# Industriefunkuhren

*hopf*
Elektronik GmbH

_____

# Technical Manual

NTP/SINEC H1 LAN Board

# Model 7273 and 7273RC

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

ENGLISH

**Version: 05.01  –  24.10.2016**

_____

## 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 7271/7273 (SEE *CHAPTER 6.3.5.1 Device Information* AND *CHAPTER 6.3.5.2 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.

## Contents            Page

# 1 Board Description 7273 and 7273RC

The LAN Boards 7273 and 7273RC 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 7273 and 7273RC provide functions and fields of applications completely backward compatible to the boards 7271 and 7271RC.
>
> The boards 7273 and 7273RC can be used as direct replacements for already supplied boards 7271 or rather 7271RC. The successor boards provide all functions, adjustment options and protocols as offered by the boards 7271 and 7271RC.
>
> The successor boards are suitable for extensions of *hopf* Clock Systems, already operating boards 7271 or rather 7271RC (mixed operation) without problems.

The boards 7273 and 7273RC are equipped with Ethernet interface (ETH0) 10/100 Base-T (autosensing).

> **i**
>
> The boards 7273 and 7273RC are prepared for a later operation in IPv6 networks. Currently just IPv4 is supported.

The boards 7273 and 7273RC 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

The network connection of the LAN boards 7273 and 7273RC can be installed at any desired point on the network. Each board 7273/7273RC 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 7273 or 7273RC 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:
    o HTTP/HTTPS WebGUI (**G**raphical **U**ser **I**nterface)
    o Or text-based menus over Telnet and SSH
- Various protocols (e.g. IPv4, http, https, Telnet etc.) are available for the Ethernet connection.

Some basic features of the boards:

**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
- SINEC H1 time datagram
- RFC-867 DAYTIME Server
- RFC-868 TIME Server

**Network Protocols**

- HTTP/ HTTPS
- DHCP
- Telnet
- SSH
- SNMPv2 / SNMPv3, SNMP Traps (MIB II, Private Enterprise MIB)
- NTP (including SNTP)
- SINEC H1 time datagram

**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 7273RC only
- *hopf* 7001 system keypad and display – Board 7273 only
- *hopf* 68xx system (3U/Slim Line) keypad and display – Board 7273 only
- *hmc* Remote connection (for basic systems with remote function)

**Ethernet Interface**

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

**Additionally at Board 7273RC**

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

**Features**

- HTTP/HTTPS (status, control)
- SNMPv2 / SNMPv3, SNMP Traps (MIB-II, Private Enterprise MIB)
- E-mail notification
- Syslog messages to external syslog server
- Update via TCP/IP
- Fail-safe
- Watchdog circuit
- Power management
- System management
- Customized security banner

## 1.1 Differences between the Boards 7273 and 7273RC

The board 7273RC is identical in function to the board 7273 but designed for the use in System 7001RC. For this purpose the board 7273RC additionally provides "Hot-Plug" and appropriate internal interface functionality for the operation in a **hopf** 7001RC Base System.

> The boards 7273 and 7273RC should only be operated in the suitable Base Systems.
>
> The board 7273RC only works in a System 7001RC.

> As the boards 7273 and 7273RC are identical in their most important functions, the designation **7273(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 7273(RC)
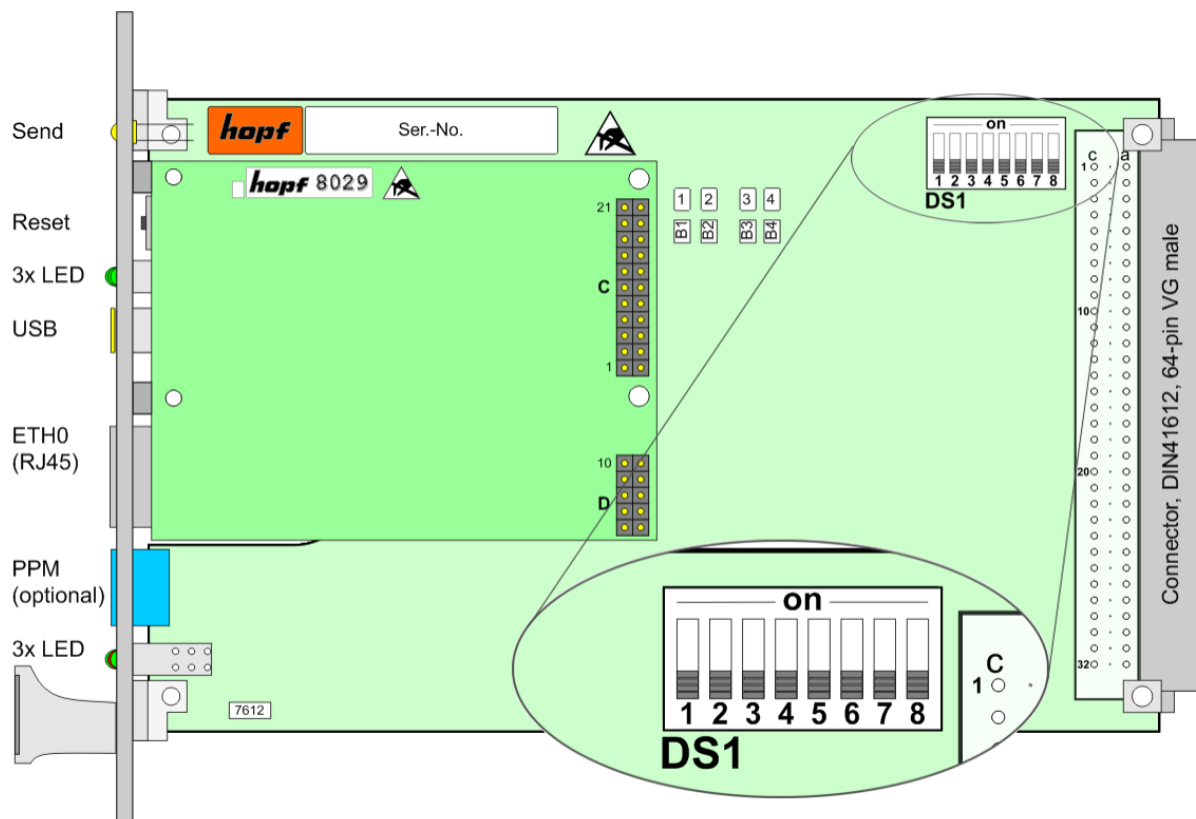


## 1.2.1 DIP Switch DS1

Depending on the type of board (7273 or 7273RC) the DIP switch DS1 is differently assigned.

### 1.2.1.1 Functions of the DIP Switch DS1 for Board 7273

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 6.3.2.5.3*) |
| 5 | Board number in System 7001 / 68xx (see *Chapter 3.3.1 + 3.4.1* ) |
| 4 | |
| 3 | |
| 2 | |
| 1 | |

### 1.2.1.2 Functions of the DIP Switch DS1 for Board 7273RC

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 7273RC 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 6.3.2.5.3***) |
| 5 | |
| 4 | Board number in System 7001RC |
| 3 | (see ***Chapter 3.5.1*** ) |
| 2 | |
| 1 | |

## 1.2.2   MAC Address for ETH0

Each LAN interface is uniquely identifiable in the Ethernet by means of a MAC address (hardware address).

The MAC address assigned for the LAN interface ETH0 can be read in the WebGUI of the appropriate board or determined by means of the ***hmc*** **Network Configuration Assisant .** A unique MAC address is assigned for each LAN interface by ***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 7273(RC) is correctly integrated into the respective System. |
| Off | Board 7273(RC) is not ready for operation. |
| On | Fault on Board 7273(RC). |

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)
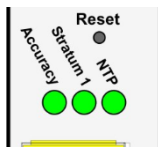
| NTP-LED (Green) | NTP Service of the Board 7273(RC) |
|---|---|
| On | **Normal case**, is started |
| Off | not started |
| **Stratum1-LED (Green)** | **NTP Service of the Board 7273(RC) works with:** |
| On | Stratum 1 |
| Flashing | Stratum 2-15 |
| Off | Stratum16 (no synchronization of NTP clients) |
| **Accuracy-LED (Green)** | **NTP Service of the Board 7273(RC) works with accuracy:** |
| On | High accuracy |
| Flashing | Medium accuracy |
| Off | Low accuracy |

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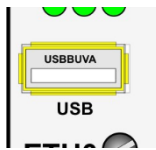
The USB connection can be used for certain problems and after consulting the *hopf* support for a System recovery.

