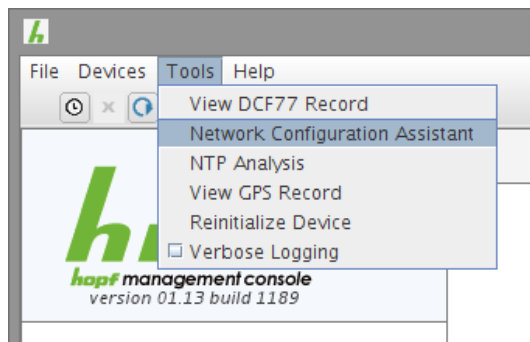
After a successful start of the *hmc* **Network Configuration Assistant** and completed search of the *hopf* LAN Modules, the configuration of the base LAN parameters can be done.

The LAN boards are listed in the **Device List** as:

727400	- Board 7274 1U and 3U
727400DIN	- Board 7274DIN-Rail
7274RC00	- Board 7274RC

The determination of different **hopf** LAN boards of the same type is made via **Hardware Address** (MAC Address).

For an extended configuration (**WebGUI**) of the LAN Board 7274(RC) via a browser the following base parameters are mandatory:

- **Host Name** ⇨ e.g. hopf7274
- **Network Configuration Type** ⇨ **Static IP Address**
- **IP Address** ⇨ e.g. 192.168.0.1
- **Netmask** ⇨ e.g. 255.255.255.0
- **Gateway** ⇨ 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 '.'. There should be no distinction between upper-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.
i	The network parameters being assigned should be pre-determined with the network administrator.

After entering the above mentioned LAN parameters they needed to be transferred to the LAN Board 7274(RC) via Button **Apply** . Afterwards the entry of the **Device Password** is requested:

Device Password <**device**> is set for LAN boards 7274(RC) on delivery. So no further entry is required here – click on the button **OK** to confirm.

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

5 Network Configuration for ETH0 via the Base System

The only configuration that is carried out on Board 7274(RC) via the Base System is to enable it to be reachable on the network via **ETH0**. All other configurations on the Board are carried out over the WebGUI.

LAN Board 7274(RC) is configured via the keyboard of the respective Base System. The necessary network parameters are configured such as IP address, gateway address, network mask and a general control byte.

The Technical Description of the respective Base System is the basis for configuration. The following covers only the Board-specific menus of the respective Base System.

> **i**   **Not all Base System do accept LAN parameters** which are changed via the WebGUI and thus they are no longer displayed correctly in the Base System. For this reason the assignment of LAN parameters via the Base System is recommended. For the exact behaviour of the Base System the appropriate manual should be considered.

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.xxx to 127.xxx.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

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.xxx - 239.xxx.xxx.xxx are used as multicast addresses.

Class E Networks

The addresses from 240.xxx.xxx.xxx - 254.xxx.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.

Network Mask

The network mask is used to partition IP addresses outside of network classes A, B and C. When entering the network mask it is possible to designate the number of bits of the IP-address to be used as the network part and the number to be used as the host part, e.g.:

Network Class	Network Part	Host Part	Network Mask Binary	Network Mask Decimal
A	8 Bit	24 Bit	11111111.00000000.00000000.00000000	255.0.0.0
B	16 Bit	16 Bit	11111111.11111111.00000000.00000000	255.255.0.0
C	24 Bit	8 Bit	11111111.11111111.11111111.00000000	255.255.255.0

The number of bits for the host part is entered in order to calculate the network mask:

Network Mask	Host Bits
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.000	8
255.255.254.000	9
255.255.252.000	10
255.255.248.000	11
.	.
.	.
255.128.000.000	23
255.000.000.000	24

Example:

Desired network mask: **255.255.255.128**

Value to be entered: **7**

5.1 Input Functions of Base Systems 6844, 6844RC and 6855 (Board 7274 only)

> ⚠ After they have been entered fully, the LAN parameters configured through the system menu are transferred to the control board by pressing the `ENT` key.
>
> In order for the LAN parameters to be transferred from the control board to Board 7274 it is necessary to exit the respective menu by pressing the `BR` key.

5.1.1 Entry the Static IPv4 Address / DHCP Mode

The IP address and DHCP mode for the LAN interface ETH0 are entered via the following selection frames:

```
    SET LAN 1
    ADR.   Y/N
```

or

```
    SET LAN 2
    ADR.   Y/N
```

After entering `Y` the display changes to the input frame (LAN 1 in this case):

```
LAN 1 >
```

Static IPv4 Address

The IPv4 address is entered in 4 groups of digits configurable from 000 to 255. They are separated by a dot (**.**). Input must be in the form of 3 digits (e.g.: 2 ⇨ 002).

An example of a complete entry would be as follows:

```
AN 1 >192.168.
      017.001<
```

In the case of an implausible entry (such as 265), an INPUT ERROR is sent and the complete entry is rejected.

DHCP / Static IP Address Assignment

For the use of DHCP, the IP address are all to be fully set to **>000.000.000.000<** (invalid IP address).

All other addresses are interpreted as static IP addresses.

5.1.2 Entry the Gateway Address

The gateway address for the LAN interfaces is entered via the following selection frames:

```
      S E T   L A N   1
G A T E W A Y   A D R .   Y / N
```

or

```
      S E T   L A N   2
G A T E W A Y   A D R .   Y / N
```

After entering ⬚Y⬚ the display changes to the input frame:

```
G . W   1   >
```

The gateway address can now be entered in the same way as the IP address.

5.1.3 Entry the Network Mask

The entry of the net mask differs between the Systems 6844 / 6844RC and the System 6855.

5.1.3.1 Entry the Network Mask - Systems 6844 and 6844RC

The net mask is decimally entered with these systems.

Set Net Mask

```
   S E T   L A N _ 1
   N E T M A S K     Y / N
```

```
 L A N _ 1     N E T M A S K
> 2 5 5 . 2 5 5 . 2 5 5 . 0 0 0
```

5.1.3.2 Entry of Network Mask - System 6855

The net mask is entered via the number of HOST bits with this System.

The network mask for the LAN interface ETH0 is entered via the following selection frames:

```
      S E T   L A N   1
N E T - M A S K .   Y / N
```

or

```
      S E T   L A N   2
N E T - M A S K .   Y / N
```

After entering ⬚Y⬚ the display changes to the input frame:

```
N E T - M A S K   L A N   1
            > _
```

The network mask can now be entered in the range from 0-31.

5.1.4   Entry the Control Byte

Various settings can be made with the control byte.
The control byte is entered via the following selection frames:

```
       S E T   L A N   1
C N T R L . - B Y T E   Y / N
```

or

```
       S E T   L A N   2
C N T R L . - B Y T E   Y / N
```

After entering Y the display changes to the input frame.
For editing purposes, the individual bits of the new byte are entered on the second line with **"0"** and **"1"**.

The bits of the parameter byte are numbered consecutively in descending order:

e.g.:

```
B I T   7 6 5 4   3 2 1 0
        0 0 0 0   0 0 0 0
```

The entry must be concluded by pressing the ENT key.

5.1.4.1 Bit 7-0 - No function at present

Bit 7-0	No function at present
0	These bits should always be set to **"0"** for reasons of compatibility.

5.2 Base System 7001 Input Functions (Board 7274 only)

The input and display functions are called up by means of the menu header **BOARDS:3** under **BOARD 7270 / 7271 / 7272 / 7274**.

The following LAN Board menu for the LAN interface ETH0 appears:

```
No:1   CB:  00000000    IP:  000.000.000.000
NEW      >_              >    .   .   .      <
```

The first input expected under **No:** is the System Board Number (**1-8**) of the LAN Board to be configured (in this case Board number 1) and this is confirmed with the `ENT` key.

After the Board number has been entered, the current configuration of the selected LAN Board ETH0 is displayed on the first menu line.

The new parameters can be entered on the second line. It is possible to change to the next menu header without making a new entry by pressing the `ENT` key.

> ⚠ After they have been entered fully, the LAN parameters configured through the system menu are transferred to the control board by pressing the `ENT` key. In order for the LAN parameters to be transferred from the control board to Board 7274 and to be stored there it is necessary to exit the respective menu by pressing the `BR` key.

5.2.1 Entry the Control Byte

Various settings can be made with the control byte (CB:).

```
No:1   CB:  00000000    IP:  192.168.017.001
NEW      > 76543210     >    .   .   .      <
```

The individual bits of the control byte are configured by entering `0` and `1`.

The complete entry is completed by pressing the `ENT` key. The new control byte appears on the top line.

5.2.1.1 Bit 7-0 - No Function at Present

Bit 7-0	No function at present
0	These bits should always be set to **"0"** for reasons of compatibility.

5.2.2 Entry the Static IPv4 Address / DHCP Mode

The currently valid IP address for the LAN interface ETH0 appears on the top line.

| N | o | : | 1 | | C | B | : | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | I | P | : | | 1 | 9 | 2 | . | 1 | 6 | 8 | . | 0 | 1 | 7 | . | 0 | 0 | 1 |
| N | E | W | | | | | | > | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | > | | | | . | | | . | | | . | | | | < |

The IPv4 address is entered in 4 groups of digits each separated by a dot (**.**). The entry must take place in 3 digits in the value range from 000 - 255.

The entry is completed by pressing the ⌈ **ENT** ⌋ key. The new address appears on the top line. In the case of an incorrect entry this menu header is exited and an error message is sent.

DHCP / Static IP Address Assignment

For the use of DHCP, the IP address are all to be fully set to **>000.000.000.000<** (invalid IP address).

All other addresses are interpreted as static IP addresses.

5.2.3   Entry the Network Mask

The currently valid network mask for the LAN interface ETH0 appears on the top line as host bits.

N	o	:	1		N	M	:		0	0					G	W	:		1	9	2	.	1	6	8	.	0	1	7	.	1	5	2
N	E	W				>	_										>				.			.			.						<

The input range for the network mask lies between **0-31**.

The entry is completed by pressing the $\boxed{\text{ENT}}$ key. The new network mask appears on the top line. In the case of an incorrect entry this menu header is exited and an error message is sent.

5.2.4   Entry the Gateway Address

The next menu header to appear concerns the editing of the gateway or router.

N	o	:	1		N	M	:		1	6					G	W	:		1	9	2	.	1	6	8	.	0	1	7	.	1	5	2
N	E	W				>	1	6									>	_			.			.			.						<

The gateway address can now be entered in the same way as the IP address described in *Chapter 5.2.2 Entry the Static IPv4 Address / DHCP Mode*.

5.3   Input Functions of Base System 7001RC (Board 7274RC only)

> ⚠ Any modification of parameters requires checking of **all** menu points of the LAN menu. Menu points which do not require any change of value or just checked with the key $\boxed{\text{ENT}}$. Only the complete check of **all single** menu points allow the adoption of all changes and their transfer to the board 7274RC.

The input and display functions of the board parameters are polled in the menu heading
BOARD-SETUP:4

with $\boxed{\text{ENT}}$ key   ⇨ Main menu
with $\boxed{4}$ key   ⇨ Board setup
with $\boxed{N}$ key   ⇨ Scroll to menu heading:

S	E	T		S	Y	S	T	E	M	-	B	O	A	R	D	S		P	A	R	A	M	E	T	E	R			Y	/	N		

Select with key $\boxed{Y}$

Search for board to be parameterized with key $\boxed{N}$ and select with key $\boxed{Y}$.

Example:

```
P A R A M E T E R   B O A R D   0 3   O F   2 5     7 2 7 3   N O . : 0 1
S T A T U S : M / -     B O A R D N A M E : " E T H E R N E T "   S E T > Y / N
```

PARAMETER BOARD 03 OF 25   ⇨   board **03** of **25** implemented

7274 NO.: 01   ⇨   board type **7274RC** with board number **01**

STATUS: M (I)**/-** (E)   ⇨   **M or I** = monitoring **or** no monitoring (idle)

   ⇨   **E or –** = without error operating **or** board error

BOARDNAME: "ETHERNET "   ⇨   **ETHERNET** board name freely selected by customer, up to 8 characters

5.3.1   Entry the Static IPv4 Address / DHCP Mode

Static IPv4 Address

In the upper line the selected board appears with its board number and IPv4 address of the LAN interface ETH0. For configuration of a new IPv4 address the complete entry of the 4 groups of digits is necessary.

The IPv4 address is entered in 4 groups of digits configurable from 000 to 255. They are separated by a dot (**.**). Input must be in the form of 3 digits (e.g.: 2 ⇨ 002).

An example of a complete entry would be as follows:

```
B . 7 2 7 3   N O . : 0 1     I P - A D R   > 1 9 2 . 1 6 8 . 0 1 7 . 0 0 1 <
                N E W   I P - A D D R E S S   > ~ ~ ~ . ~ ~ ~ . ~ ~ ~ . ~ ~ ~ <
```

In the case of an implausible entry (such as 265), an INPUT ERROR is sent and the complete entry is rejected.

DHCP / Static IP Address Assignment

For the use of DHCP, the IP address, gateway address and network mask are all to be fully set to **>000.000.000.000<** (invalid IP address).

All other addresses are interpreted as static IP addresses.

5.3.2   Entry the Gateway Address

The gateway address can be entered via the selection screen:

```
B . 7 2 7 3   N O . : 0 1     G W - A D R   > 2 5 5 . 0 0 0 . 0 0 0 . 0 0 0 <
                N E W   G W - A D D R E S S   > ~ ~ ~ . ~ ~ ~ . ~ ~ ~ . ~ ~ ~ <
```

The Gateway address can now be entered in the same way as the IP address, as described in **_Chapter 5.3.1 Entry the Static IPv4 Address / DHCP Mode_**.

5.3.3 Entry the Network Mask

The network mask can be entered via the selection screen:

```
B.7273 NO.:01 NETMASK >255.255.000.000<
       NEW NETMASK >~~~.~~~.~~~.~~~<
```

The network mask for LAN interface ETH0 can now be entered in the same way as the IP address, as described in **Chapter 5.3.1 Entry the Static IPv4 Address / DHCP Mode**.

5.3.4 Entry the Control Byte

The Control-Byte is shown on the top line with the currently set values.

```
B.7273 NR.:01 CONTROL-BYTE  00000010
       NEW CONTROL-BYTE >~~~~~~~~<
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using **"0"** and **"1"**. The complete Control Byte must always be recorded and confirmed with the ⎡ **ENT** ⎤ key.

The bits of the Control Byte are numbered in descending order:

```
CONTROL-BYTE >76543210<
```

5.3.4.1 Bit 7-0 - No Function at Present

Bit 7-0	No function at present
0	These bits should always be set to **"0"** for reasons of compatibility.

5.3.5 Entry the Parameterbyte 01 (no function at present)

Parameter of Parameter-Byte 01 is shown on the top line with the currently set values.

```
B . 7 2 7 3   N O . : 0 1     O L D :   B Y T E   0 1   > 0 0 0 0 0 0 0 0 <
B Y T E   =   B I T   7 . . 0   N E W :   B Y T E   0 1   > ~ ~ ~ ~ ~ ~ ~ ~ <
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using **"0"** and **"1"**. The complete Parameter Byte must always be recorded and confirmed with the ⌷ **ENT** ⌷ key.

The bits of the Parameter Byte are numbered in descending order:

```
B Y T E   0 1   > 7 6 5 4 3 2 1 0 <
```

Bits 7-0	No function at present
0	These bits should always be set to **"0"** for reasons of compatibility.

5.3.6 Entry the Parameterbyte 02 (no function at present)

Parameter of Parameterbyte 02 is shown on the top line with the currently set values.

```
B . 7 2 7 3   N O . : 0 1     O L D :   B Y T E   0 2   > 0 0 0 0 0 0 0 0 <
B Y T E   =   B I T   7 . . 0   N E W :   B Y T E   0 2   > ~ ~ ~ ~ ~ ~ ~ ~ <
```

For the purposes of manipulation, the individual bits of the new byte are to be entered on the second line using **"0"** and **"1"**. The complete Parameter Byte must always be recorded and confirmed with the ⌷ **ENT** ⌷ key.

The bits of the Parameter Byte are numbered in descending order:

```
B Y T E   0 2   > 7 6 5 4 3 2 1 0 <
```

Bits 7-0	No function at present
0	These bits should always be set to **"0"** for reasons of compatibility.

5.4 Configuration in DIN Rail Modules

It is described in the appropriate manual of the DIN Rail module whether there is the possibility of parameterization via the System or the LAN parameterization of the board may be carried out via the *hmc* **Network Configuration Assistant** (see chapter *4 Network Configuration for ETH0 via LAN Connection through hmc*).

5.5 Configuration via *hmc* (*hopf* Management Console) Remote Access

The parameters can also be set via the *hmc*, insofar the Base System provides remote communication.

6   HTTP/HTTPS WebGUI – Web Browser Configuration Interface

> ⚠ JavaScript and Cookies must be enabled in the browser in order for the WebGUI to display and function correctly.

6.1   Quick Configuration

This Chapter briefly describes the basic operation of the WebGUI installed on the Board.