### 1.3.1.5 RJ45 Socket (ETH0)
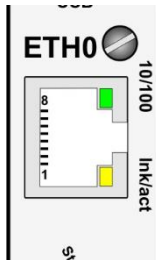
| 10/100-LED (Green) | Description |
|---|---|
| Off | 10 MBit Ethernet detected. |
| On | 100 MBit Ethernet detected. |

| Ink/act-LED (Yellow) | Description |
|---|---|
| Off | No LAN connection to a network. |
| On | LAN connection available. |
| Flashes | Network activity (transmission / reception) at ETH0. |

| Pin-Nr. | Description |
|---|---|
| 1 | Tx+ |
| 2 | Tx– |
| 3 | Rx+ |
| 4 | Not in use |
| 5 | Not in use |
| 6 | Rx– |
| 7 | Not in use |
| 8 | Not in use |
| 9 | Not in use |

### 1.3.1.6 Board Status LEDs (Operation/ERROR/Status last 24h)
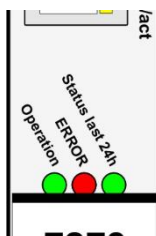
The board 7273(RC) has 3 Status LEDs indicating the function status of the board.

### 1.3.1.6.1 General Function

This describes the LED functions for the standard operation mode..
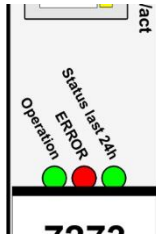
| Operation-LED (Green) | Description |
|---|---|
| On | **Normal case**, board 7273(RC) is in operation. |
| 1Hz Flashing | Board 7273(RC) boots its operation system (Duration approx. 1-1.5 minutes). |
| 3Hz Flashing | A firmware update (Image) of board 7273(RC) is processed (duration approx. 2-3 minutes). |
| Off | Board 7273(RC) **is not** ready for operation. |
| **ERROR-LED (Red)** | **Description** |
| Off | **Normal case**, board 7273(RC) is in operation |
| 1Hz Flashing | Internal System error detected (incorrect communication with the Base System). |
| 5Hz Flashing | Fail-safe basic parameterization is not available (emergency operation) |
| On | The primary CPU on board 7273(RC) shows no activity. |
| **Status last 24h-LED (Green)** | **Description** |
| Off | The NTP services of board 7273(RC) works less than 1 hour with Stratum 1 or / and accuracy = high |
| 1Hz Flashing | The NTP services of board 7273(RC) continuously works equal or greater to the value of 1 hour with Stratum 1 and accuracy = HIGH (optimum operation condition) |
| On | The NTP services of board 7273(RC) continuously works more than 24 hours with Stratum 1 and accuracy = HIGH (optimum operation condition) |

### 1.3.1.6.1 Function by Pressing the Reset Button
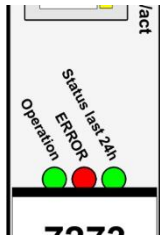
The duration of pressing the Reset button in the front panel of the board can be read by the behaviour of all 3 Status LEDs.
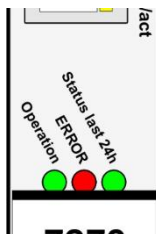
| All 3 LED (Operation-LED, ERROR-LED and Status last 24h-LED) | Description of Special Function |
|---|---|
| LED Basis Function | Keypress: 0-1 second |
| 2Hz Flashing | Keypress: 1-10 seconds |
| 5Hz Flashing | Keypress: >10 seconds |

### 1.3.1.6.2  Special Function for Update and Hardware Problems

A malfunction of the onboard µController (update/defect) can be recognized by the behaviour of the 3 Status LEDs.

| All 3 LED (Operation-LED, ERROR-LED and Status last 24h-LED) | Description of Special Function |
|---|---|
| 0,5Hz Flashing | Firmware update of µController is active or the µController is defective |

### 1.3.1.7  Option: Active 12V DC PPM (Minute Pulse)

For output of an active minute pulse (PPM) the board 7273(RC) is optionally available with an additional 3 pole pluggable screw terminal (FG7273/PPM). An upgrade of this option by the customer is not possible.

Version 7273(RC) für 3HE Systeme          Version 7273 DIN-Rail
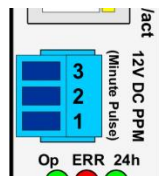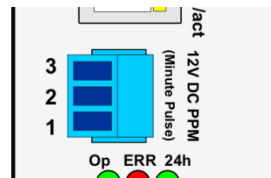
| Pin No. | Assignment |
|---|---|
| 1 | Defined duration of minute pulse (isolated, reference potential GND1) |
| 2 | +12V DC (isolated, reference potential GND1) |
| 3 | GND1 (isolated for minute pulse / +12V DC) |

## 1.3.2 Front Panel of Boards 7273 and 7273RC for 3U / 19" Racks

**Board 7273**
**3U/4HP**
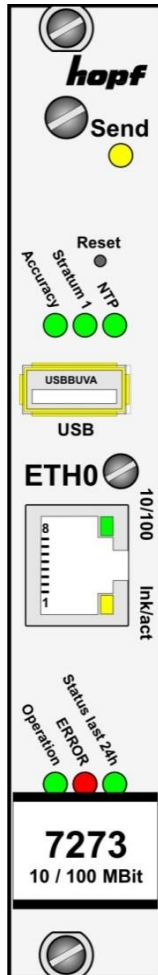
**Board 7273**
**3U/4HP**
with Option
**FG7273/PPM**
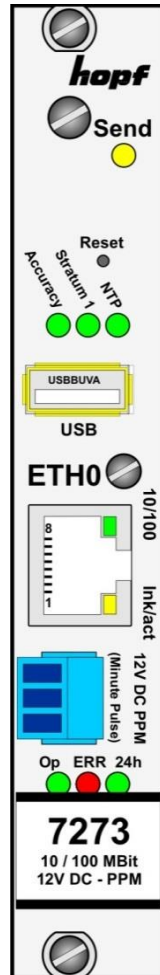
**Board 7273RC**
**3U/4HP**
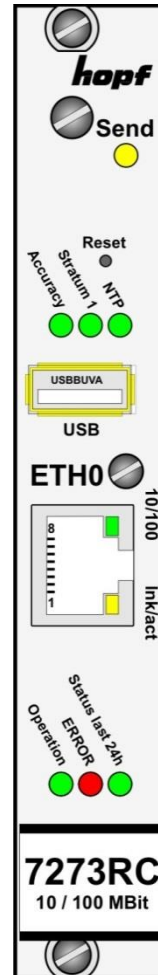
**Board 7273RC**
**3U/4HP**
with Option
**FG7273/PPM**
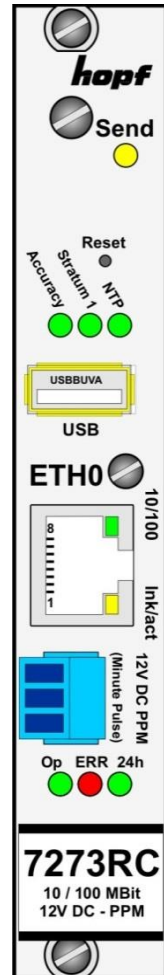
Optionally the board 7273(RC) is assembled with a 3 pole pluggable screw terminal for output of a minute pulse (PPM).

Parameterization see **Chapter 6.3.5.9 Option FG7273/PPM: Minute Pulse Length (PPM)**

## 1.3.3   Front Panel of Board 7273 for 1U / 19" Racks (Slim Line)

**Board 7273/1U**
**1U (Slim Line)**
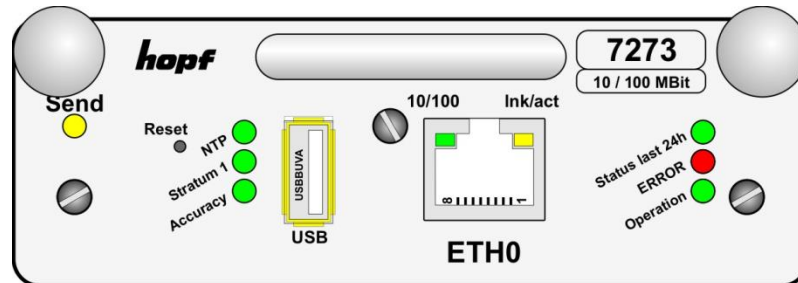


**Board 7273/1U**
**1U (Slim Line)**

with Option
**FG7273/PPM**
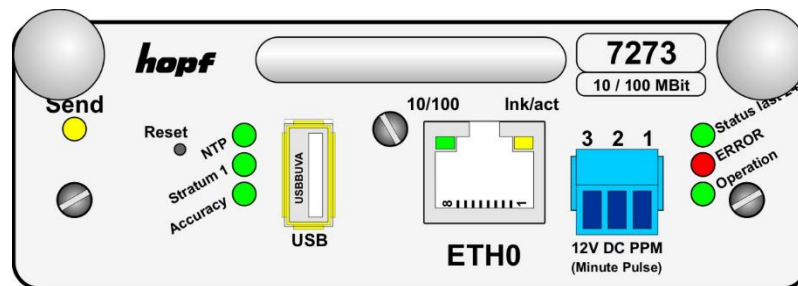


Optionally the board 7273(RC) is assembled with a 3 pole pluggable screw terminal for output of a minute pulse (PPM).

Parameterization see *Chapter 6.3.5.9 Option FG7273/PPM: Minute Pulse Length (PPM)*

## 1.3.4 Front Panel of Board 7273 for DIN Rail Mounting
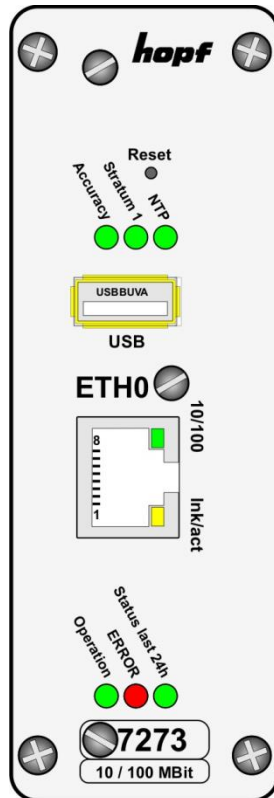
**Board 7273DIN-Rail**  |  **Board 7273DIN-Rail**
with Option
**FG7273/PPM**
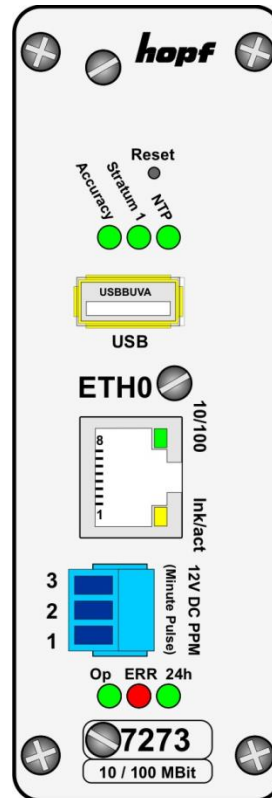


> ⚠ The board 7273DIN-Rail is non-modular pluggable. A replacement of board can only be done in the factory at company **hopf**.

Optionally the board 7273(RC) is assembled with a 3 pole pluggable screw terminal for output of a minute pulse (PPM).

Parameterization see **Chapter 6.3.5.9 Option FG7273/PPM: Minute Pulse Length (PPM)**

# 2 System Behaviour of the Board 7273(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.

The boot process is indicated via the Status LEDs on the front panel and lasts approx. 1-1.5 minutes.

## 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 7273(RC) can be reset or set to the factory default status by a reset button behind the front panel of the board. The reset button is accessible with a thin objective through the small drilling in the front panel.

| Reset Button | Function |
|---|---|
| Keypress: 0-1 second | None |
| Keypress: 1-10 secons | Board reset is initiated after releasing |
| Keypress: >10 seconds | The board is set to factory default values after releasing |

LED behaviour see *chapter 1.3.1.6.2 Special Function for Update and Hardware Problems*

### 2.3.1 Board Reset

A short pressing of the Factory-Default-Button (between 1 and 10 seconds) a reset is initiated on board 7273(RC).

> **i** For the duration of pushing the reset button between 1-10 seconds the 3 status LEDs on the board (Operation/ERROR/Status last 24h) are all rhythmically flashing in a **2Hz** cycle.

Release of a Board Reset:

1. Press reset button until the 3 board LEDs rhythmically flashing in **2Hz** cycle.
2. Maximum 5 seconds after release of the reset button a board reset is performed.
3. The operation LED flashes in 1Hz cycle ⇨ Upload of the operation system of board 7273(RC) (the board is not yet operational).
4. The standard operation condition is reached again after approx. 1-1.5 minutes. This is shown by the following behaviour of the 3 Status LEDs:
   - Operation LED is on
   - NTP LED is on
   - Send LED flashes (not applicable for DIN Rail)

> **!** After a reset board 7273(RC) in only accessible again via LAN after booting.

### 2.3.2 Set Board to Factory-Default-State (incl. LAN Parameter)

If the board is not accessible in the Ethernet after an invalid configuration (e.g. via the Ethernet), the board 7273(RC) can be set to factory default status by pressing the reset button for more than 10 seconds.

> **i** When pressing the reset button for more than 10 seconds the 3 LEDs on the board (Operation/ERROR/Status last 24h) are all rhythmically flashing in **5Hz** cycle.

> **i** List of the Factory-Default Parameters see *Chapter 9 Factory Defaults of Board 7273(RC)*

Pressing the reset button for more than 10 seconds the LAN parameters saved in the board are deleted and the board is set to DHCP mode:

- IP          000.000.000.000
- Gateway   000.000.000.000
- Net Mask  000.000.000.000

> **!** All parameters modified via the reset button are **not** updated depending on the Base System and thus not correctly indicated in the menu of the Base System after default.
> After the default the LAN parameters of the board 7272(RC) have to be completely configured and entered via the Base System.

Set board 7273(RC) to the Default Status

1. Pressing the reset button for more than 10 seconds this is indicated 3 board LEDs rhythmically flashing in **5Hz cycle** (>10 seconds)

2. Maximum 5 seconds after release of the reset button the board is set to default values.

3. Board 7273(RC) automatically initiates a board reset.

4. Reset desired LAN parameters for ETH0 (IP-address, gateway and net mask) via the Base System or via *hmc* **Network Configuration Assistant.**

5. All configurations in WebGUI should be checked and may need to be reset.

## 2.4    Firmware Update

The board 7273(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.

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 7273(RC) in cases of doubt.

The general process of a complete software update of the board 7273(RC) is described below:

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

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

3. Select the file with the file extension **.mot** via the selection window.

4. The selected file is shown in the selection window.

5. The update process is started wit the button **Upload now**.

6. In WebGUI the successful file transfer to the board is indicated.

7. Now the update of the board automatically starts after a few seconds.

8. The update is indicated on the board by the 3 Status Board LEDs
   (the LEDs are rhythmically flashing in **<u>0,5Hz</u>** cycle).