6.1.1   Requirements

- Ready-for-operation *hopf* Base System with implemented Board 7274(RC)

- Board configured for network operation (see **Chapter 4 Network Configuration for ETH0 via LAN Connection through *hmc*** and **5 Network Configuration for ETH0 via the Base System**)

- PC with installed web browser (e.g. Internet Explorer) in the sub-network of Board 7274(RC)

6.1.2   Configuration Steps

- Create the connection to the Board with a web browser

- Login as a **'master'** user (default password <master> is set by delivery)

- Switch to "Network" tab and if available enter the DNS Server (required for NTP and the alarm messages depending on the network)

- Save the configuration

- Switch to "Device" tab and restart Network Time Server via "Reboot Device"

- NTP Service is now available with the standard settings

- NTP specified settings can be done in the "NTP" tab

- Alarm messages via Syslog/SNMP/Email can be configured in "Alarm" tab

> ⚠ The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.
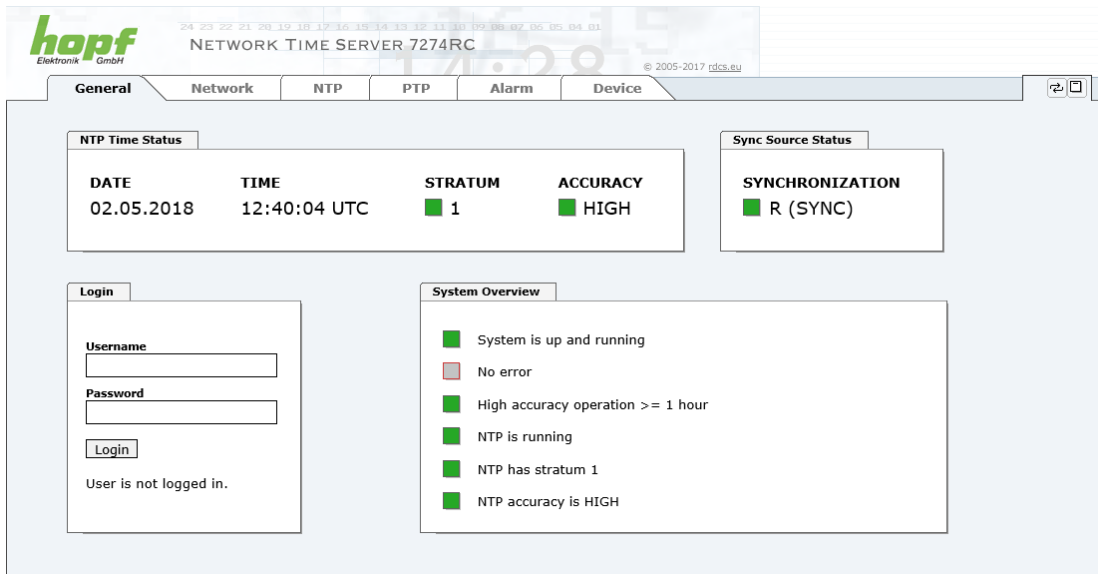
6.2   General – Introduction

Board 7274(RC) should be accessible to a web browser if it has been set up correctly. Enter the IPv4 address - as set up on the Board earlier - or the DNS name on the address line <http://xxx.xxx.xxx.xxx> and the following screen should appear

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

> ⚠ Configuration can only be completed via the Board's WebGUI!

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

6.2.1 LOGIN and LOGOUT as a User

All of the Board's data can be read without being logged on as a special user. However, the Board data can only be configured or modified by an authorised user! Two types of user are defined:

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

- "**device**" user (default password on delivery: <**device**>)
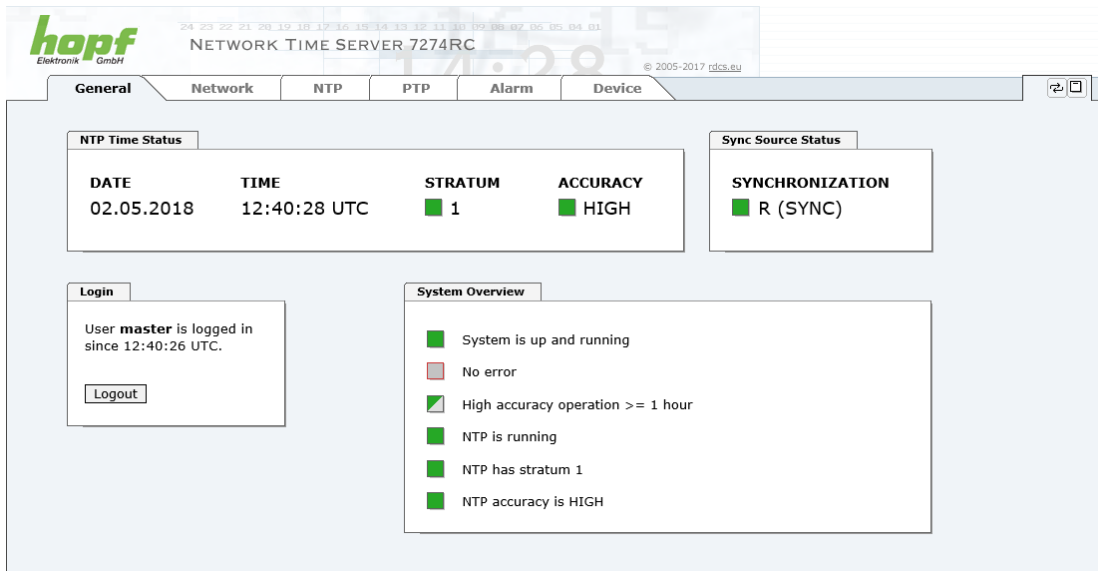
> **i** Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: **[ ] ( ) * - _ ! $ % & / = ?**

> **i** The password should be changed after the first login for security reasons.

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

Click on the `Logout` button to log out.

The WebGUI is equipped with session management. If a user does not log out, he or she is automatically logged off 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 Board 7274(RC).

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

6.2.2   Navigation via the Web Interface

The WebGUI is divided into function 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).

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

JavaScript should be enabled in the browser in order to guarantee the correct operation of the web interface.
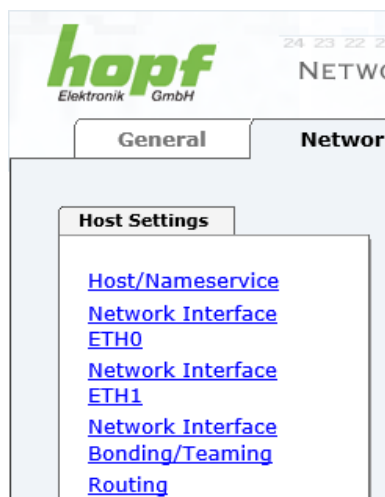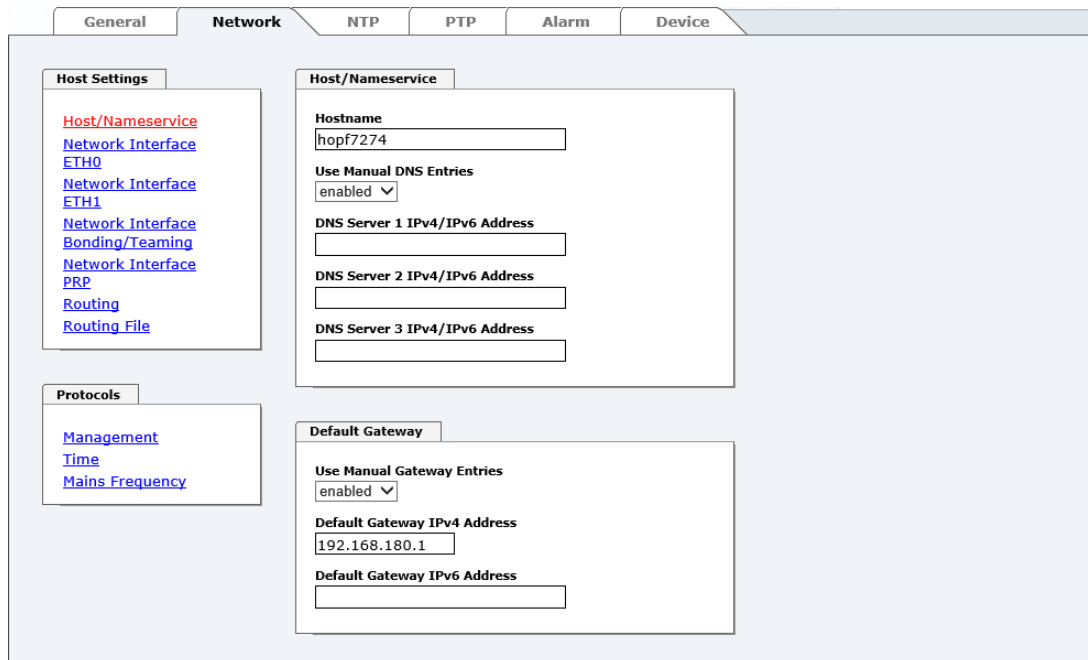
All the links within the tabs on the left hand side lead to corresponding detailed display or setting options.

6.2.3   Entry or Changing Data

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

After an entry has been made the configured field is marked with a star ' * '. This means that a value has been entered or changed but is not yet stored in the flash memory. It is necessary to be acquainted with the symbols shown below in order to be able to save the configuration or the changed value.

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

For permanent storage the value MUST be accepted by the Board with **Apply** and then saved with **Save**.

However, this data is then lost when the *hopf* Base System is switched off or restarted.

If the data is only to be tested it is sufficient to accept the changes with **Apply**.
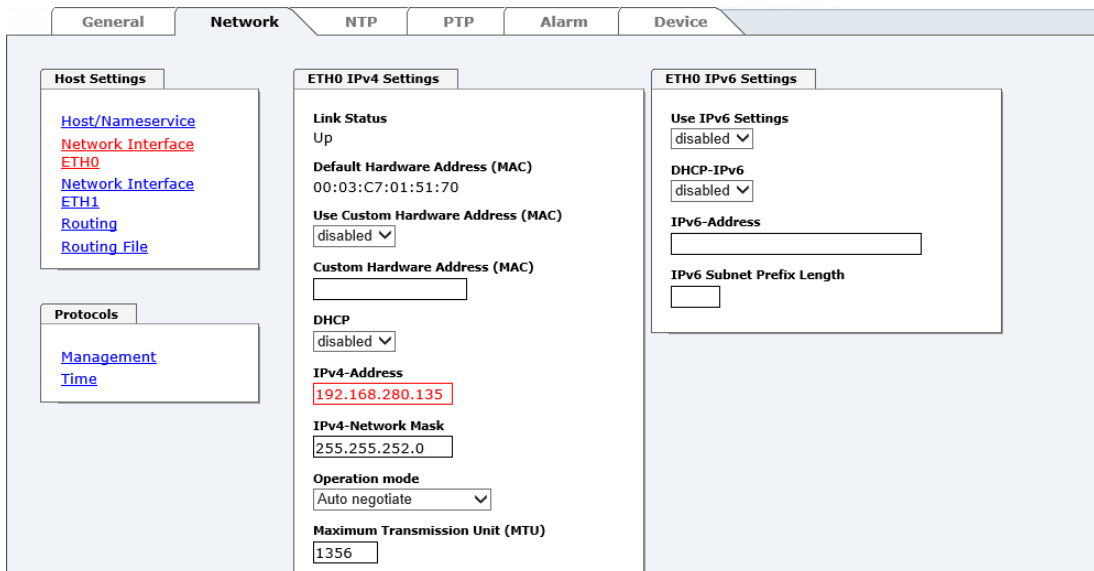
> ⚠ **Changing Network Parameters**
>
> Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.
>
> However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.

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

6.2.4   Plausibility Check during Input

A plausibility check is generally carried out during input.

As it can be seen in the above image, an invalid value (e.g. text where a number should be entered, IP address instead of a range etc.) is identified by a red border when an attempt is made to accept these settings. It should be noted here that this is only a semantic check and not to test whether an entered IP address can be used on the network or in the configuration! If an error message is displayed it is not possible to save the configuration in the Board's flash memory.

> ⚠ The error check only verifies semantics and the validity of ranges. It is **NOT a logic or network check** for entered data.

6.3   Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Network
- NTP
- PTP
- Alarm
- Device

6.3.1   GENERAL Tab

This is the first tab which is displayed when using the web interface.
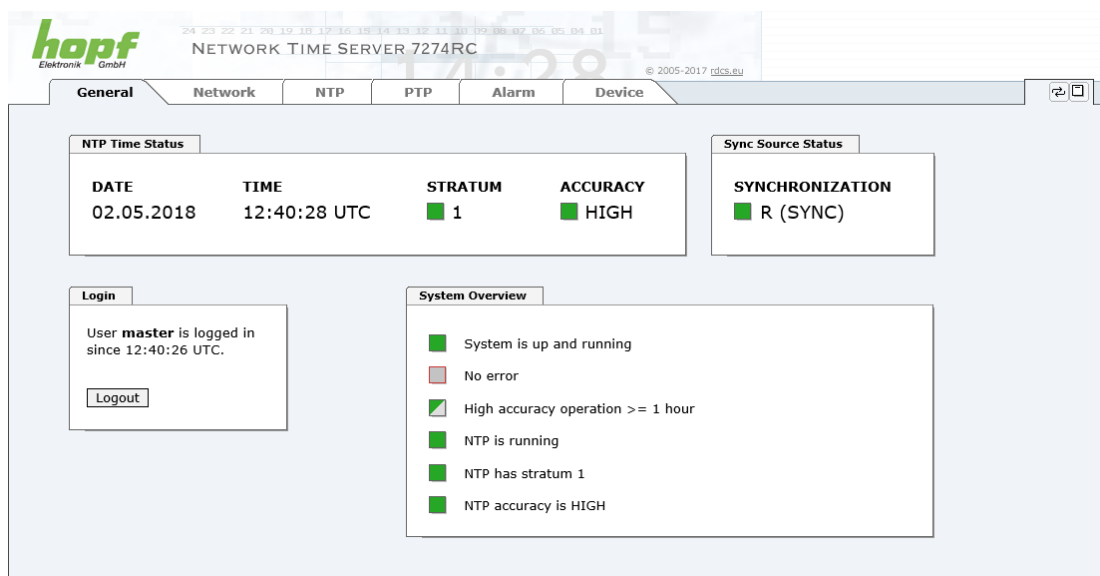
NTP Time Status

This area shows basic information about the current time and date of the Board. The time **always** corresponds to UTC time. The reason for this is that NTP always works with UTC and not local time.

Stratum displays the actual NTP stratum value of the bard 7274(RC) (value range from 1-16).

The **ACCURACY** field (accuracy of NTP) contains the values LOW, MEDIUM and HIGH. The meaning of these values is explained in *Chapter 10.6 Accuracy & NTP Basic Principles* and *Chapter 8 Technical Data*.

Sync Source Status

Display of the actual status of synchronization of the base system with these possible values:

R (SYNC)	Time synchronized + Quartz regulation started/running
R (SYOF)	Time synchronized + SyncOFF running
Q (QUSE)	Quartz/Crystal time after reset or manual setting
- (INVA)	Invalid time

Login

The **Login** box is used how described in ***Chapter 6.2.1 LOGIN and LOGOUT as a User***.

System Overview
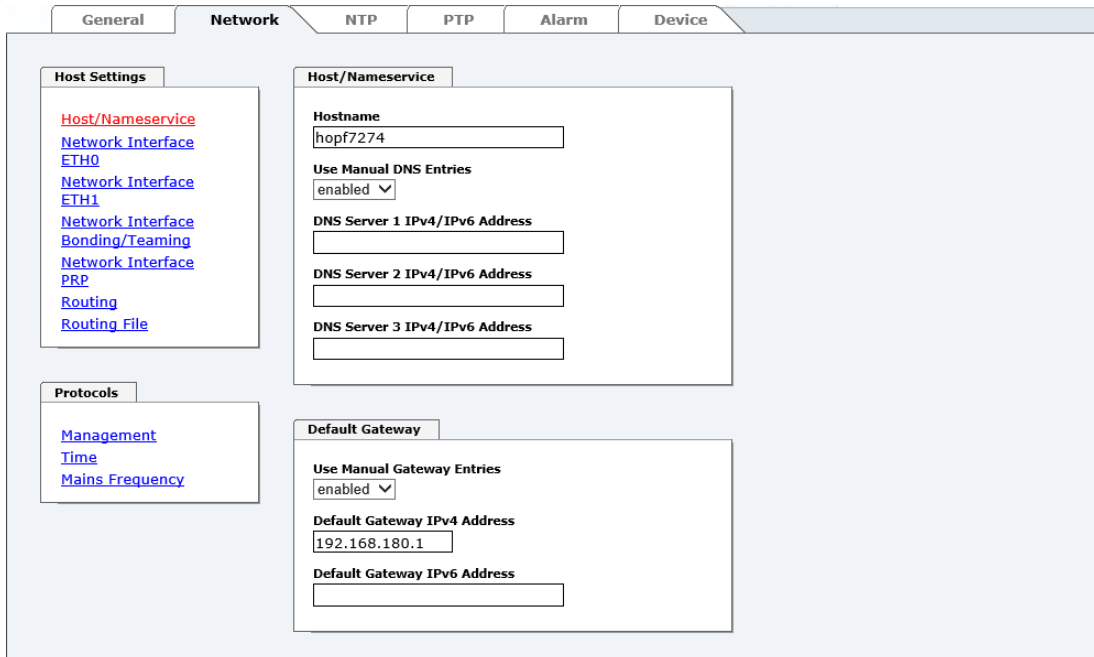
This table gives a direct overview of the Board 7274(RC) current operating states.