9. After successful update the board automatically performs a reboot.

10. After approx. 2 minutes the first part of the update process is finished and the board via WebGUI accessible.

11. Again log in as Master in WebGUI of the board.

12. Select in the directory **Device** the menu item **Image Update**.

13. Select the file with the file extension **.img** via the selection window.

14. The selected file is shown in the selection window.

15. Start of the update process with the button **Upload now**.

16. In WebGUI the successful file transfer and writing in the board is indicated.

17. During the update process the status LED Operation on the board is rhythmically flashing in **3Hz** cycle.

18. In WebGUI the successful update is indicated after 2-3 minutes with the request to release a reboot of the board.

19. After the successful activation and processing of the reboot of the board the entire update process is finished.

## 2.5   Board ERROR

In case the board 7273(RC) does not behave as specified, the board LED should be checked with regard to errors (see ***Chapter 1.3.1.6 Board Status LEDs (Operation/ERROR/Status last 24h)***)

# 3 Implementing Board 7273(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 7273 **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 7273 und 7273RC 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 7273(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 7273 and 7273RC (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 7273(RC) via DIP switch bank (**DS1**).

## 3.3 *hopf* Base Systems 6844, 6844RC, and 6855 – Only Board 7273

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 7273 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 7271 and board 7273) 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 7273

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 7273 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 7271 and board 7273) 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 7273RC

### 3.5.1  Setting the Board Number for Base 7001RC

A maximum number of 31 LAN boards (also different types – e.g. board 7271RC and board 7273RC) 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 7273RC 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 7273(RC) is supplied with the setting DHCP-Mode (this matches with the factory-default setting).

> **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 LAN interface of the board 7273(RC), the board can be searched for in the network via the ***hmc*** (***hopf* Management Console)**. Afterwards the base LAN parameter (IP address, netmask and gateway) 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 SUB Net**.

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:

| | |
|---|---|
| 727300 | - Board 7273 1U and 3U |
| 727300DIN | - Board 7273DIN-Rail |
| 7273RC00 | - Board 7273RC |

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 7273(RC) via a browser the following base parameters are mandatory:

- **Host Name** ⇨ e.g. hopf7273
- **Network Configuration Type** ⇨ **Static IP Address**
- **IP Address** ⇨ e.g. 192.168.232.1
- **Netmask** ⇨ e.g. 255.255.224.0
- **Gateway** ⇨ e.g. 192.168.224.1

| ! | The **hostname must** meet the following conditions:<br><br>• The hostname may only contain the characters 'A'-'Z', '0'-'9', '-' and '.'. There should be no distinction between upper-and lower-case letters.<br>• The character '.' may only appear as a separator between labels in domain names.<br>• 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 7273(RC) via Button ` Apply `. Afterwards the entry of the **Device Password** is requested:



Device Password <**device**> is set for LAN boards 7273(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 7273(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 7273(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 7273 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 7273 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:

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

or

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

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

```
L A N   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:

```
  A N   1   > 1 9 2 . 1 6 8 .
          0 1 7 . 0 0 1 <
```

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 $\boxed{\text{Y}}$ 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 $\boxed{\text{ENT}}$ 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 7273 only)

The input and display functions are called up by means of the menu header **BOARDS:3** under **BOARD 7270 / 7271 / 7272 / 7273**.

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 7273 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.

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

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 ⎡ **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 7273RC 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 ⎡ **ENT** ⎤. Only the complete check of **all single** menu points allow the adoption of all changes and their transfer to the board 7273RC.

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

with ⎡ **ENT** ⎤ key    ⇨ Main menu
with ⎡ **4** ⎤ key     ⇨ Board setup
with ⎡ **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 ⎡ **Y** ⎤

Search for board to be parameterized with key ⎡ **N** ⎤ and select with key ⎡ **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

**7273 NO.: 01**   ⇨ board type **7273RC** 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 <u>265</u>), 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*.

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

### 5.3.3 Entry the Network Mask

The network mask can be entered via the selection screen:

```
B . 7 2 7 3   N O . : 0 1   N E T M A S K   > 2 5 5 . 2 5 5 . 0 0 0 . 0 0 0 <
                            N E W   N E T M A S K   > ~ ~ ~ . ~ ~ ~ . ~ ~ ~ . ~ ~ ~ <
```

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 . 7 2 7 3   N R . : 0 1   C O N T R O L - B Y T E   0 0 0 0 0 0 1 0
                            N E W   C O N T R O L - B Y T E   > ~ ~ ~ ~ ~ ~ ~ ~ <
```

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:

```
C O N T R O L - B Y T E   > 7 6 5 4 3 2 1 0 <
```

### 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.7273 NO.:01    OLD: BYTE 01 >0000000<
BYTE = BIT 7..0 NEW: BYTE 01 >~~~~~~~<
```

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:

```
BYTE 01 >76543210<
```

| 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.7273 NO.:01    OLD: BYTE 02 >0000000<
BYTE = BIT 7..0 NEW: BYTE 02 >~~~~~~~<
```

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:

```
BYTE 02 >76543210<
```

| 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.

> ℹ️ The WebGUI has been tested with the following browsers: MOZILLA 1.x, Netscape 7.x and IE 6.x – some functions do not run on older versions.

## 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 7273(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 7273(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
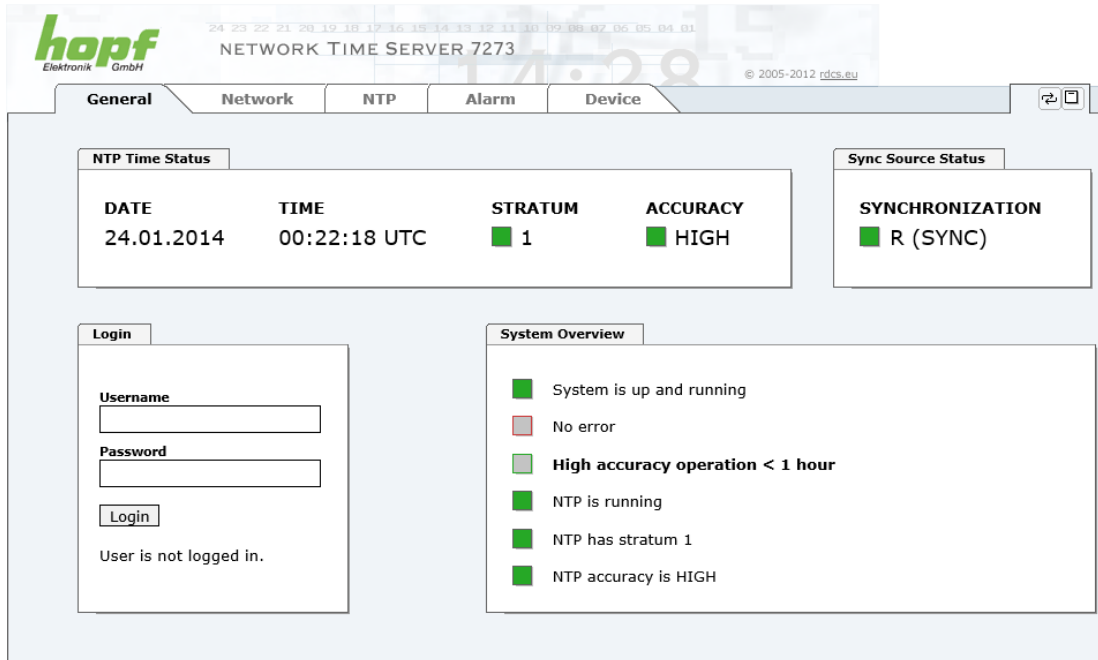
> ⚠️ The following detailed explanatory information should be read if anything is unclear while executing the configuration steps.

## 6.2    General – Introduction

Board 7273(RC) should be accessible to a web browser if it has been set up correctly. Enter the IP 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.