WebGUI	LED	Bedeutung
System Status	On 1Hz flashing 1Hz flashing Off	System 7274(RC) is up and running Firmware update System is booting System not ready
Error	An 1Hz flashing 1Hz flashing Aus	Emergency operation PCID not found System bus error No error
High accuracy operation	An flashing Aus	>= 24 hour >= 1 hour < 1 hour
NTP is (NOT) running	An Aus	NTP is running and active NTP is not running
NTP has stratum …	An 1Hz flashing Aus	NTP has Stratum 1 NTP has Stratum 2-15 NTP has Stratum 16
NTP Accuracy is …	An 1Hz flashing Aus	NTP accuracy HIGH NTP accuracy MEDIUM NTP accuracy LOW

6.3.2 NETWORK Tab

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

⚠	**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 with **Save** permanently.

6.3.2.1 Host/Nameservice

Setting for the unique network identification.

6.3.2.1.1 Hostname

The standard setting for the Hostname is "**hopf7274**". This name should also be adapted to the respective network infrastructure.

In case of doubt, just leave the standard setting as it is or ask your network administrator.

⚠	The **hostname must** meet the following conditions:
	• The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.' . There should be no distinction between upper-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 **must not** be left blank.

6.3.2.1.2 Use Manual DNS Entries

With this setting you can select whether the manually entered DNS servers (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, then **Use Manual DNS Entries** should be set to disabled.

6.3.2.1.3 DNS Server 1 to 3

The IP address (IPv4 or IPv6) of the DNS server should be entered if you wish to use the Fully-Qualified Host Name (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.

6.3.2.1.4 Use Manual Gateway Entries

With this setting, you can select whether the manually entered gateways (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, then Use Manual Gateway Entries should be set to disabled.

6.3.2.1.5 Default Gateway IPv4

The standard gateway is generally configured via the Base System menu. However it can also be changed via the web interface.

> In Base System 7001 / 68xx the changed LAN configuration is only stored in the Board's flash memory and is ALWAYS overwritten when a new value is entered.
>
> Values modified via LAN are not automatically updated in the Base System and thus are no longer correctly displayed in the Base System after the modification. For this reason it is recommended to configure the default gateway via the Base System. For the respective behaviour of the Base System the appropriate manual should be considered.

If the IPv4 default gateway is not known, it must be requested by 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.
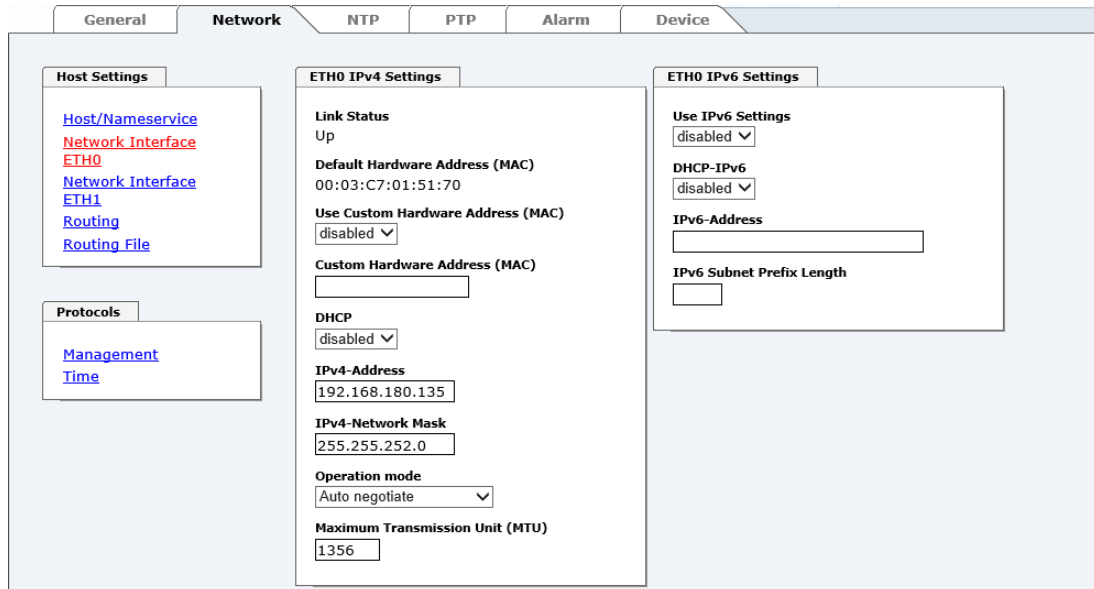
6.3.2.1.6 Default Gateway IPv6

If the Ipv6 default gateway is not known, it must be requested by the network administrator. If no standard gateway is available (special case), enter :: in the input field or leave the field blank.

6.3.2.2 Network Interface ETH0/ETH1

Configuration of the Ethernet interface ETH0/ETH1 of the Board 7274(RC)

| General | **Network** | NTP | PTP | Alarm | Device |

Host Settings

Host/Nameservice
Network Interface ETH0
Network Interface ETH1
Routing
Routing File

Protocols

Management
Time

ETH0 IPv4 Settings

Link Status
Up

Default Hardware Address (MAC)
00:03:C7:01:51:70

Use Custom Hardware Address (MAC)
disabled ▾

Custom Hardware Address (MAC)
[   ]

DHCP
disabled ▾

IPv4-Address
192.168.180.135

IPv4-Network Mask
255.255.252.0

Operation mode
Auto negotiate ▾

Maximum Transmission Unit (MTU)
1356

ETH0 IPv6 Settings

Use IPv6 Settings
disabled ▾

DHCP-IPv6
disabled ▾

IPv6-Address
[   ]

IPv6 Subnet Prefix Length
[   ]

6.3.2.2.1 Default Hardware Address (MAC)

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

For further information about the MAC address refer to ***chapter 1.2.2 1 Board Description 7274 and 7274RC*** for Board 7274(RC).

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

6.3.2.2.2 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.

> Please avoid a double of customer MAC address in the Ethernet.
>
> If the MAC address is not known please contact yours network administrator.

The use of customers MAC address needs to be activated by the function **Use Custom Hardware 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 7274(RC) has to be restarted via "Device" ☐ "Reboot Device" (see ***Chapter 6.3.6.4 Restarting the Board (Reboot Device / Hardware Reset)***

6.3.2.2.3 DHCP

If DHCP is to be used, 0.0.0.0 should be entered as the IPv4 address via the *hopf* Base System menu (likewise for gateway and network mask). This change can also be made via the web interface by enabling the DHCP mode.

6.3.2.2.4 IPv4 Address

The IPv4 address is generally configured via the *hopf* Base System menu. However it can also be changed via the web interface.

> In Base System 7001 / 68xx, the changed LAN configuration is only stored in the Board's flash memory and is ALWAYS overwritten when a new value is entered.
>
> Values modified via LAN are not automatically updated in the Base System and thus are no longer correctly displayed after the modification. For this reason it is recommended to configure the IPv4 address via the Base System. For the respective behaviour of the Base System the appropriate manual should be considered.

Contact your network administrator for details of the IPv4 address if not known.

6.3.2.2.5 IPv4 Network Mask

The IPv4 network mask is generally configured via the **hopf** Base System menu. However it can also be changed via the web interface.

> **i**
>
> In the Base System 7001 / 68xx, the changed LAN configuration is only stored in the Board's flash memory and is ALWAYS overwritten when a new value is entered.
>
> Values modified via LAN are not automatically updated in the Base System and thus are no longer correctly displayed after the modification. For this reason it is recommended to configure the IPv4 network mask via the Base System. For the respective behaviour of the Base System the appropriate manual should be considered.

Contact your network administrator for details of the IPv4 network mask if not known.

6.3.2.2.6 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.

Operation mode

```
Auto negotiate
10 Mbps / half duplex
100 Mbps / half duplex
10 Mbps / full duplex
100 Mbps / full duplex
1000 Mbps / full duplex
```

> **i**
>
> 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 the Board 7274(RC) **and** the connected network components manually to the same value.

6.3.2.2.7 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 7274(RC) is going to be delivered with default setting 1356.

6.3.2.2.8 IPv6

The Board 7274(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 zeros 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   **2001:0:0:0:1319:8a2e::7344**

6.3.2.2.9 DHCP-IPv6

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

6.3.2.2.10 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.

6.3.2.2.11 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.

6.3.2.2.12 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 7274(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 ▾

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

Activation Status
enabled ▾

VLAN Interfaces

[Add] [Remove]

	ID	Label	Remark	DHCP	IPv4-Address	IPv4-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 7274(RC) via the network interface. Furthermore it must be ensured that the network appliance is accurately configured with the same VLANs.
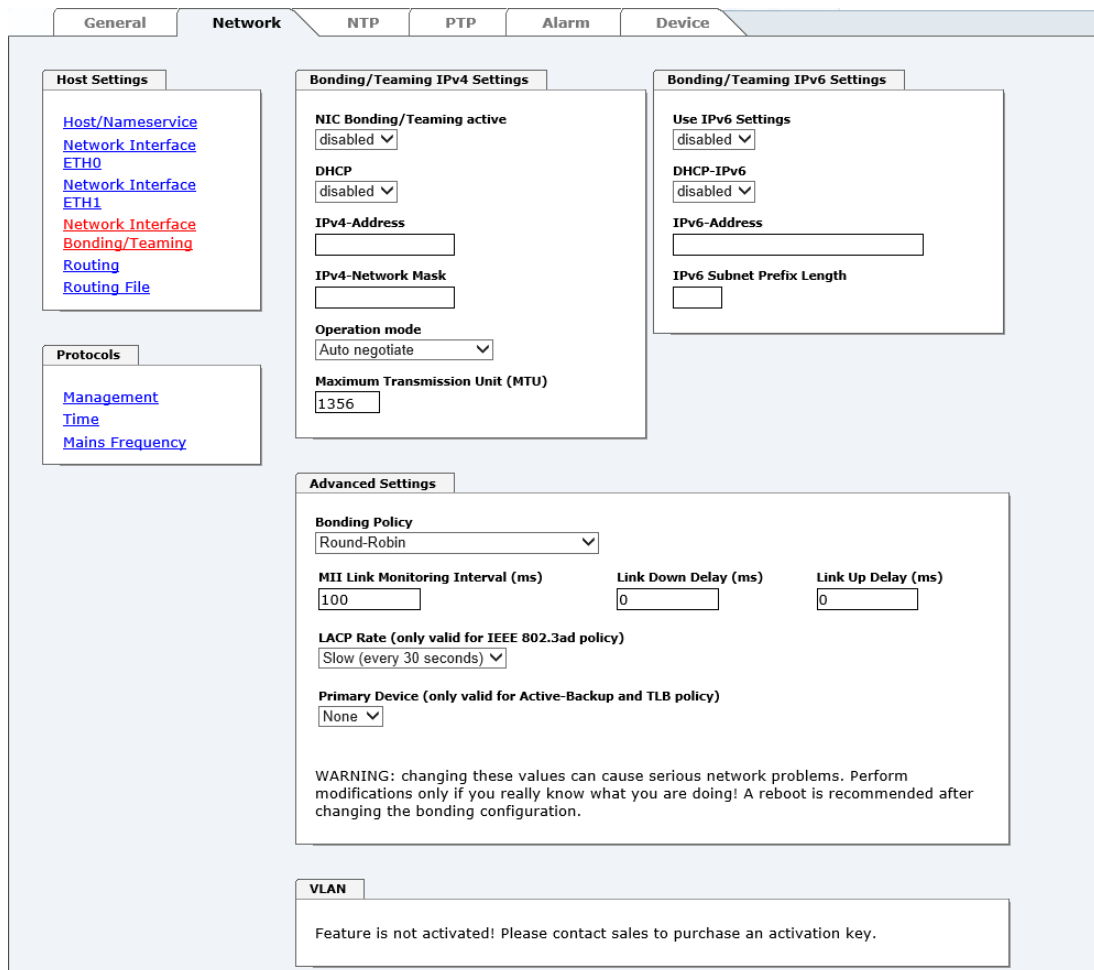
> **!** VLAN ID one (1) and two (2) are reserved and are therefore not permitted!

6.3.2.3 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 a logical network interface.

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 7274(RC) is going to be refused.

In this case settings of Board 7274(RC) must be set back to default settings!

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.

6.3.2.3.1 Basic Configuration

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

```
Bonding/Teaming IPv4 Settings

NIC Bonding/Teaming active
disabled ▾

DHCP
disabled ▾

IPv4-Address
[                    ]

IPv4-Network Mask
[                    ]

Operation mode
Auto negotiate        ▾

Maximum Transmission Unit (MTU)
1356
```

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 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.

6.3.2.3.2 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 ▼                        │
│                                     │
│   IPv6-Address                      │
│   ┌───────────────────────────┐     │
│   └───────────────────────────┘     │
│                                     │
│   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 by the network administrator.

IPv6 Subnet Prefix Length
Input of the IPv6 network length for the " Bonding interface".

6.3.2.3.3 Advanced Settings

```
┌─────────────────────────────────────────────────────────────────┐
│ ┌──────────────────┐                                             │
│ │ Advanced Settings │                                            │
│ └──────────────────┘                                             │
│                                                                   │
│  Bonding Policy                                                   │
│  ┌──────────────────────────────┬──┐                             │
│  │ Active-Backup                │ ▽│                             │
│  └──────────────────────────────┴──┘                             │
│                                                                   │
│  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)                   │
│  ┌──────────────────────┬──┐                                     │
│  │ 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 │
│  changing the bonding configuration.                              │
└─────────────────────────────────────────────────────────────────┘
```

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 7274(RC) are connected also needs to be configured correctly! A wrong configuration can lead to a loss of availability of Board 7274(RC)!

- **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.

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

6.3.2.4 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 a 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.
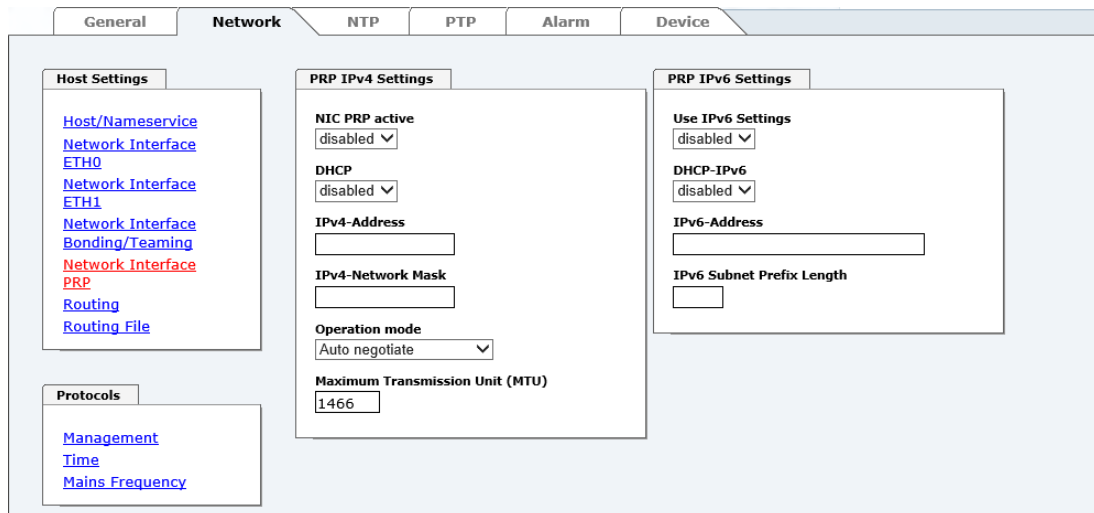
The following illustration shows an example of a PRP network:
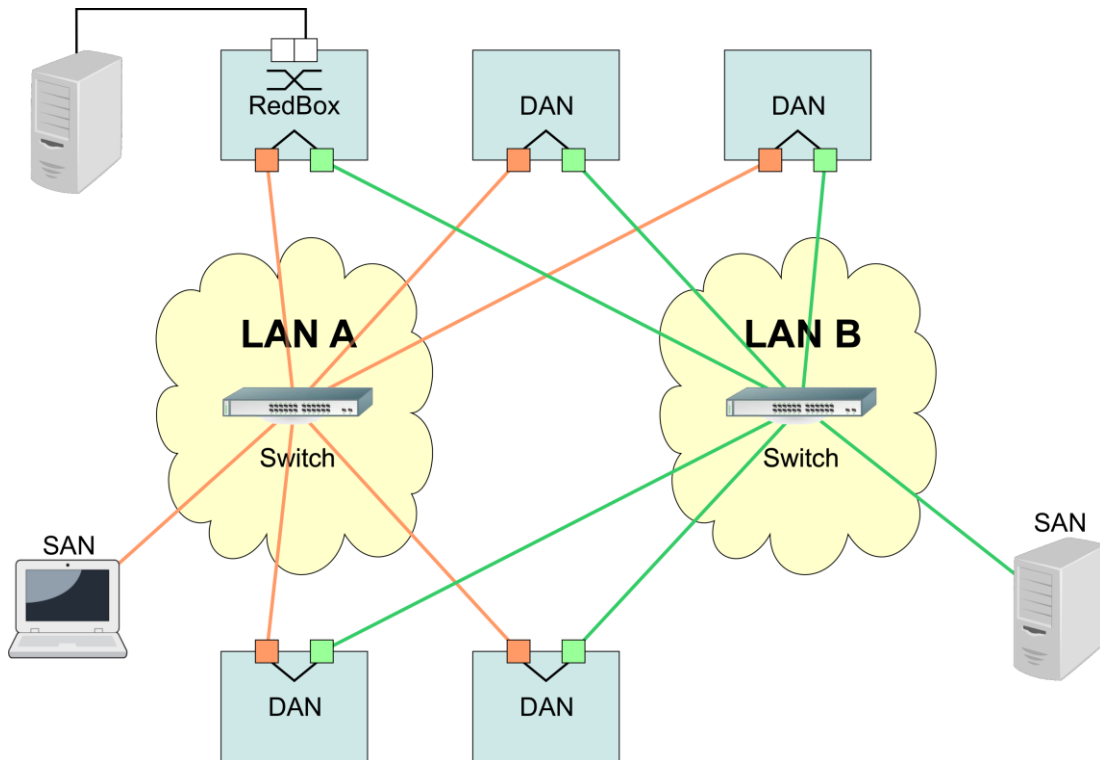
PRP-suitable applications are known as DAN (Dual Attached Node) and are going to be connected to the independent networks "LAN A" and "LAN B". The advantage of PRP is that cost-efficient and common network switches can be used which do not have to support the PRP standard. Applications which do not need 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.

Time Server 7274(RC) supports PRP as DAN and can therefore directly be integrated into a PRP network without using a RedBox.

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.

Network Mask

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

> ⚠ A change of the IP 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".

> Changing the MTU default setting with value 1466 should not be necessary by default.
>
> An incorrect configuration can lead to a loss of the network connection which refuses the Ethernet access to Time Server 7274(RC).
>
> In that case the settings of Time Server 7274(RC) need to be set to "factory default"!

The network interface ETH0 of Time Server 7274(RC) need to be connected to PRP network "LAN A", network interface ETH1 need to be connected to PRP network "LAN B"!

> 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 Time Server 7274(RC).
>
> In that case the settings of Time Server 7274(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.

6.3.2.4.1 IPv6 Network Configuration

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 by the network administrator.
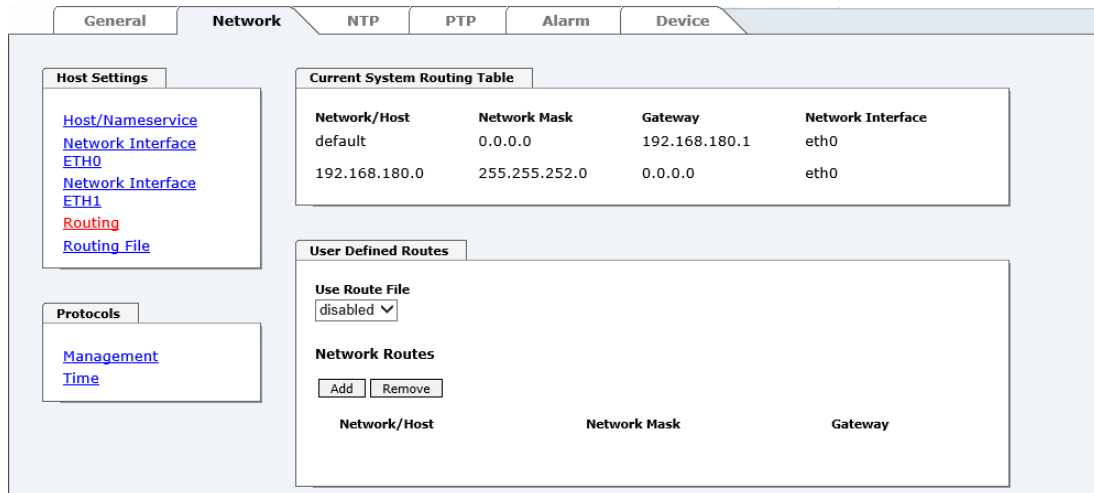
IPv6 Subnet Prefix Length
Input of the IPv6 network length for the " PRP interface".

6.3.2.5 Routing

A route must be configured if the Board is to be used in more than the local sub-network.

Routes cannot be used where the gateway / gateway host is not in the local sub-network range of the Board.

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

The image above shows every configured route of the Base System Routing Table as well as the User Defined Routes.

> ℹ The Board cannot be used as a router!

Select **Use Route File** to set whether the routing configuration set under **User Defined Routes** should be used, or routing configuration using a routing file.

> ℹ If IPv6 routes are required, the routes must be made using the settings in *Chapter 6.3.2.6 Routing File*.

6.3.2.6 Routing File

In order to activate this function, **Use Route File** must be set to **enabled** on the Routing Page.

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. When uploading the file is checked whether the file is error-free and 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].

If the host 192.168.20.11 is to be reached 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.

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

6.3.2.7 Management-Protocols – HTTP, SNMP etc.

Protocols that are not required should be disabled for security reasons. A correctly configured Board is always accessible via the web interface.
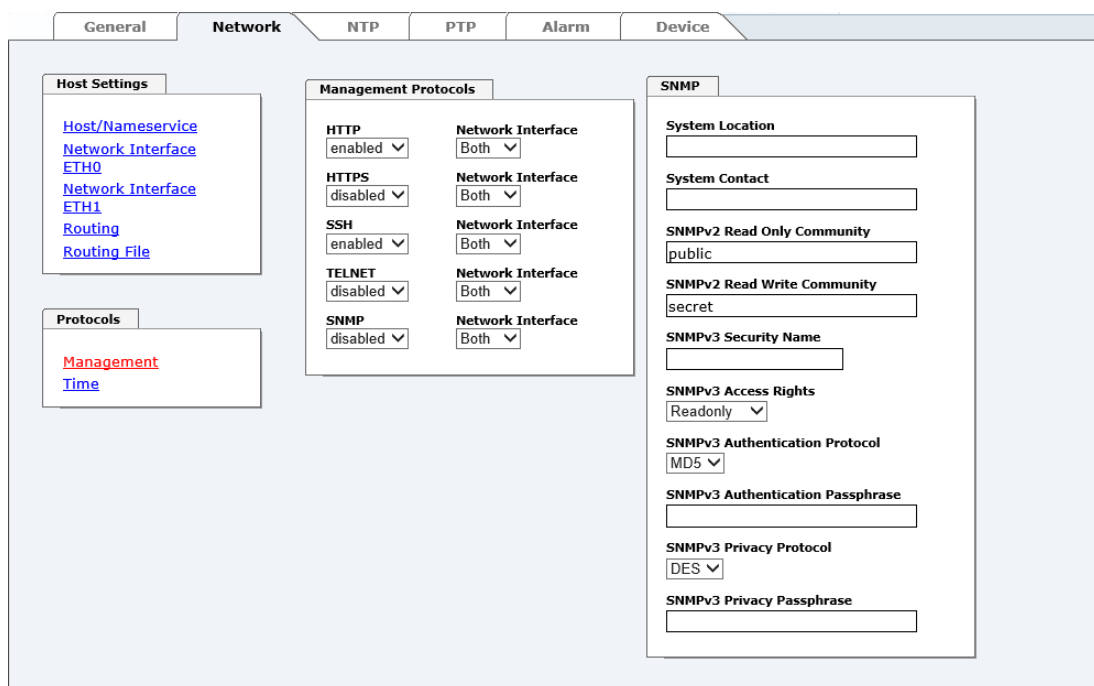
Changes to the availability for a protocol (enable/disable) take effect immediately.

> ⚠ If by mistake all protocol channels become "disabled" the SSH channel automatically get "enabled" after the attempt to save.

> ⚠ After a factory default the HTTP channel is "enabled".

All fields must be completed for the SNMP to operate correctly. Contact your network administrator if you do not have all the data.

The SNMP protocol should be enabled when using SNMP Traps.

> ℹ These service settings are applicable across the board! Services with "disabled" status are not externally accessible and are not made externally available by the Board!

6.3.2.7.1 SNMPv2c / SNMPv3

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
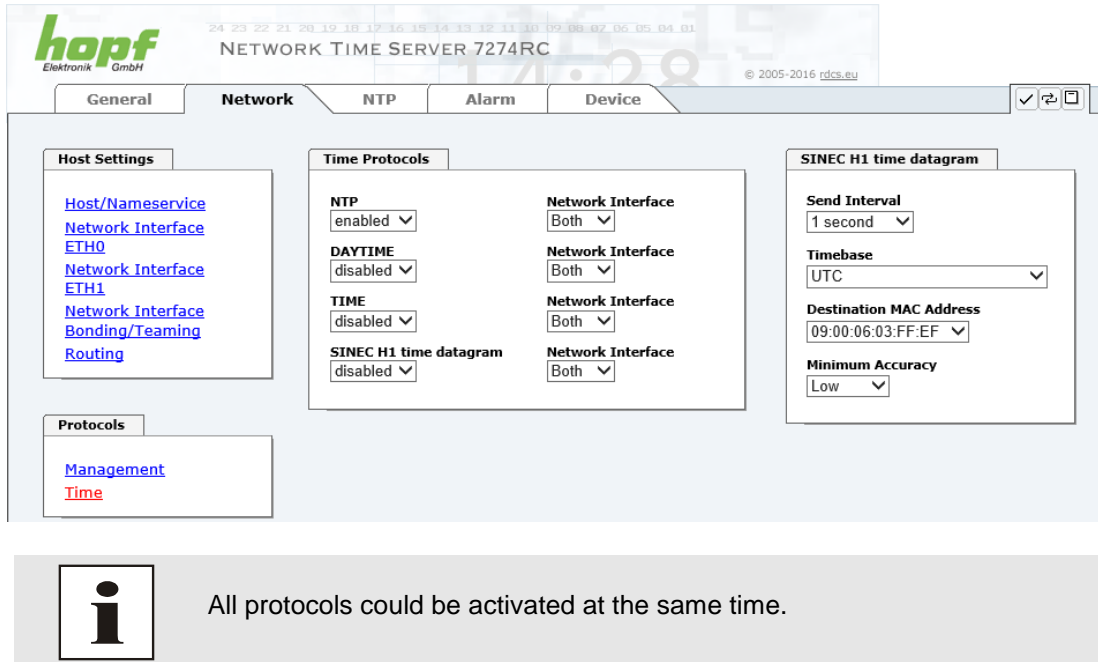
> ⚠ Right now only one user is supported.

6.3.2.8 Time (Time Protocols – NTP, DAYTIME etc.)

Activation and configuration of different time protocols

> **i** All protocols could be activated at the same time.

6.3.2.8.1 Time Protocols – NTP, SNTP etc.

Needed time protocols can be activated here.

- NTP (including SNTP)
- DAYTIME
- TIME
- SINEC H1 time datagram

6.3.2.8.2 SINEC H1 time datagram

Configuration of SINEC H1 time datagram.

Configuration of the broadcast transmission intervals SINEC H1 time datagram (Send Interval):

- every second
- 10 second
- 60 second

Timebase (see also chapter *10.2.1 Time-specific expressions:*

- Local time
- UTC
- Standard time
- Standard time with daylight / standard time status

Destination MAC Address:

- 09:00:06:03:FF:EF
- 09:00:06:01:FF:EF
- FF:FF:FF:FF:FF:FF

Minimum Accuracy for starting transmission:

This setting defines at which internal control process the SINEC H1 Time Datagram should be transmitted (see *Chapter 10.6 Accuracy & NTP Basic Principles* and *Chapter 8 Technical Data*):

- low
- medium
- high

	The setting Minimum Accuracy = LOW may lead to the output of non-synchronised (thus possibly wrong) time information.

6.3.2.8.3 Transmission point of SINEC H1 time datagram

DIP Switch **DS1 switch SW6** sets the transmission point of the SINEC H1 time datagram.

DS1 SW6	Transmission point of the SINEC H1 time datagram		
off	**Same second** (default)		
	e.g.	transmission point (UTC, absolute):	with time information:
		12**:**33:**00**,001	12:33:**00**,000
on	**ONE second delayed**		
	z.B.	transmission point (UTC, absolute):	with time information:
		12:33:**01**,002	12:33:**00**,000
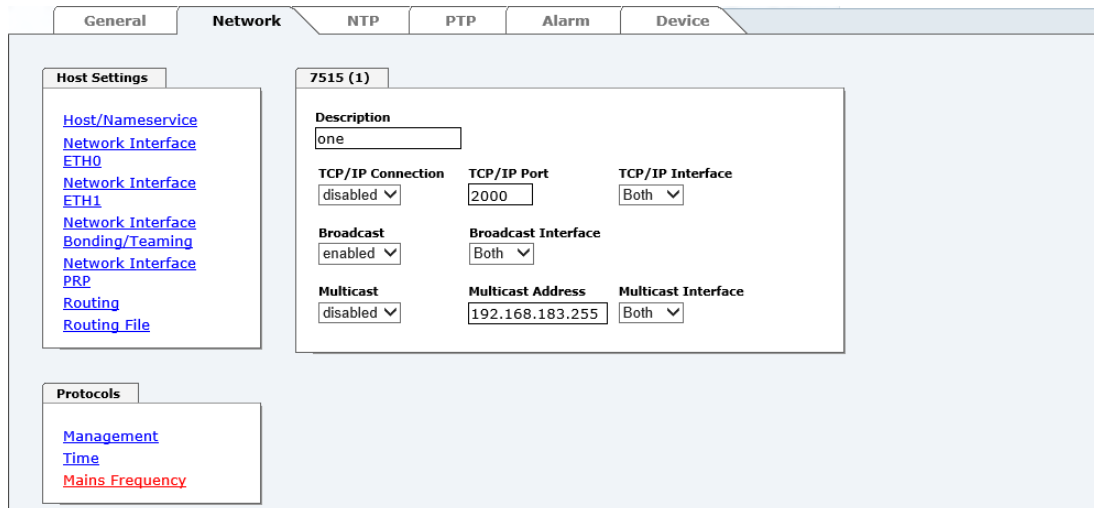
6.3.2.9 Option: 7515RC Mains Frequency Data

This option is only available for board 7274RC and enables the distribution of network time and network frequency (via Ethernet) of a net frequency board 7515RC mounted in system 7001RC.

The large matrix display 4985NTP can use the Ethernet information for displaying the network details.

This option can only be used with a special activation key. If this function is not activated, it cannot be selected in the menu point "protocols".

After activating this function a sub-menu called "mains frequency" will be displayed in the menu point "protocols".

The procedures of distributing the network information of any in system 7001RC mounted board 7515RC can be configured differently. The board number of the specific board 7515RC will be displayed in the brackets of the relevant board tab, e.g. 7515 (1).

6.3.3 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Board 7274(RC). The NTP service is the significant main service of the Board 7274(RC).

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

NTP functionality is provided by an NTP-Demon, which runs on the embedded Linux of the Board.

Depending on the *hopf* Base System it may take several hours under unfavorable conditions until long-term accuracy is obtained. During this time the NTP algorithm adjusts the internal accuracy parameters.

> **!** NTP time protocol must be enabled in order to use NTP
> (see *Chapter 6.3.3 NTP Tab*)

> **!** After all changes (according to NTP) have been done a restart of the NTP service on the board is necessary (see *Chapter 6.3.3.6 Restart* NTP).
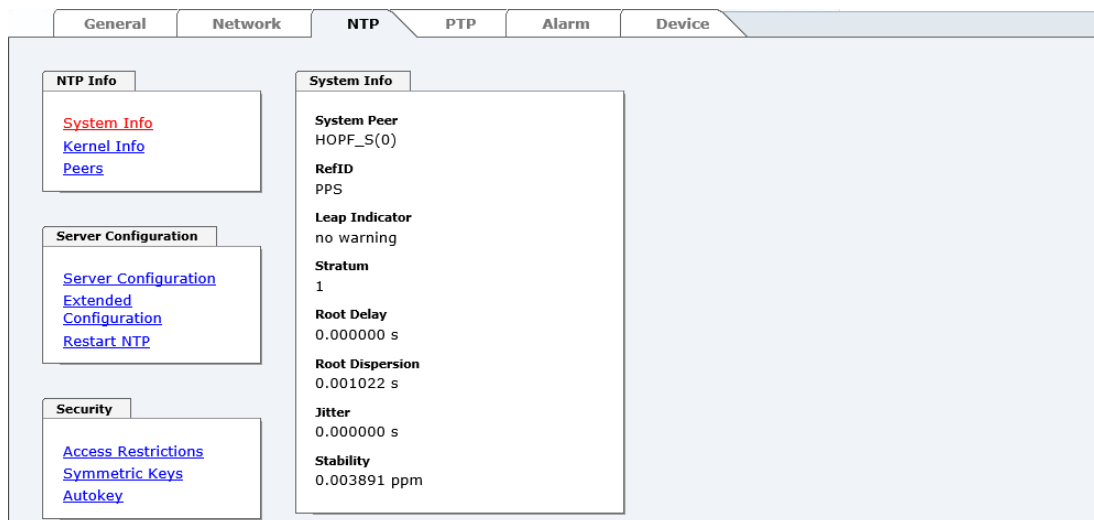
> **i** Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

6.3.3.1 System Info

In the window "System Info" the current NTP values of the NTP service running on the embedded Linux of the Board 7274(RC) are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Board 7274(RC), the status to the leap second, and the current system peer are also found here.