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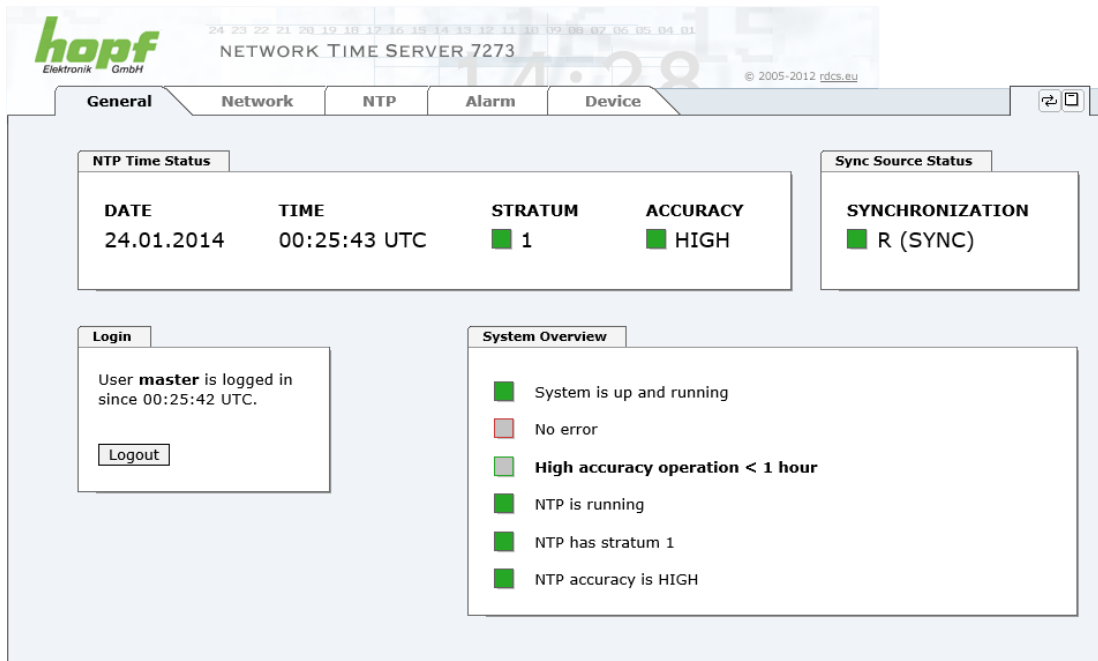
| | |
|---|---|
| **i** | Differentiation is made between **upper and lower case** characters in the password. Alphanumeric characters and the following symbols can be used: **[ ] ( ) * - _ ! $ % & / = ?** |

| | |
|---|---|
| **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. 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 7273(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
- 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.
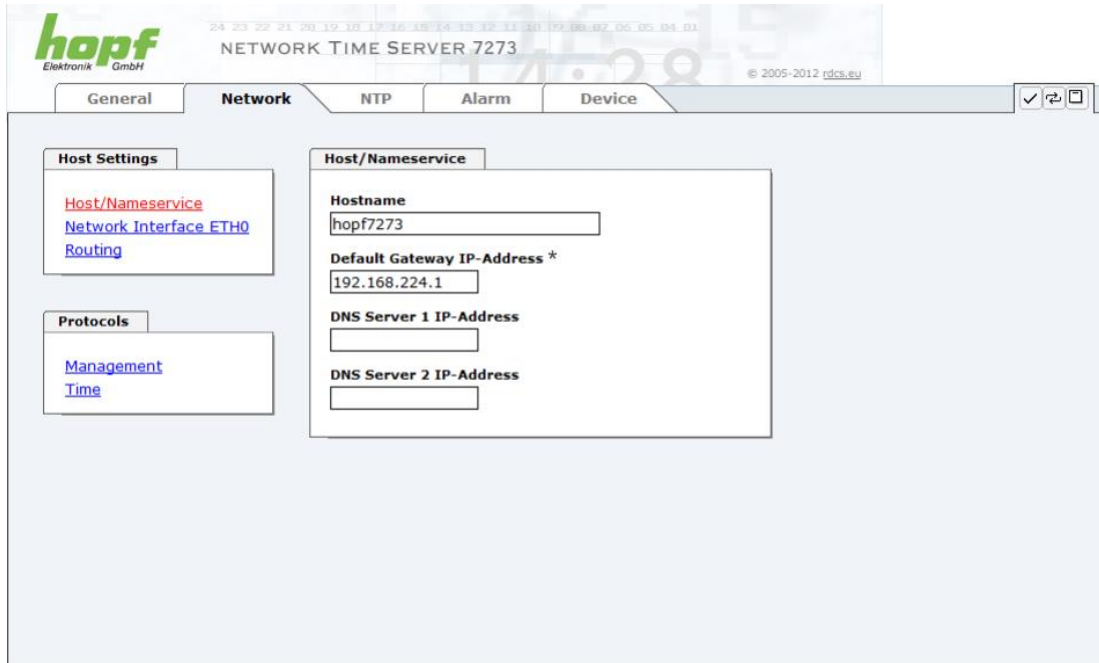
 JavaScript should be enabled in the browser in order to guarantee the correct operation of the web interface.
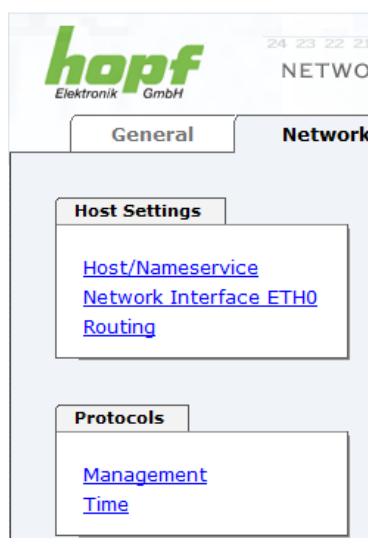
 All the links within the tabs on the left hand side lead to corresponding detailed setting options.

## 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**
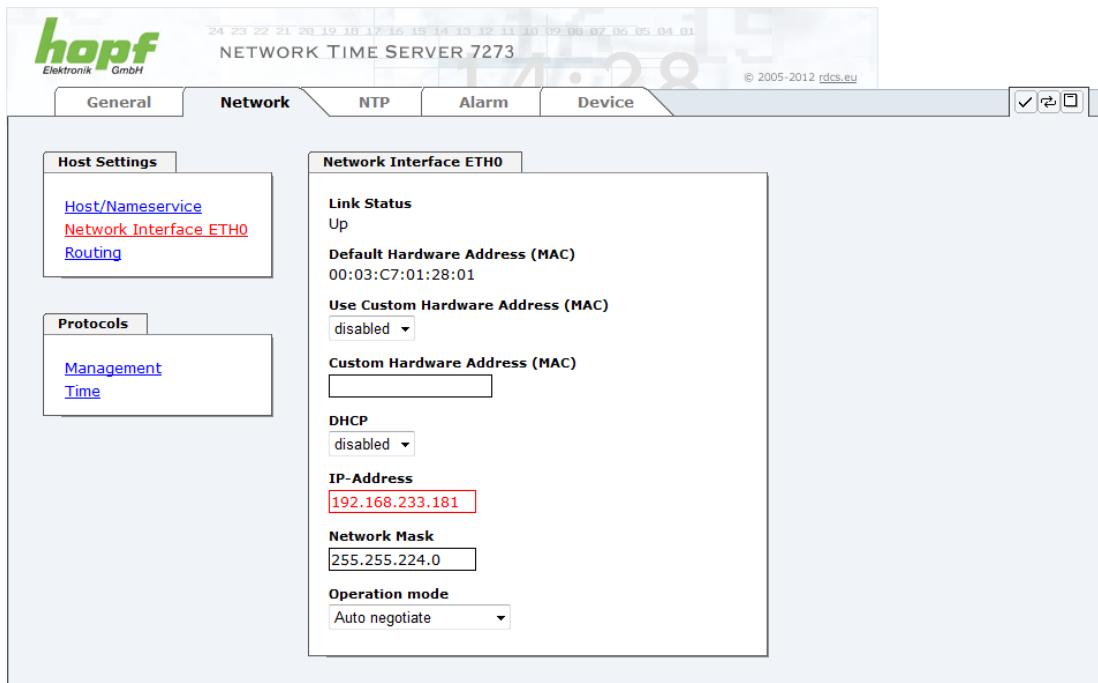
Modifications of the network parameters (e.g. IP address) are immediately effective clicking on **Apply** to confirm.
However, the modifications are not permanently saved yet. This requires to access the WebGUI with the new network parameters again and to save the data with **Save** permanently.