The NTP version used correctly adjusts the leap second.

The Board 7274(RC) works as NTP Server with stratum 1 and belongs to the best available class of NTP server, as it has a reference clock with direct access.

6.3.3.2 Kernel Info

The "Kernel Info" summary shows the current error values of the internal embedded Linux clock. Both values are internally updated every second.

This screenshot shows a maximum kernel clock error of 16 sec (seconds). The estimated error value is 3.5ms (milliseconds).

The values indicated here are based on the calculation of the NTP service and have no significance for the accuracy of the **hopf** Base System.

6.3.3.3 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 programmes.

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, reachable).
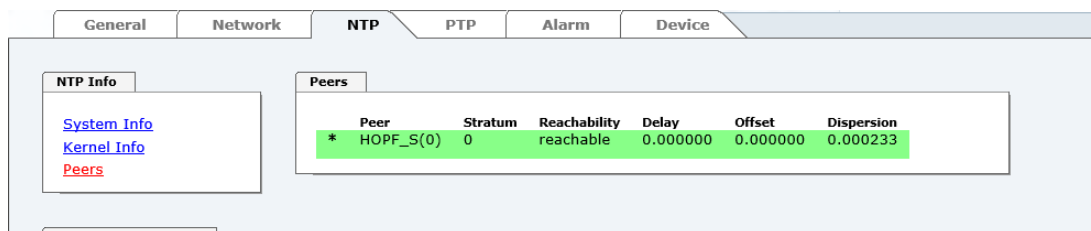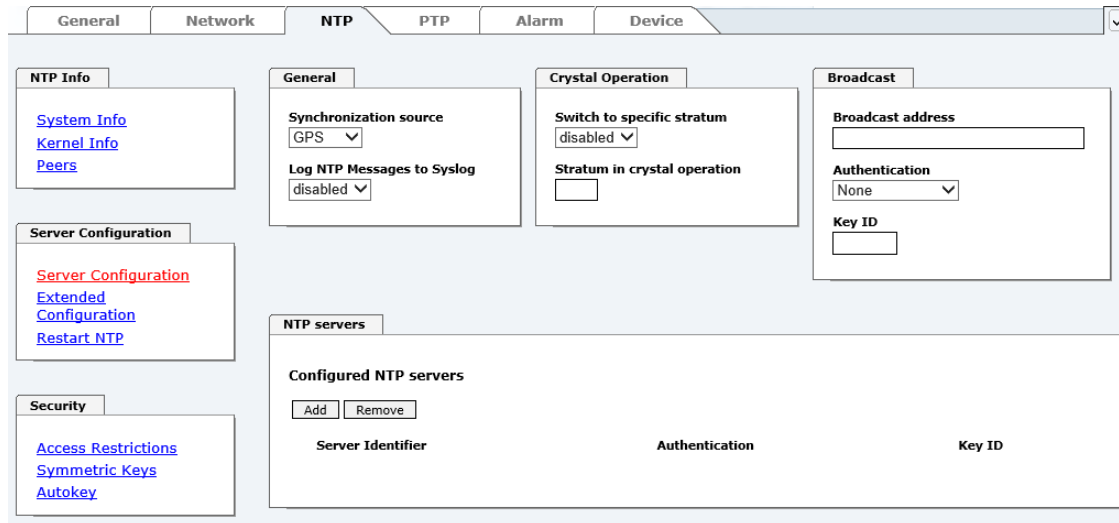
A short explanation and definition of the displayed values can be found in **chapter 10.6 Accuracy & NTP Basic Principles**.

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 10.2 Tally Codes (NTP-specific)**).

6.3.3.4 Server Configuration

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

The NTP-hopf-refclock driver is already configured as standard (127.127.38.0 in the "Peers Summary") and is not explicitly displayed here.

6.3.3.4.1 General / Synchronization Source

As *"Synchronization source"* either GPS or DCF77, depending on the appropriate Sync Source of the *hopf* Base System, has to be selected. This is reuiqred in order to align the NTP algorithm for the calculation of the accuracy with the synchronization source.

> ⚠ Based on the selection of GPS, even though GPS is not the source of the Sync Source (with the appropriate high accuracy) the value **HIGH** for **Accuracy** may never be reached.

6.3.3.4.2 General / Log NTP Messages to Syslog

This option enables or disables Syslog messages which are generated from the NTP service.

This value has no effect if this option is disabled or Syslog is not configured in the ALARM tab (see **Chapter 6.3.5.1 Syslog Configuration**).

6.3.3.4.3 Crystal Operation

Crystal Operation / Switch to specific stratum

If the **hopf** Base System runs in crystal operation (status "crystal") the NTP service of the Board 7274(RC) usually behaves in the way that the receipt of time information is stopped from the Sync Source and the stratum value reset to 16 (defined as invalid in NTP).

> ! NTP Clients does not accept time information from a NTP time server with stratum 16 (invalid). Briefly, as long as the Board 7274(RC) indicates the stratum value 16, NTP Clients are not synchronized.

This behaviour of NTP during crystal operation of the **hopf** Base System can be changed. Therefore the function "*Switch to specific stratum*" should be enabled by setting the value to "*enabled*" and the so-called downgrading stratum (= stratum value of the Board 7274(RC) during crystal operation of the Base System).

For the sychronization of NTP Clients during crystal operation of the Base System or for testing the system without connected synchronization source, in the setting "*enabled*" any stratum value between 1 and 15 can be set.

Crystal Operation / Stratum in crystal operation

The value defined here (range 1-15) designates the transmitted fallback NTP stratum level of the Board in "*Quartz*" synchronisation status. Stratum 1 should be configured if downgrading is not desired in status "Quartz" of the base system.

> ! The NTP service MUST also be restarted (see **Chapter 6.3.3.6 Restart NTP**.

> ! Using the option "*Switch to specific stratum*" the NTP Clients are synchronized with time information indicated in the general menu of the WebGUI of the Sync Source during crystal operating of the Base System. Whether this time information (e.g. through drift) is imprecise or the time is manually set (wrong) cannot be detected by the NTP Client!

> ! In case the value 1 is used for *"Stratum in crystal operation"*, the NTP Client cannot not verify whether the Base System is synchronised or runs in crystal operation. Should a differentiation be wished between synchronized and crystal operation the downgrading stratum needs to be set to a value between 2 and 15.

The value is only adjustable if the "*Switch to specific stratum*" function is enabled.

6.3.3.4.4 Broadcast / Broadcast Address

This section is used to configure the Board as a broadcast or multicast server.

The broadcast mode in NTPv3 and NTPv4 is limited to clients on the same sub-network and Ethernet 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) on the LAN Board. Care should be taken to ensure that the correct broadcast address is used for the sub-network, usually xxx.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 LAN Board 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.

6.3.3.4.5 Broadcast / 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.

6.3.3.4.6 Additional NTP SERVERS

The addition of further NTP servers provides the opportunity to implement a security system for the time service. However, this has an effect on the accuracy and stability of the Board.

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

6.3.3.5 Extended NTP Configuration

NTP is a protocol for synchronising clocks of computer systems over packet-switched data networks. For special applications the NTP time base of Board 7274(RC) can be configured to local and standard time via the base system.

For activation of this special NTP output, the customer's approval shown in the WebGUI needed to be declared by checking the field "I agree".

6.3.3.5.1 Suppression of unspecified NTP outputs (Block Output when Stratum Unspecified)

Unspecified NTP outputs that e.g. are generated by NTP at re-start, are suppressed when this function is activated.

6.3.3.5.2 NTP Timebase

For custom applications this function enables adjustment of the time base of the NTP output.

Entering this function the transmitted time protocol of the Board 7274(RC) is not conform to the NTP standard anymore.
According to the NTP standard NTP uses only the UTC time base. The NTP time protocol does not allow any leaps in time.

This function is only allowed for the Output of NTP
In case of activated function the output of the Board 7274(RC) for *SINEC H1 TIME DATAGRAM / TIME / DAYTIME* is released with a wrong time basis. Therefore this datagram should be deactivated for security reasons.

Following configuration steps for the activation of the NTP time basis are required:

- Select the wished NTP time base.

- Transfer the setting with **Apply Changes** to the board 7274.

- Fail-save storage of the configuration by pressing **Save to Flash within 10 seconds**.
  Depending on the activated time base leap a board reset might be released after transfer with Apply Changes eliminating non saved configurations.

UTC - NTP with Time Basis UTC

According to the RFC standard NTP uses only the UTC time base.

NTP with the Time Base Standard Time

Using the NTP time protocol with the standard time base the released time information correspond with UTC plus the time difference, adjusted in the base system **<u>without</u>** considering the daylight saving time changeover.

NTP with the Time Base Local Time

Output of the NTP time protocol with the local time base the released time information correspond with UTC plus the time difference and the additional offset for the possible summer time, adjusted in the base system.

NTP does not allow any leaps in time. Using the NTP time protocol with the local time base the internal NTP process of a board is restarted based on a summer-/winter time adjustment.

Using the NTP time protocol with the local time base the summer-/winter time adjustment is released one to two minutes belated.

Afterwards the local time is correctly available in the NTP time protocol. Therefore, within this transition period a requested NTP time protocol is replied by the former time base.
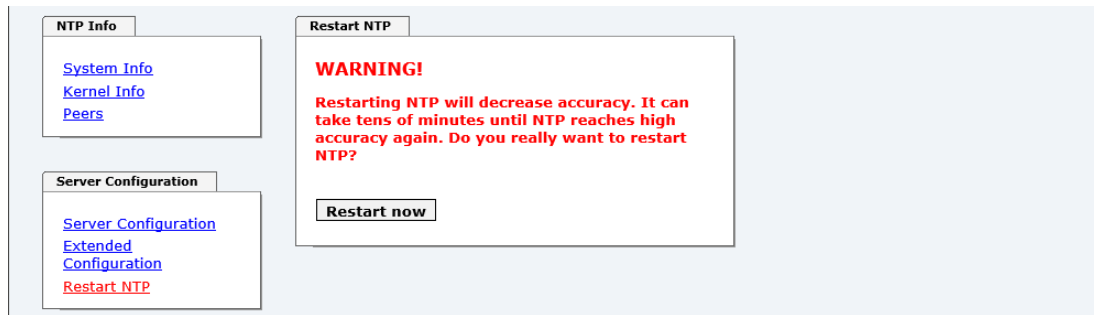
Changing the time base for the output of the protocol for NTP is only designed for customized applications and does not correspond with the standard of NTP. The synchronisation of a standard NTP-Client with a time basis deviating from UTC results in a wrong time information in the standard NTP-Client and might cause time leaps!

6.3.3.6 Restart NTP

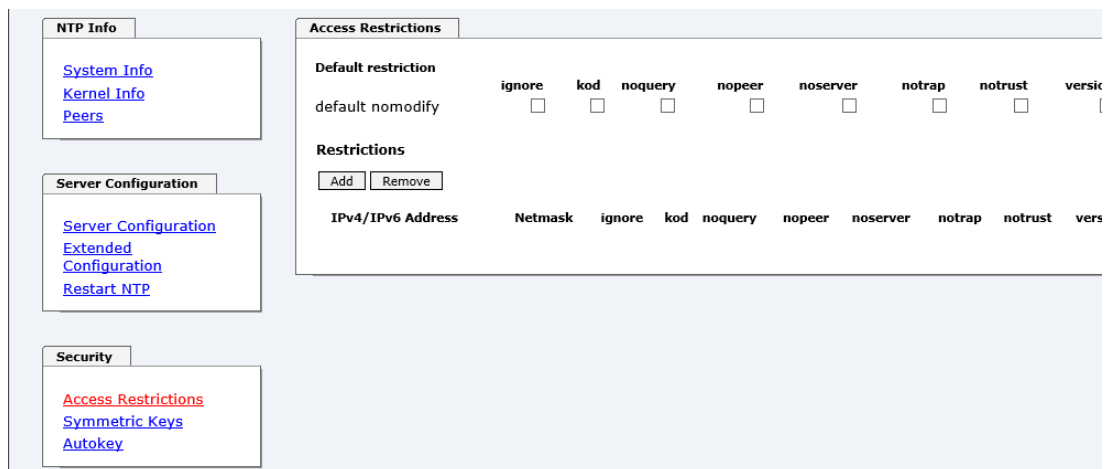The following screen appears after clicking on the Restart NTP option:

Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Board 7274(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 up to 10 minutes until the NTP service on the Board 7274(RC) is completely adjusted and synchronised with the system time of the base system again.

6.3.3.7 Access Restrictions / Configuring the NTP Service Restrictions

One of the extended configuration options for NTP is "Access Restrictions".

Restrictions are used in order to control access to the Board'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 http://www.ntp.org/.

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

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

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 from hosts (including remote time servers) and sub-networks which otherwise have no special restrictions.

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

Before beginning the configuration the points *6.3.3.7.1* to *6.3.3.7.4* must be checked by the user:

6.3.3.7.1 NAT or Firewall

Are incoming connections to the NTP Service blocked by NAT or a Stateful Inspection Firewall?	
No	Proceed to *Chapter 6.3.3.7.2 Blocking Unauthorised Access*
Yes	No restrictions are required in this case. Proceed further to *Chapter 6.3.3.7.4 Internal Client Protection / Local Network Threat Level*

6.3.3.7.2 Blocking Unauthorised Access

Is it really necessary to block all connections from unauthorised hosts if the NTP Service is openly accessible?	
No	Proceed to *Chapter 6.3.3.7.3 Allow Client* Requests
Yes	In this case the following restrictions are to be used: **ignore in the default restrictions** ☑ 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 *Chapter 6.3.3.7.5 Addition of Exceptions to Standard*

6.3.3.7.3 Allow Client Requests

	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 LAN Board, operating system and NTPD version)?	
No	In this case select from the following standard restrictions: See *Chapter 6.3.3.7.6 Access Control Options* **kod** **notrap** **nopeer** **noquery**.	✓ ✓ ✓ ✓
Yes	In this case select from the following standard restrictions: See *Chapter 6.3.3.7.6 Access Control Options*: **kod** **notrap** **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 *Chapter 6.3.3.7.5 Addition of Exceptions to Standard .*	✓ ✓ ✓

6.3.3.7.4 Internal Client Protection / Local Network Threat Level

	How much protection from internal network clients is required?	
Yes	The following restrictions can be enabled if greater security settings than the installed authentication are required in order to protect the NTP service from the clients see *Chapter 6.3.3.7.6 Access Control Options.* **kod** **notrap** **nopeer**	✓ ✓ ✓

6.3.3.7.5 Addition of Exceptions to Standard Restrictions

After the standard restrictions have been set, 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.

> ℹ️ Unrestricted access of Board 7274(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 of the remote time server.

Enable restrictions: e.g.

notrap / nopeer / **noquery** ☑

Allow **unrestricted access** 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 and query server statistics:

Restrictions: Press ADD

IP address 192.168.1.0

Network mask   255.255.255.0

notrap / nopeer   ☑

6.3.3.7.6 Access Control Options

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

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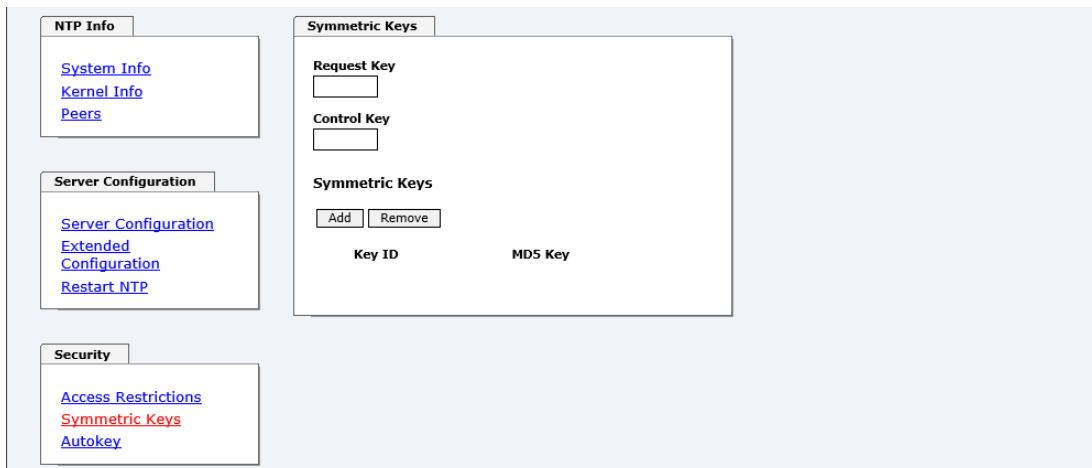
version – "Denies packets which do not correspond to the current NTP version."

> **⚠** Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see **Chapter 6.3.3.6 Restart NTP**).

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

6.3.3.8 Symmetric Key and Autokey

6.3.3.8.1 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

6.3.3.8.2 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 is 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" 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 NTP LAN board). 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.

6.3.3.8.3 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:**[ ] ( ) * - _ ! $ % & / = ?**).

A new line can be inserted by pressing the `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/.

6.3.3.8.4 How does authentication work?

Basic authentication is a digital signature and not data encryption (if there is any difference between the two). The data packet and the key are used to create a non-reversible number which is attached to the packet.
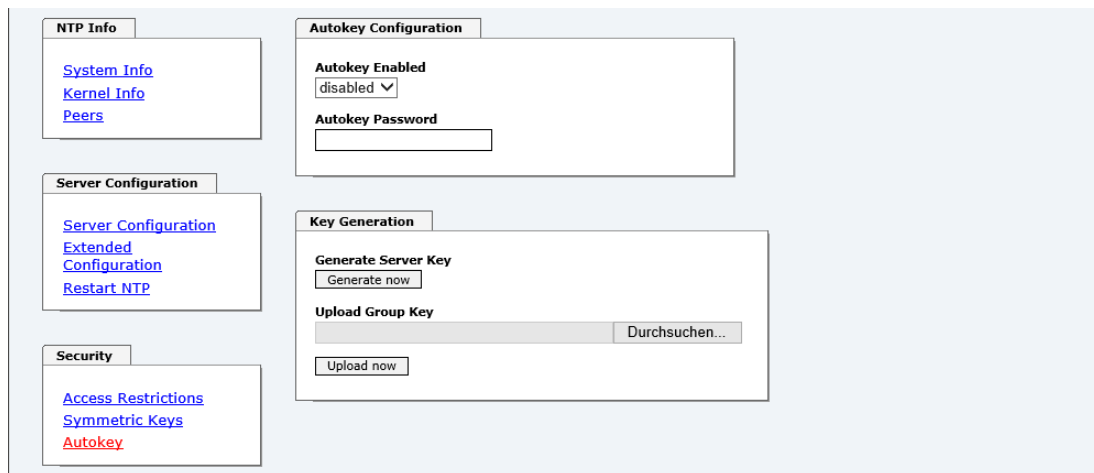
The receiver (which has the same key) carries out the same calculation and compares the results. Authentication has been successful if the results concur.

6.3.3.9 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.

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 7274(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 (http://www.ntp.org/).

> ⚠ Changes in data do not take effect immediately after clicking on the "Apply" symbol. The NTP service MUST also be restarted (see **Chapter 6.3.3.6 Restart** NTP).

6.3.4　PTP Tab

This Tab shows information and adjustment possibilities of the PTP service of the Time Server 7274(RC).
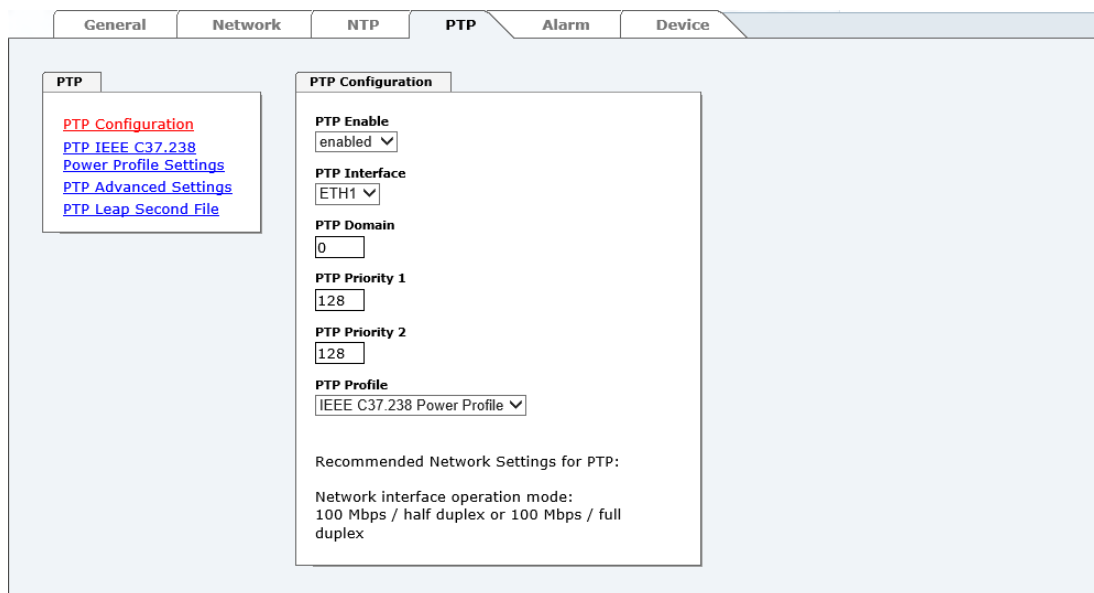
PTP functionality is provided by a PTP-Demon running on the embedded Linux of the Time Server 7274(RC).

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.

6.3.4.1　PTP Configuration

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

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".

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. The options in the "PTP IEEE C37.238 Power Profile Settings" window are only used by the PTP service when this profile is selected.

If "None" is selected, the settings in the "PTP Advanced Settings" window can be modified and the settings in the "PTP IEEE C37.238 Power Profile Settings" window are not used by the PTP service.

6.3.4.2 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.

PTP Grandmaster ID

This option controls the PTP Grandmaster ID.

- Value-range: 3 to 254

Time Zone Name
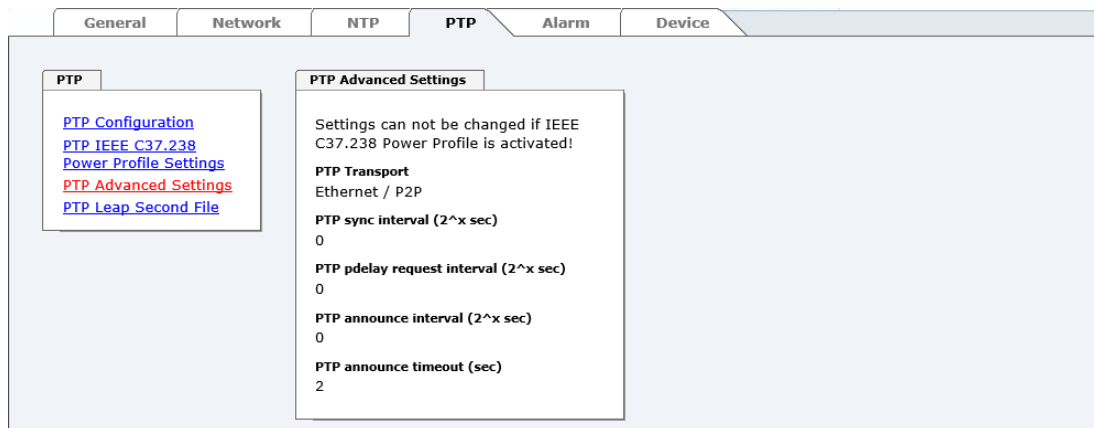
This option controls the time zone name.

- String length: 10 characters

This setting is used as "display name" in the "ALTERNATE_TIME_OFFSET_INDICATOR TLV". The other parameters that are needed by this TLV are taken from the system settings.

6.3.4.3 PTP Advanced Settings

The "PTP Advanced Settings" window supplies settings for the communication of the PTP service. These settings can be only changed, if the "PTP Profile" is set to "None" in the "PTP Configuration" window.

PTP Transport

This setting determines the network protocol that is used by the PTP service.

Possible choices: "Ethernet / P2P", "Ethernet / E2E" and "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^x 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.

6.3.4.4 PTP Leap Second File

The "PTP Leap Second File" window supplies a functionality to upload a Leap-Second-File to the Time Server 7274(RC).

This file informs the PTP service, how many seconds UTC and TAI time differs.

In case of announcing a leap second by the synchronization source the leap second file will automatically be updated.

If the device is not in operation during the whole announcing time, it is not possible for the application to update its leap second file. The leap second file needs to be updated next time when the device is put in operation.

> **i** On the following website
> https://www.ietf.org/timezones/data/leap-seconds.list
> a current version of the leap second file can be downloaded.

UTC-TAI offset

This field shows the actual value, that the PTP service uses, for the difference of UTC and TAI time.

Date of Next Leap Second

This box shows if and if yes when the next leap second is going to be inserted.

6.3.5 ALARM Tab

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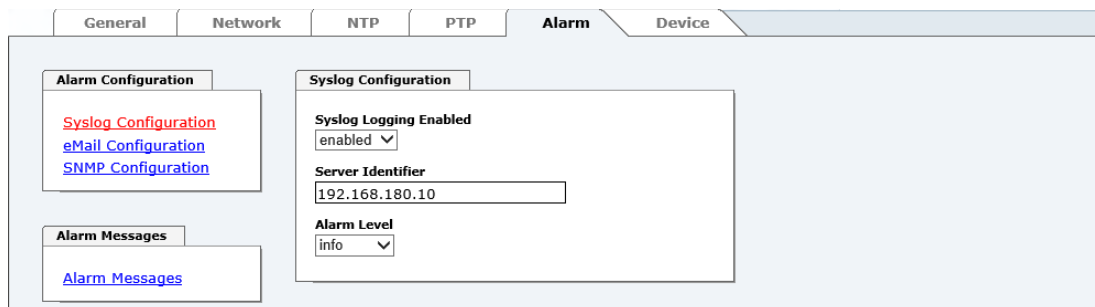
6.3.5.1 Syslog Configuration

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 Linux/Unix 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 internal memory is not of sufficient size.

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

The alarm level designates the priority level of the messages to be transmitted and the level from which transmission is to take place (see ***Chapter 6.3.5.4 Alarm Messages***).

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

The NTP service implemented on this Board can transmit its own Syslog messages
(see ***Chapter 6.3.3.4.2 General / Log NTP Messages to Syslog***).

Generated Syslog messages of Board 7274(RC) are described in ***Chapter 10.5 Syslog Messages***.

6.3.5.2 E-mail Configuration

E-mail notification is one of the important features of this device which offer 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.

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

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.
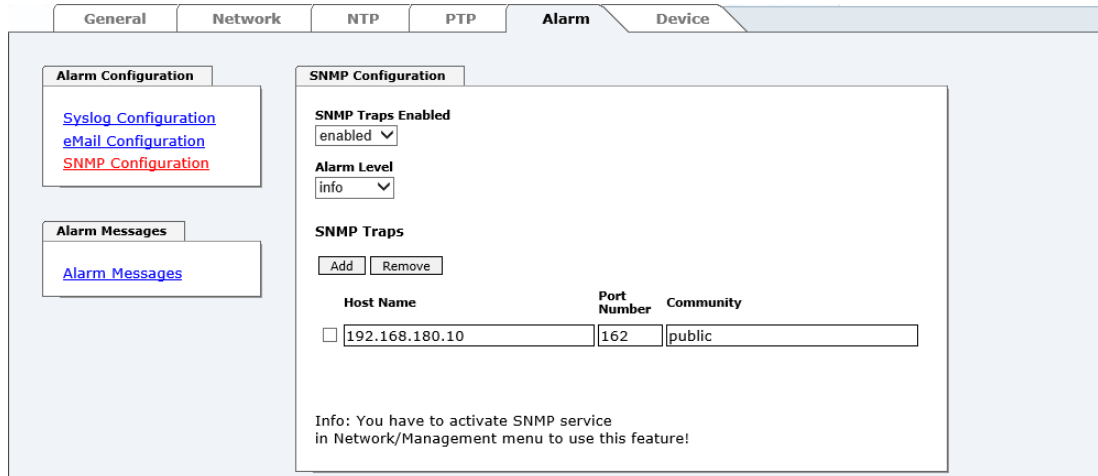
The Alarm Level designates the priority level of the messages to be sent and the level from which they are to be sent (see **Chapter 6.3.5.4 Alarm Messages**).

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

6.3.5.3 SNMP Configuration / TRAP Configuration

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

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 6.3.6.11 Downloading Configurations / SNMP MIB**).

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 6.3.5.4 Alarm Messages**).

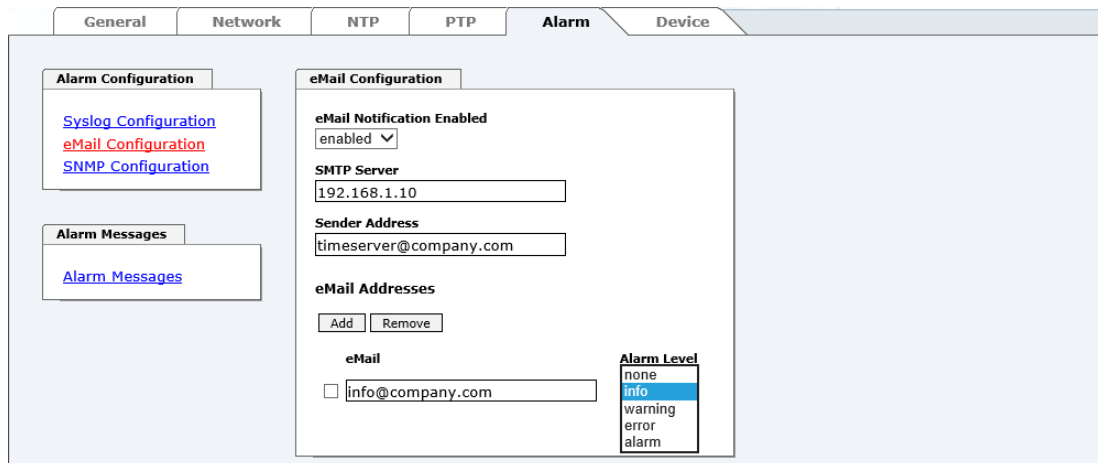| Alarm Level	Transmitted Messages
none	no messages
info	info / warning / error / alarm
warning	warning / error / alarm
error	error / alarm
alarm	alarm
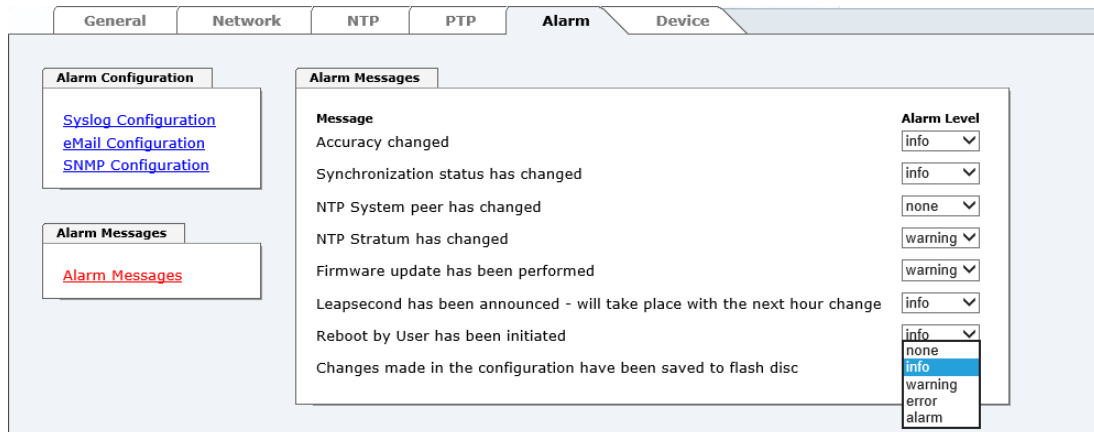
> ⚠ SNMP protocol must be enabled in order to use SNMP (see **Chapter 6.3.2.7 Management-Protocols – HTTP, SNMP etc.**).

6.3.5.4 Alarm Messages

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.

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.

6.3.6 DEVICE Tab

All the links within the tabs on the left hand side lead to corresponding detailed setting options.
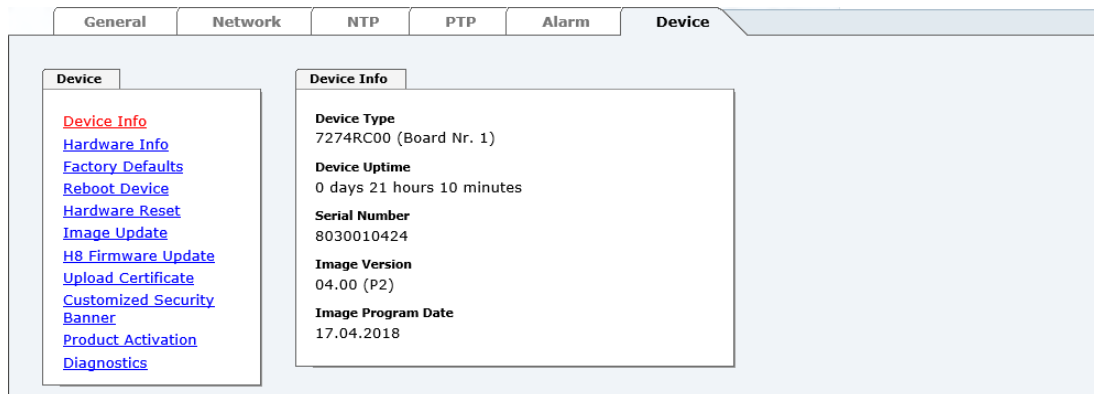
This tab provides the basic information about the Board hardware and software/firmware. Password administration and the update services for the Board are also made accessible via this website. The complete download zone is also a component of this site.