---

**!** 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.

---

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

## 6.3 Description of the Tabs

The WebGUI is divided into the following tabs:

- General
- Network
- NTP
- Alarm
- Device

### 6.3.1 GENERAL Tab

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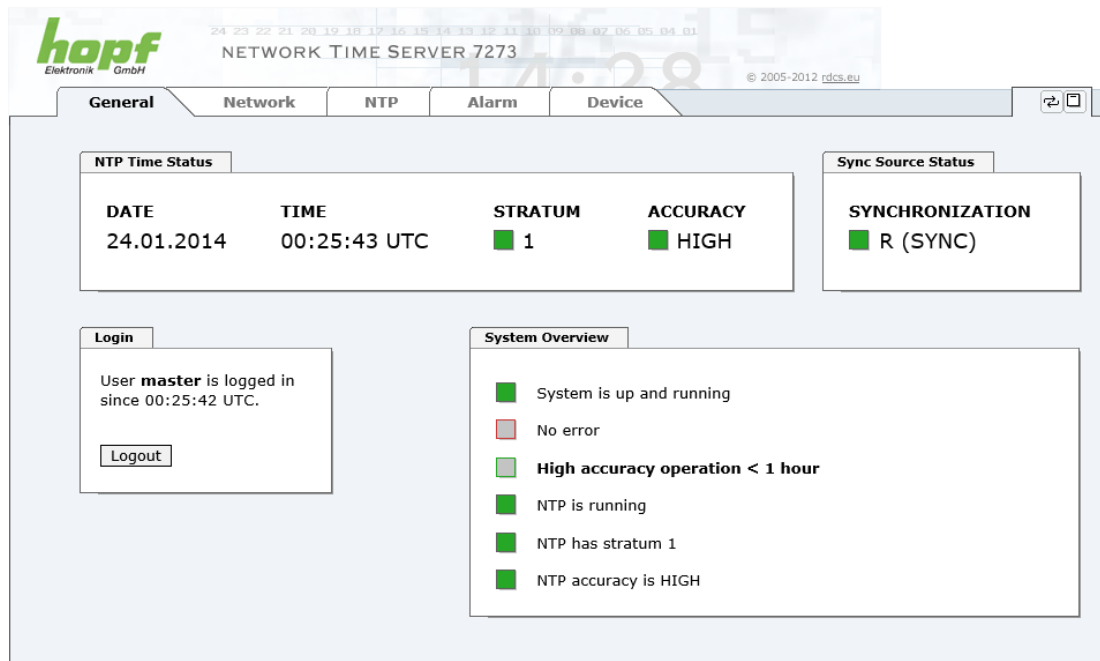


#### NTP Time Status

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 7273(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*.

#### Clock Status

Display of the actual status of synchronisation of *hopf* Base systems with this possible values:
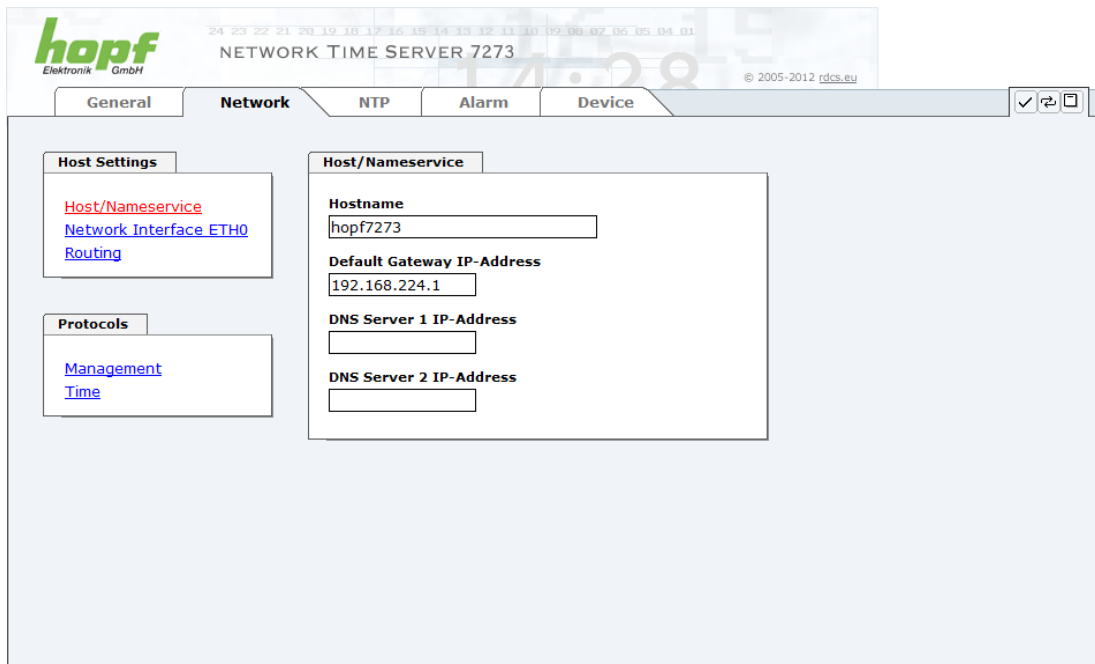
| | |
|---|---|
| **invalid** | Invalid time |
| **C** | The system is in crystal mode (C = Crystal) |
| **r** | The system is synchronous to the synchronization source |
| **R** | The system is synchronous to the synchronization source and the crystal generator will be regulated (**optimum operating condition**) |

#### Login

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

## 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 "**hopf7273**". 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.<br>• The character '.' may only appear as a separator between labels in domain names.<br>• 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 Default Gateway

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. |
|---|---|
| ℹ | 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. |

Contact your network administrator for details of the standard gateway if not known. If no standard gateway is available (special case), enter 0.0.0.0 in the input field or leave the field blank.
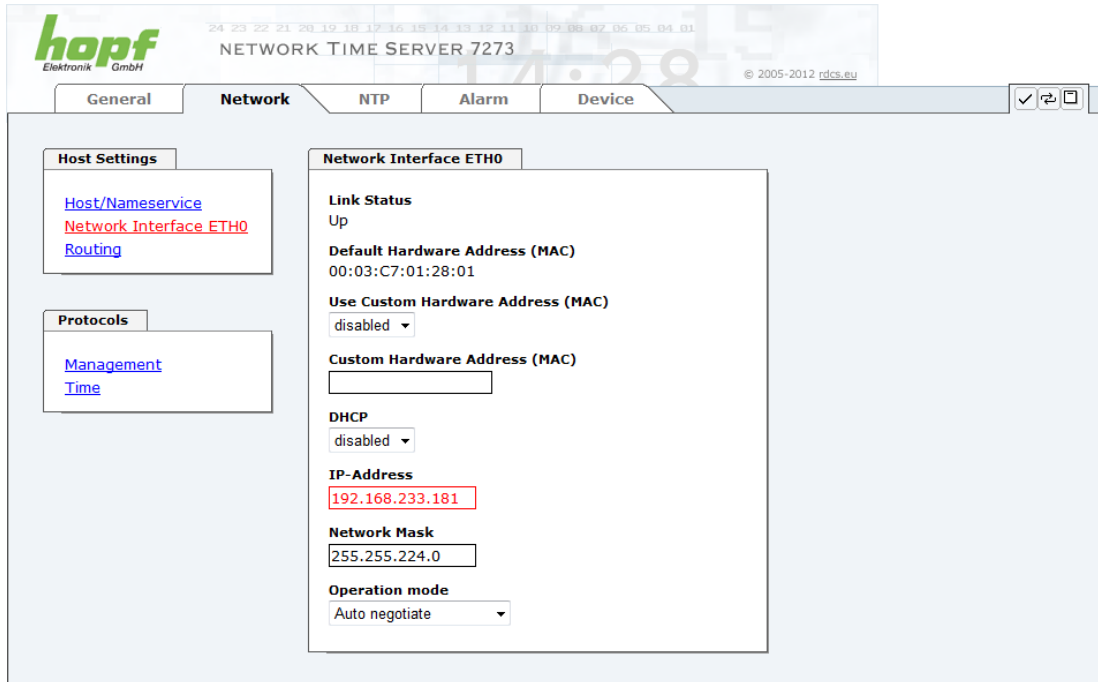
#### 6.3.2.1.3 DNS Server 1 & 2

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

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

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

### 6.3.2.2 Network Interface ETH0

Configuration of the Ethernet interface ETH0 of the board 7273(RC)



### 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 MAC Address for ETH0*** for board 7273(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.

To use the 'customers MAC address function' you have to activate it by setting the function '**Use Custom Hardware Address (MAC)**'.

You have to enter the customers MAC address is hexadecimal form with a colon to separate (e.g. **00:03:c7:55:55:02**).

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

> **!** There are no MAC multicast addresses allowed!

### 6.3.2.2.3  DHCP

If DHCP is to be used, 0.0.0.0 should be entered as the IP 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  IP Address

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

> **i** 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.
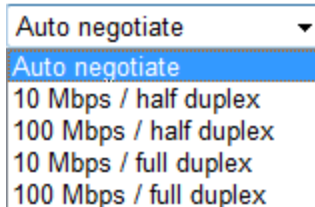>
> Values modified via LAN are not automatically updated in the Base System and thus are no longer correctly displayed after the modification. For this reason it is recommended to configure the IP address via the Base System. For the respective behaviour of the Base System the appropriate manual should be considered.

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

### 6.3.2.2.5  Network Mask

The 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 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 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.
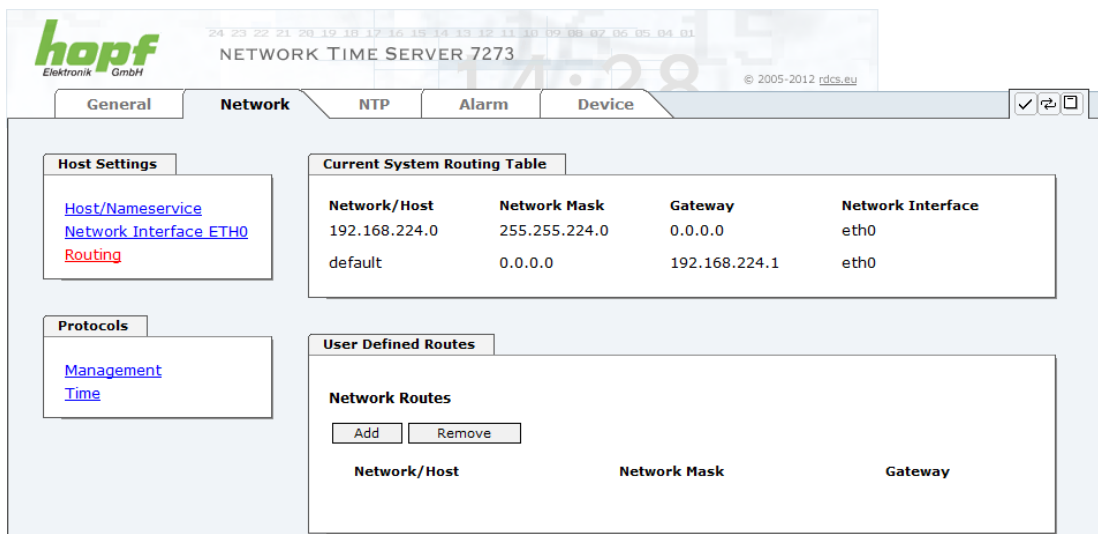
**Operation mode**

| Auto negotiate ▼ |
| --- |
| Auto negotiate |
| 10 Mbps / half duplex |
| 100 Mbps / half duplex |
| 10 Mbps / full duplex |
| 100 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 7273(RC) **and** the connected network components manually to the same value.

## 6.3.2.3 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!

### 6.3.2.4 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.
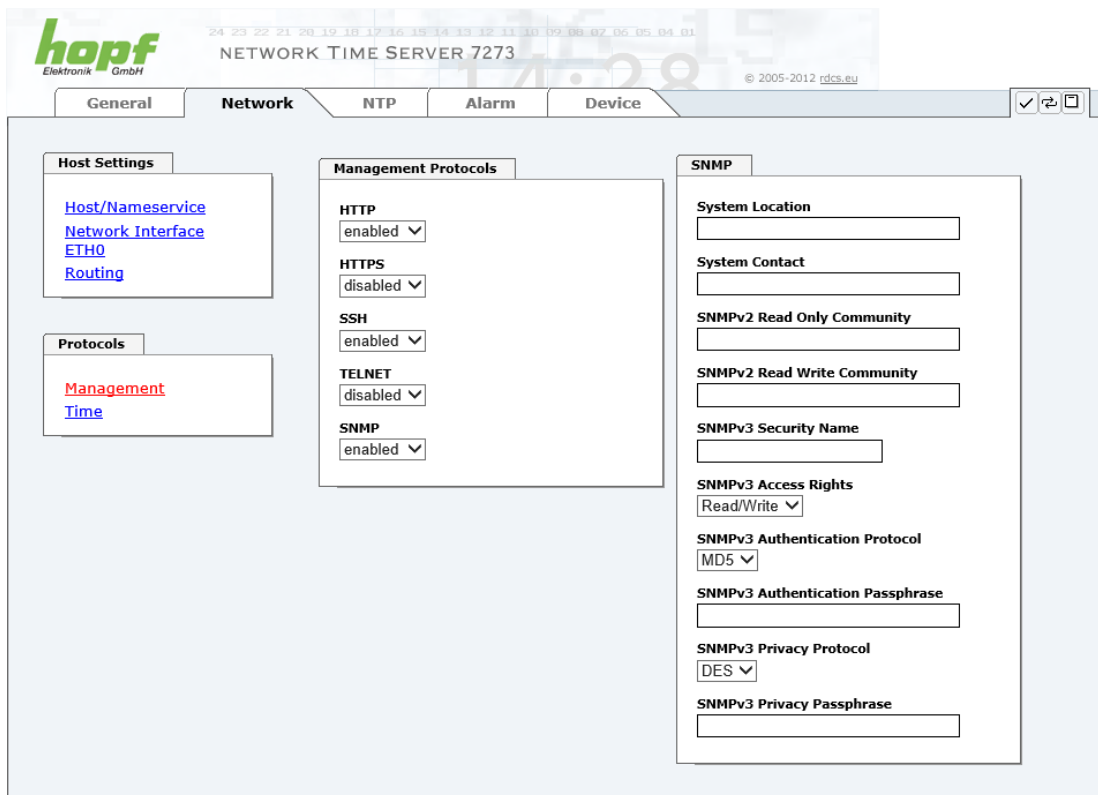
Changes to the availability for a protocol (enable/disable) take effect immediately.

> ⚠ 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!

### 6.3.2.4.1  SNMPv2 / SNMPv3

Both protocols SNMPv2 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 (SNMPv2 / SNMPv3).