6.3.6.1 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.

6.3.6.2 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, hardware status etc.
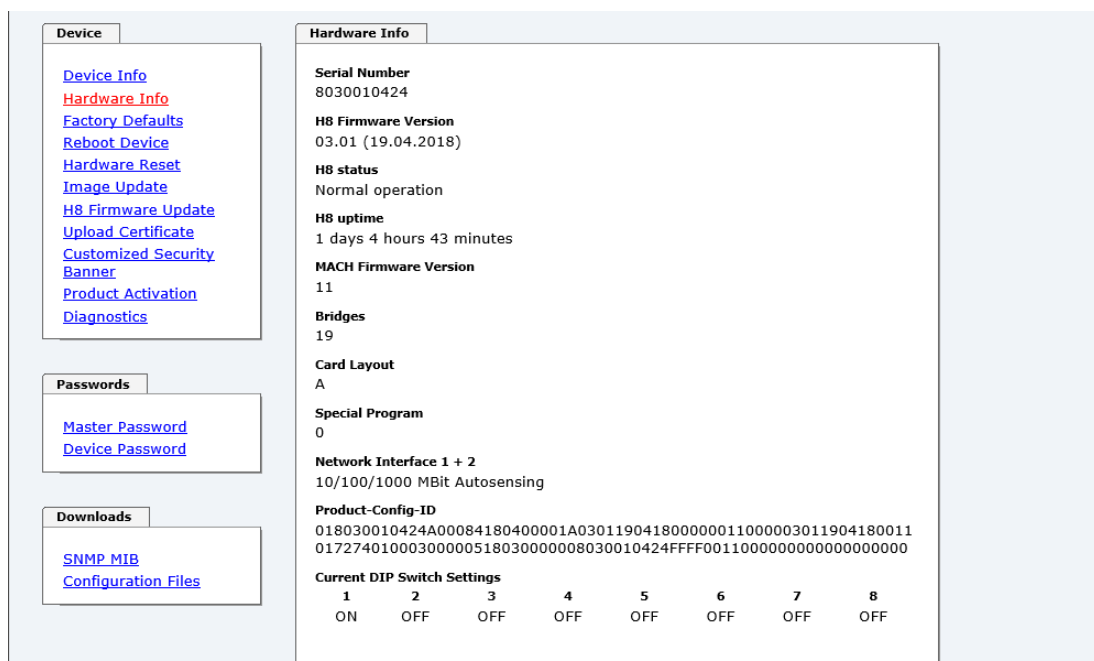
The settings of the DIP-switch on the Board 7274(RC) will be shown under the point "Current DIP Switch Settings".

6.3.6.3 Restoring the Factory Settings - Factory Defaults

In some cases it may be necessary or desirable to restore all of the Board's settings to their delivered condition (factory defaults).
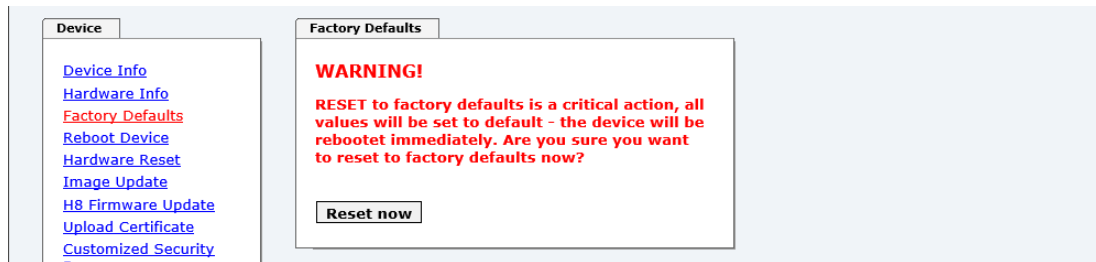
This function serves to restore all values in the flash memory to their default values. This also includes passwords (see *Chapter 9 Factory Defaults of Board 7274(RC)*).

Please log in as a "Master" user in accordance with the description in *Chapter 6.2.1 LOGIN and LOGOUT as a User*

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

Once this procedure has been triggered there is NO possibility of restoring the deleted configuration.

> After a factory default a complete check (and reconfiguration of the Board where appropriate) is required. In particular, the default MASTER and DEVICE passwords must be reset.

6.3.6.4 Restarting the Board (Reboot Device / Hardware Reset)

> ⚠ The restart concerns Board 7274(RC) only.

Reboot Device: Restart of the internal Operating System

Hardware Reset: Board Reset including all Hardware components

> ⚠ All settings not saved with "**Save**" are lost on Reboot / Hardware Reset (see **Chapter 6.2.3 Entry 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 6.2.1 LOGIN and LOGOUT as a User**.

Pressing the "**Reset now**" or "**Perform Reset now**" button releases a restart.

6.3.6.5 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 2.4 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.
> - 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 *hopf* 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 Internet 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 always executed as software set. I.e. H8 firmware update + 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 2.4 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_8030_v0114_128.**mot**   for the **H8 firmware**
(update takes approx. 1-1.5 minutes)

upgrade_8030gen_v0120.**img**   for the **embedded image**
(update takes approx. 2-3 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.
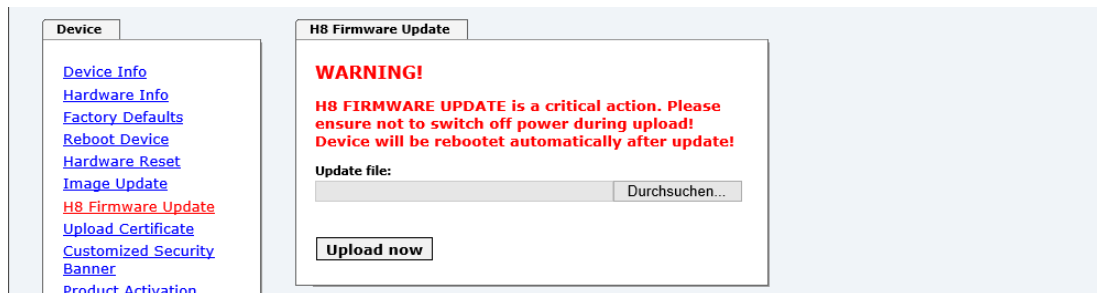
A restart of the Board with the new Firmware is done automatically after the H8-Firmware update.

The procedure for the **Image update** differs only in how the Board is restarted.
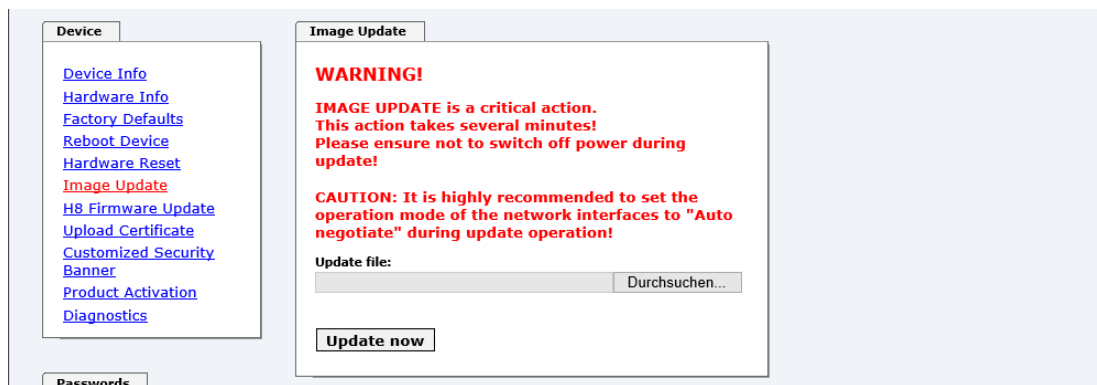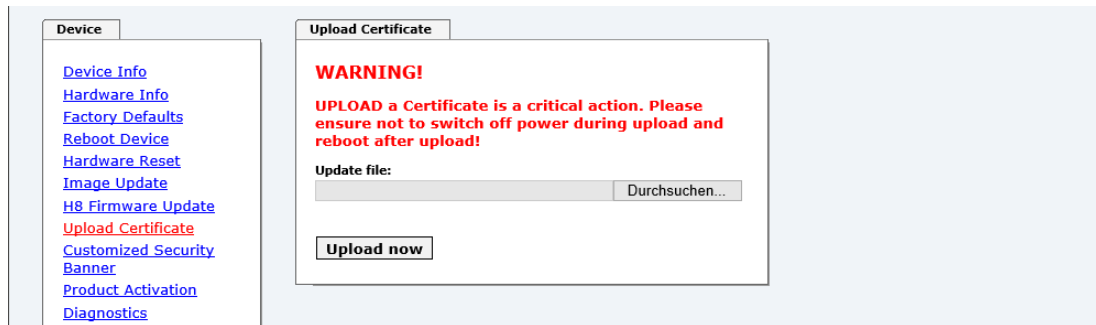
After the image-update the WebGUI displays a window to confirm the restart (reboot) of the board.
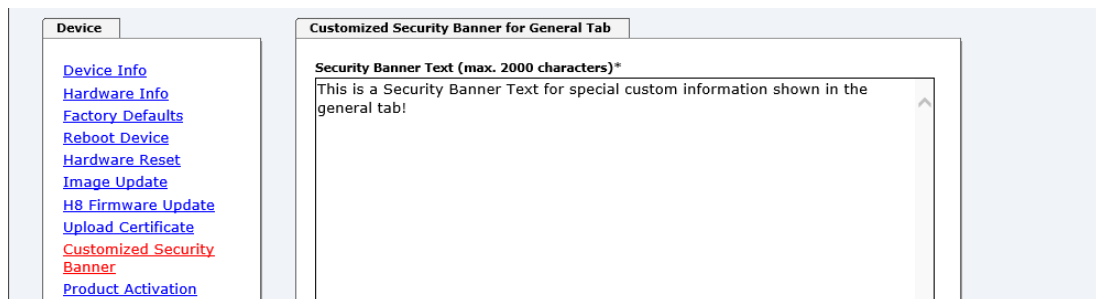
6.3.6.6 Upload SSL-Server-Certificate

This offers the possibility to encrypt the https connections to the board 7274 (RC) with a user-provided SSL server certificate.

6.3.6.7 Customized Security Banner
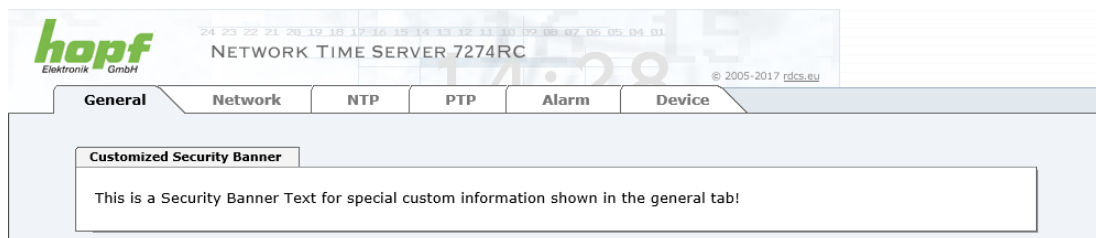
Special security information which are displayed in the General-Tab can be entered here by the user.

The security information can be written as 'unformatted' text. 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 ("**?**")

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.

6.3.6.8 Product Activation

Optional features (e.g. Network Interface Bonding/Teaming) can be activated using a special activation key which can be requested from *hopf* Elektronik GmbH.
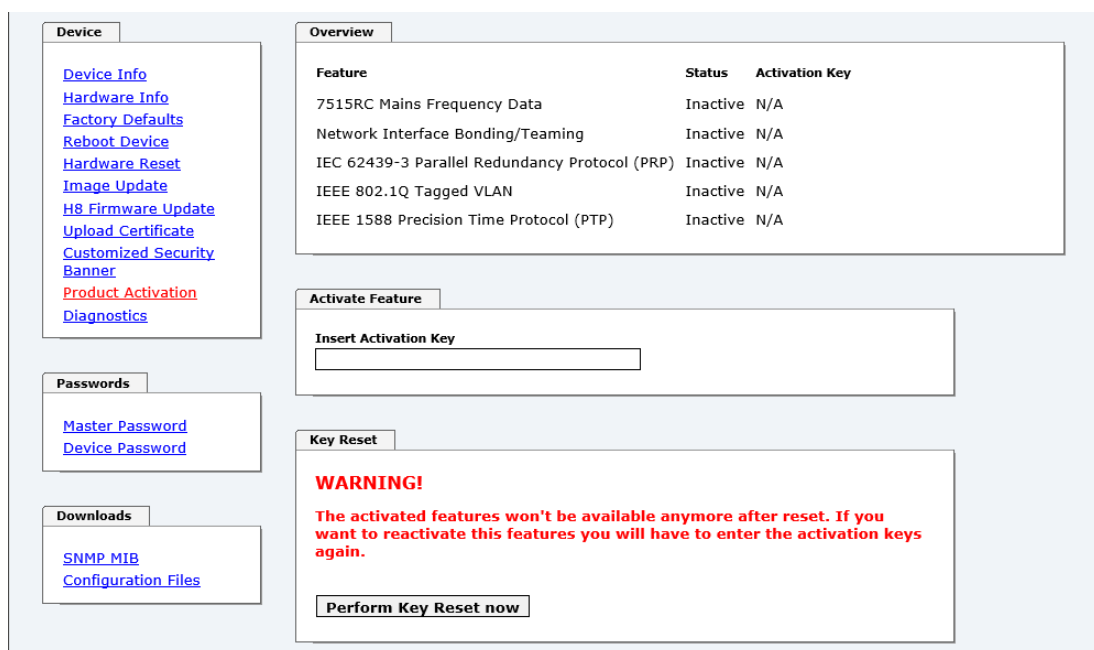
An activation key is bound to a specific board and cannot be shared between different boards.

⚠	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.

Device

Device Info
Hardware Info
Factory Defaults
Reboot Device
Hardware Reset
Image Update
H8 Firmware Update
Upload Certificate
Customized Security Banner
Product Activation
Diagnostics

Passwords

Master Password
Device Password

Downloads

SNMP MIB
Configuration Files

Overview

Feature	Status	Activation Key
7515RC Mains Frequency Data	Inactive	N/A
Network Interface Bonding/Teaming	Inactive	N/A
IEC 62439-3 Parallel Redundancy Protocol (PRP)	Inactive	N/A
IEEE 802.1Q Tagged VLAN	Inactive	N/A
IEEE 1588 Precision Time Protocol (PTP)	Inactive	N/A

Activate Feature

Insert Activation Key

Key Reset

WARNING!
The activated features won't be available anymore after reset. If you want to reactivate this features you will have to enter the activation keys again.

Perform Key Reset now

Overview
List of all options with its current activation status and the stored activation key.

Activate Feature
Input field to enter a new activation key. The activation key has 26 characters and can be entered case insensitive. After entering a key the feature can be activated by pressing the ☑ Apply button. If 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". No optional feature is available anymore after performing the Key Reset. If the feature is enabled again, the last configuration for the optional feature is restored.

6.3.6.9 Diagnostics Function

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

Device	Real Time Diagnostics
Device Info Hardware Info Factory Defaults Reboot Device Hardware Reset Image Update H8 Firmware Update Upload Certificate Customized Security Banner Product Activation Diagnostics	**Status Messages** disabled ▾ **Hardware Log** **Download Hardware Log** 📄 Click here to download Refresh Hardware Log

6.3.6.10 Passwords (Master/Device)

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

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

(See also *Chapter 6.2.1 LOGIN and LOGOUT as a User*)
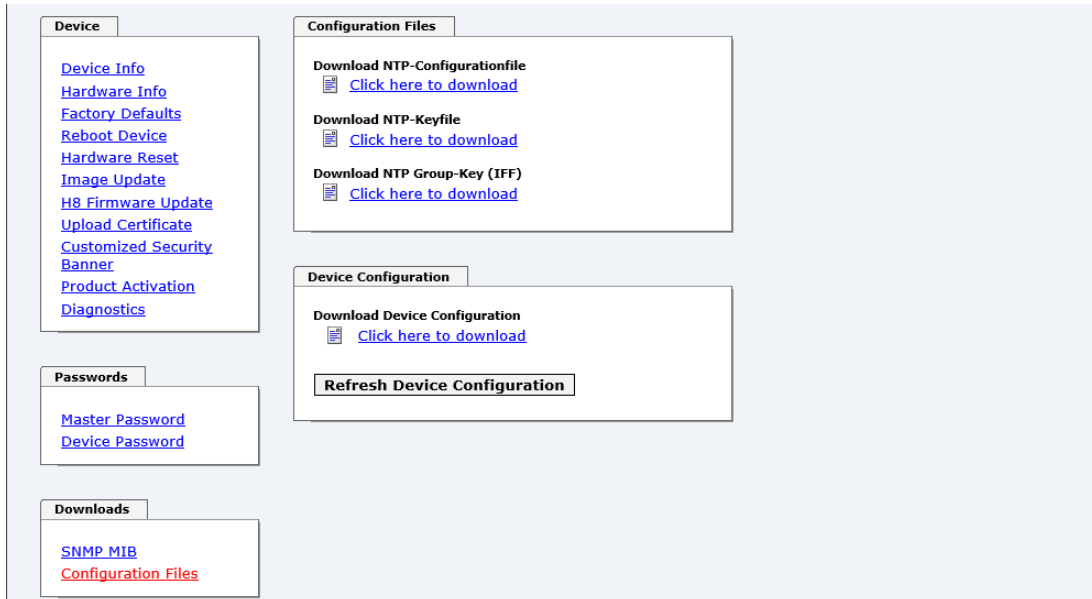
> ⚠ A new password must contain at least one capital letter and lowercase letter, a number, and six characters.

6.3.6.11 Downloading Configurations / SNMP MIB

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.

ℹ️ The loaded file **System Configuration** from the board is only used for support purposes and cannot be reloaded for adjusting the settings.

⚠️ Before a file **System Configuration** download it is imperative to press the button `Refresh System Configuration` .

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

7 SSH and Telnet Basic Configuration

> ⚠ Only basic configuration is possible via SSH or Telnet. The complete configuration of Board 7274(RC) 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 6.3.6.10 Passwords (Master/Device)**).

> ⚠ SSH does not allow blank passwords for safety reasons.

> ⚠ The corresponding service is to be enabled for the use of Telnet or SSH (see **Chapter 6.3.2.7 Management-Protocols – HTTP, SNMP etc.**)

```
  N    N  TTTTTTT   SSSSS
  NN   N     T     S     S
  N N  N     T     S
  N  N N     T      SSSSS
  N   NN     T     S     S
  N    N     T      SSSSS


  hopf 727400 NTS BOARD (c) 2006 - 2013



  Press Enter to continue



Main Menu

  1 ... General
  2 ... Network
  3 ... Alarm
  4 ... NTP
  5 ... Device Info
  0 ... Exit

Choose a Number =>
```
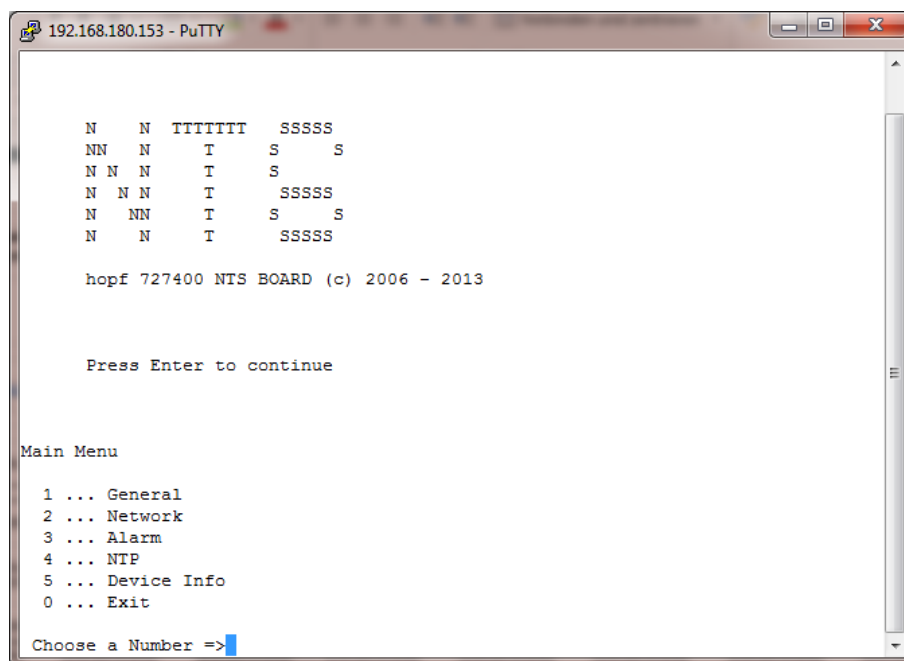
Navigation through the menu takes place by entering the respective number associated with the menu option (as can be seen in the above image).

8   Technical Data

General technical Data of the Board 7274(RC).

Assembly	
Model	Euro-board 160 x 100 mm
Power supply	
internal system voltage Vpp	5V DC ± 5% via system bus

Environmental Conditions		
Temperature range: operation:	0°C to +40°C	
storage:	-20°C to +75°C	
Humidity:	max. 95%, not condensed	

GPS System - Accuracy		
Lambda < 15ms	Stability < 0.2ppm	HIGH
Lambda < 15ms	Stability >= 0.2ppm und <= 2ppm, Offset < 1ms	HIGH
Lambda < 15ms	Stability > 2ppm oder Offset >= 1ms	MEDIUM
DCF77 System - Accuracy		
Lambda < 15ms	Stability < 0.6ppm	HIGH
Lambda < 15ms	Stability >= 0.6ppm und <= 2ppm, Offset < 2ms	HIGH
Lambda < 15ms	Stability > 2ppm oder Offset >= 2ms	MEDIUM

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
- PPS Time Source
- RFC-867 DAYTIME Server
- RFC-868 TIME Server
- SINEC H1 time datagram

TCP/IP Network Protocols

- HTTP/ HTTPS
- FTP
- Telnet
- SSH
- SNMPv2c / SNMPv3
- NTP (including SNTP)
- SINEC H1 time datagram

Configuration

- HTTP/HTTPS-WebGUI (Browser Based)
- Telnet
- SSH
- *hopf* Base System via keypad and display resp. *hmc* remote access
- *hmc* network configuration assistant

Power consumption – internal	
Normal operation	Typical: 550 mA (max. 850 mA)
Boot phase	Typical: 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 networks 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. Depending on the network configuration in use (e.g. DHCP) an extension of the boot phase can occur.
MTBF	
MTBF	> 740,000 hours

Ambient Conditions		
Temperature range:	Operation:	0°C to +55°C
	Storage:	-20°C to +75°C
Humidity:		max. 95%, non condensing

9 Factory Defaults of Board 7274(RC)

The default delivery status of the Board 7274(RC) meets the factory default values when using GPS synchronization sources. In case of DCF77 synchronization (different product variant) the function **"NTP / General / Sync Source"** is factory-set to **"DCF77"** on delivery.

> ⚠ Using the board in DCF77 systems (different product variant) the setting for **NTP / General / Sync Source"** needs to be re-configured to **"DCF77"** after a factory default.

NTP Server Configuration	Setting	WebGUI
Sync. Source	DCF77	DCF77

9.1 Network

Host/Name Service	Setting	WebGUI
Hostname	Hopf7274	Hopf7274
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 Address	Blank	---
Default Gateway IPv6 Address	Blank	---
Network Interface ETH0	**Setting**	**WebGUI**
Use Custom Hardware Address (MAC)	Disabled	Disabled
Custom Hardware Address (MAC)	Blank	---
DHCP	Disabled	Disabled
IPv4 Address	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 Address	Blank	---
IPv4 Netmask	Blank	---
Operation mode	Auto negotiate	Auto negotiate
VLAN Interfaces	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	Blank	---
Management	**Setting**	**WebGUI**
HTTP	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	---
Time	**Setting**	**WebGUI**
NTP	Enabled	Enabled
DAYTIME	Disabled	Disabled
TIME	Disabled	Disabled
SINEC H1 time datagram	**Setting**	**WebGUI**
Send Interval	Every second	1 second
Time base	UTC	UTC
Destination MAC Address	09:00:06:03:FF:EF	09:00:06:03:FF:EF
Minimum Accuracy	LOW	LOW

9.2 NTP

NTP Server Configuration	**Setting**	**WebGUI**
Sync. source	GPS	GPS
NTP to Syslog	Disabled	disabled
Switch to specific stratum	Disabled	disabled
Stratum in crystal operation	Blank	---
Broadcast address	Blank	---
Authentication	Disabled	none
Key ID	Blank	---
Additional NTP Servers	Blank	---
NTP Extended Configuration	**Setting**	**WebGUI**
Limitation of Liability	Blank	---
Block Output when Stratum Unspecified	Disabled	disabled
Timebase (default: UTC)	UTC	UTC
NTP Access Restrictions	**Setting**	**WebGUI**
Access Restrictions	Disabled	default nomodify
NTP Symmetric Keys	**Setting**	**WebGUI**
Request Key	Blank	---
Control Key	Blank	---
Symmetric Keys	Blank	---
NTP Autokey	**Setting**	**WebGUI**
Autokey	Disabled	disabled
Password	Blank	---

9.3   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 pdelay request interval (2^x sec)	1 second	0
PTP announce interval (2^x sec)	1 second	0
PTP announce timeout (sec)	2 seconds	2

9.4   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

9.5   DEVICE

User Passwords	Settings	WebGUI
Master Password	master	---
Device Password	device	---
Diagnostic	**Einstellung**	**WebGUI**
Real Time Diagnostics	Disabled	disabled

10 Glossary and Abbreviations

10.1 NTP-specific terminology

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.

10.2 Tally Codes (NTP-specific)

space	reject	Rejected peer – either the peer is not reachable or its synchronisation 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 synchronisation 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 synchronisation distance.
*	sys.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System.
o	pps.peer	The peer was selected as a system peer. Its characteristics are transferred to the Base System. The current synchronisation is derived from a PPS (pulse-per-second) signal either indirectly via PPS reference clock driver or directly via kernel interface.

10.2.1 Time-specific expressions

UTC	**UTC Time** (**U**niversal **T**ime **C**oordinated) was dependent 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 segments or time zones. Today, however, there are a number of time zones which in part apply specifically to certain individual 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 Greenwich.
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 (winter time)	**Standard Time = UTC + Time Offset** The time offset is defined by the local time zone and the local political regulations.
Daylight Saving Time (summer time)	**Offset of Daylight Saving Time = + 1h** 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 **International Earth Rotation and Reference Systems Service (IERS)**.

10.3   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
PTP	Precision Time Protocol
PRP	Parallel Redundancy Protocol
RFC	Request for Comments
SNMP	Simple Network Management Protocol (handled by more than 60 RFCs)
SNTP	Simple Network Time Protocol
S, STD	Standard Time
TCP	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
VLAN	Virtual Local Area Network
WAN	Wide Area Network
msec	millisecond (10^{-3} seconds)
µsec	microsecond (10^{-6} seconds)
ppm	parts per million (10^{-6})

10.4 Definitions

An explanation of the terms used in this document.

10.4.1 DHCP (Dynamic Host Configuration Protocol)

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

> **i** See RFC 2131 Dynamic Host Configuration Protocol for further information

10.4.2 NTP (Network Time Protocol)

Network Time Protocol (NTP) is a standard for the synchronisation of clocks in computer systems over 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 roundtrip times.

NTP uses the Marzullo algorithm (devised by Keith Marzullo of San Diego University in his dissertation) with a UTC timescale and which 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 in 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.

> **i** See RFC 5905 for further information.

10.4.3 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 every network-compatible device can be monitored. The network management tasks which are possible with 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 offer hardly any safety mechanisms. The safety mechanisms have been significantly expanded in the current Version 3.

With the aid of description files known as MIB's (Management Information Base), the management programmes are in a position to represent the hierarchical structure of the data of any desired 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.

10.4.4 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 while 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.

10.4.5 PTP (Precision Time Protocol)

The Precision Time Protocol (PTP) is a standard for synchronising clocks in computer networks. Unlike NTP it focuses on a higher accuracy and local networks.

In a network with several PTP-devices, every PTP-device executes the Best Master Clock-algorithm, to determine which PTP-device has the highest accuracy. That PTP-device serves as reference clock and is called Grandmaster Clock.

The Grandmaster Clock sends SYNC messages periodically to distribute the actual time to the slaves. The slaves periodically send Delay Request- or Path Delay Request-messages to the Grandmaster Clock. The Grandmaster Clock replies to those messages with a Delay Respond or Path Delay Respond message. The PTP-devices take sending and reception timestamps of those messages and attach those timestamps to the messages. These timestamps allow the slave to calculate the network delay and the exact actual time. For calculating the network delay the slave assumes, that the network delay in both directions is the same.

The PTP-devices use either Ethernet or UDP for their network communication. UDP uses the Ports 319 and 320.

10.5   Syslog Messages

Description of the Syslog messages of the Board 7274(RC) configured by the alarm messages. Further Syslog messages generated by the operating system (e.g. NTP, Syslog-Deamon, …) are not described here.

Type	Message	Values %1, %2
G	NTP Accuracy change - **Accuracy changed to %1 !**	**LOW, MEDIUM, HIGH**
G	Synchronization status change - **Synchstatus changed from %1 to %2**	**I, C, r, R**
G	NTP System peer change - **System peer changed from %1 to %2**	**HOPF_S(0)** *hopf-System* " " no peer, **IP-Adresse, DNS-Name**
G	NTP Stratum change - **Stratum changed from %1 to %2**	**0, 1, 2,... 16**
E	Firmware **Firmware update performed**	**-**
E	Announcement of leap second **Leap second has been announced - will take place with the next hour change**	**-**
E	Reboot **Reboot by user has been initiated**	**-**
E	Changes of configuration **Changes made in the configuration have been saved to flash disc**	**-**

Type of message (E : single-point information ; G : group information)

10.6   Accuracy & NTP Basic Principles

> ⚠ NTP is based on Internet protocol. Transmission delays and errors and the loss of data packets can lead to unpredictable accuracy data and time synchronisation effects.

> ℹ NTP protocol neither defines nor guarantees the accuracy or correctness of the time server.

Thus the QOS (Quality of Service) used for direct synchronisation with GPS or serial interface does not apply to synchronisation via NTP.

In simplified terms, accuracies of between 1msec and 1sec can be expected, depending on the accuracies of the servers used.

The accuracy of IP-based time synchronisation is dependent on the following criteria:

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

NTP 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:

1. 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 can neither be measured nor calculated by NTP. NTP works on the assumption that the transmission path to the NTP server 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 greater than the accuracy resolution of the local clock on the NTP server and NTP client.

With reference to the above mentioned error circumstances, the delivered **time offset** of the NTP 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 synchronisation 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 Board is responsible for the network conditions between the Board and the NTP clients.

As an example, we mention the case where a network has a delay of 500msec and an accuracy shift (asynchronisation.) 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.

11   List of RFC

- 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)

12   List of Open Source Packages used

Third Party Software

The **hopf** network TimeServer 7274(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 availibility of the source code the package is provided electronically (email, download etc.) on requested.

The following table includes all uses 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 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 IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, 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 ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.	no
dosfstools	3.0.28	GPL	v3	no

Package name	Version	Licence	Licence details	Patches
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
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-automake	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 modified because it originated at the Lawrence Berkeley (not Livermore!) Laboratory, which operates under a contract with the Department of Energy:	no

host-flex licence details (continued):

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:

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 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 WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES 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.

Package name	Version	Licence	Licence details	Patches
host-genext2fs	1.4.1	GPL	v2	no
host-gettext	0.19.7	GPL	v3	no
host-kmod	22	LGPL	v2.1	no
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 person obtaining a copy of this software and associated documentation 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, INCLUDING 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 LIABILITY, 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.	no
			Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation 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, INCLUDING 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 LIABILITY, 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-lzo	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.	no
			Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated	

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

Package name	Version	Licence	Licence details	Patches
			documentation 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:	
			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, INCLUDING 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 CONNECTION 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 authors (see AUTHORS).	no
			Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission 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 implied 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 alter it and redistribute it freely, subject to the following restrictions:	
			1. 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 acknowledgment in the product documentation would be appreciated 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

Package name	Version	Licence	Licence details	Patches
ipkg	0.99.163	GPL	v2	no
iproute2	4.4.0	GPL	v2	no
iptables	1.6.0	GPL		no
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
lm-sensors	3.4.0	LGPL	v2.1	no
lshw	B.02.17	GPL	v2	no
lua	5.3.2	MIT License		no
lzo	2.09	GPL	v2	no
lzop	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 software licence	Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the	no

7274 and 7274RC NTP/SINEC H1 LAN Board - V04.00

Package name	Version	Licence	Licence details	Patches
			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:	
			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, INCLUDING 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 CONNECTION 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 software 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 notice and this permission notice appear in supporting documentation, 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 provided "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 Documentation License	V1.3	no
pps-tools	0deb9c7e13 5e9380a6d0 9e9d2e938a 146bb698c8	GPL	v2	no
prp	1.4	Permissive free software licence	Copyright (c) 2007, Institute of Embedded Systems at Zurich University of Applied Sciences (http://ines.zhaw.ch) 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	yes

Package name	Version	Licence	Licence details	Patches
			disclaimer in the documentation and/or other materials provided with the distribution. - Neither the name of the Zurich University of Applied Sciences nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.	
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 domain		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
ti-tools	06dbdb2727 354b5f3ad7 c723897f40 051fddee49		Copyright(c) 1998 - 2010 Texas Instruments. All rights reserved. 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 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 Texas Instruments 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 BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, 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	no

Package name	Version	Licence	Licence details	Patches
			TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.	
uboot	2010.06	GPL	v2	no
uboot-tools	2016.01	GPL	v2	no
usb_modeswitch	2.2.6	GPL	v2	no
usb_modeswitch_data	20151101	GPL	v2	no
util-linux	2.27.1	GPL	v2	no
zlib	1.2.8	Permissive free software licence	http://www.gzip.org/zlib/zlib_license.html	no