In order to disable SNMPv2 both fields **SNMP Read Only Community** and **SNMP Read Write Community** must remain empty.

| SNMPv2 | SNMPv2 enabled | SNMPv2 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 SNMPv2 |
| 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:
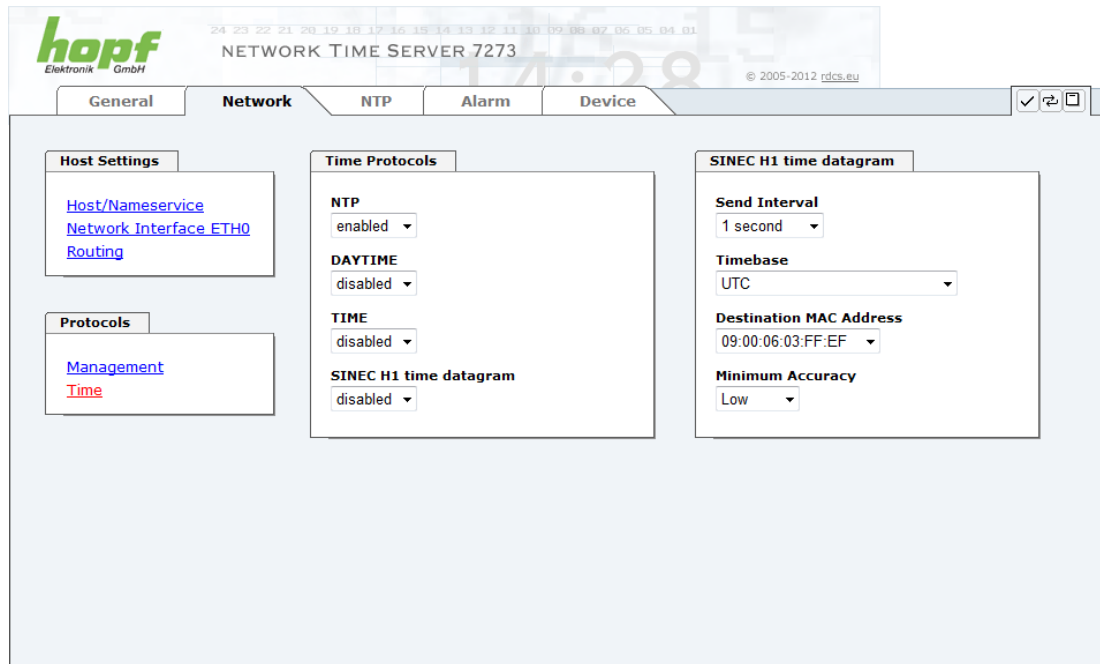
| SNMPv3 | noAuthNoPriv | authNoPriv | authPriv |
|---|---|---|---|
| Authentication Passphrase: | empty | set | set |
| Privacy Passphrase: | empty | empty | set |

> ⚠ Right now only one user is supported.

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

## 6.3.2.5 Time

Activation and configuration of different time protocols



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

### 6.3.2.5.1 Time Protocols – NTP, SNTP etc.

Needed time protocols can be activated here.

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

### 6.3.2.5.2 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.

### 6.3.2.5.3 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)<br>e.g.  transmission point (UTC, absolute):  with time information:<br>12:33:**00**,001                               12:33:**00**,000 |
| on | **ONE second delayed**<br>z.B.  transmission point (UTC, absolute):  with time information:<br>12:33:**01**,002                               12:33:**00**,000 |

## 6.3.3 NTP Tab

This tab shows information and adjustment possibilities of the NTP services of the Board 7273(RC). The NTP service is the significant main service of the Board 7273(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 6.3.2.5 Time*)

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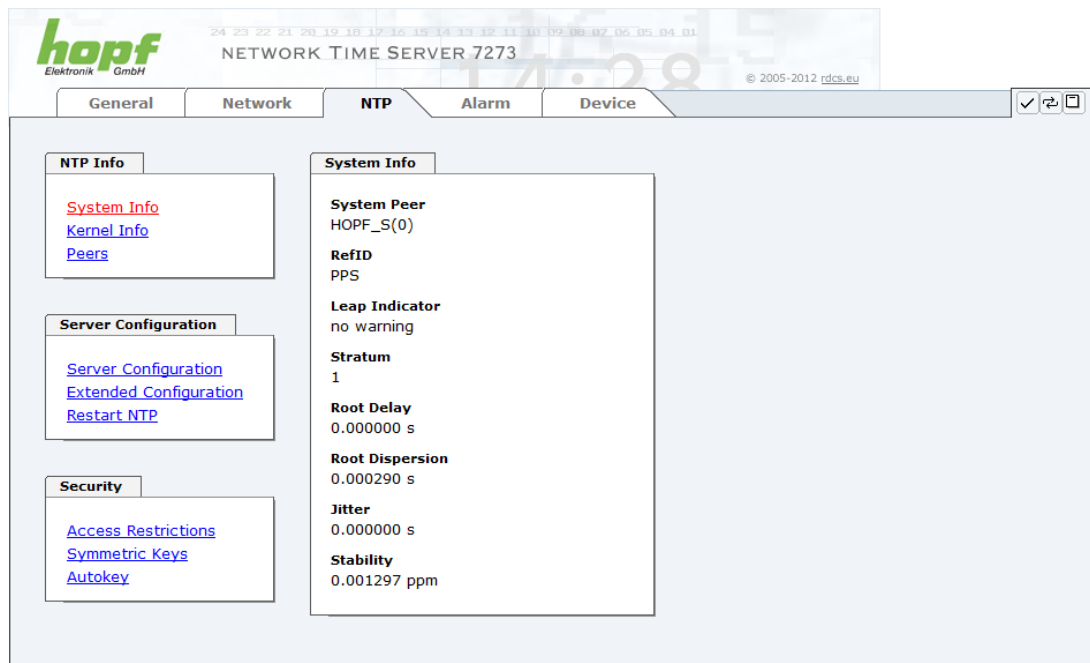
> ℹ Via the NTP protocol SNTP Clients can also be synchronized. In contrast to NTP in SNTP Clients delay times are not evaluated on the network. For this reason the accuracy reached in SNTP Clients is lower than in NTP Clients.

## 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 7273(RC) are indicated. In addition to the NTP calculated values for root delay, root dispersion, jitter, and stability the stratum value of the Board 7273(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 7273(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.
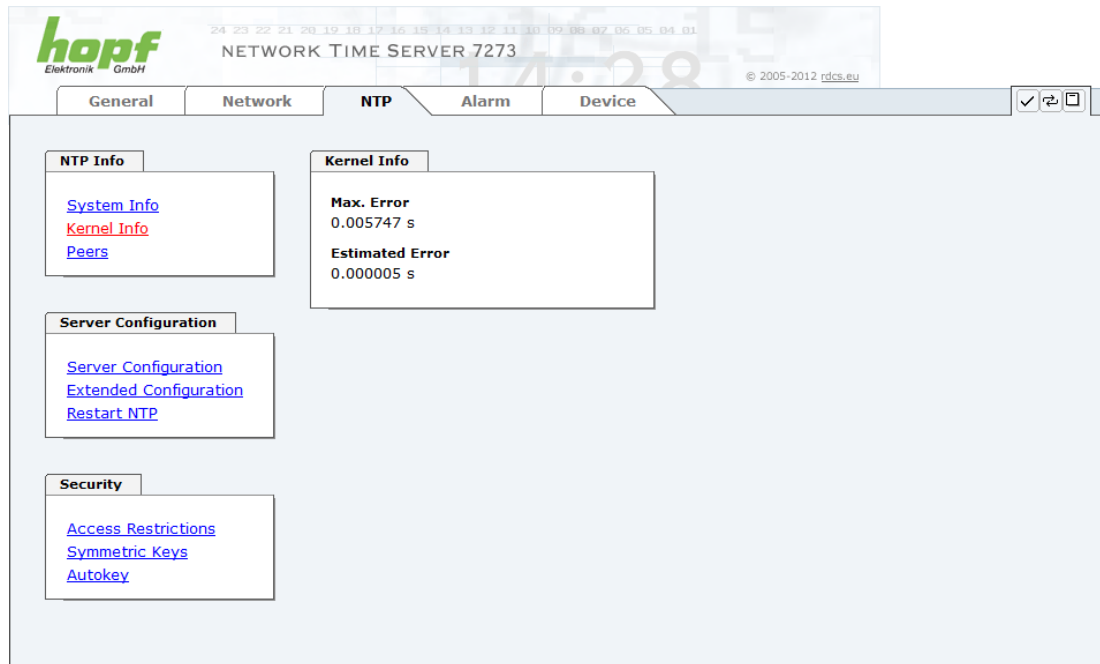


This screenshot shows a maximum kernel clock error of 5.747 msec (milliseconds). The estimated error value is 5µs (microseconds).

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.
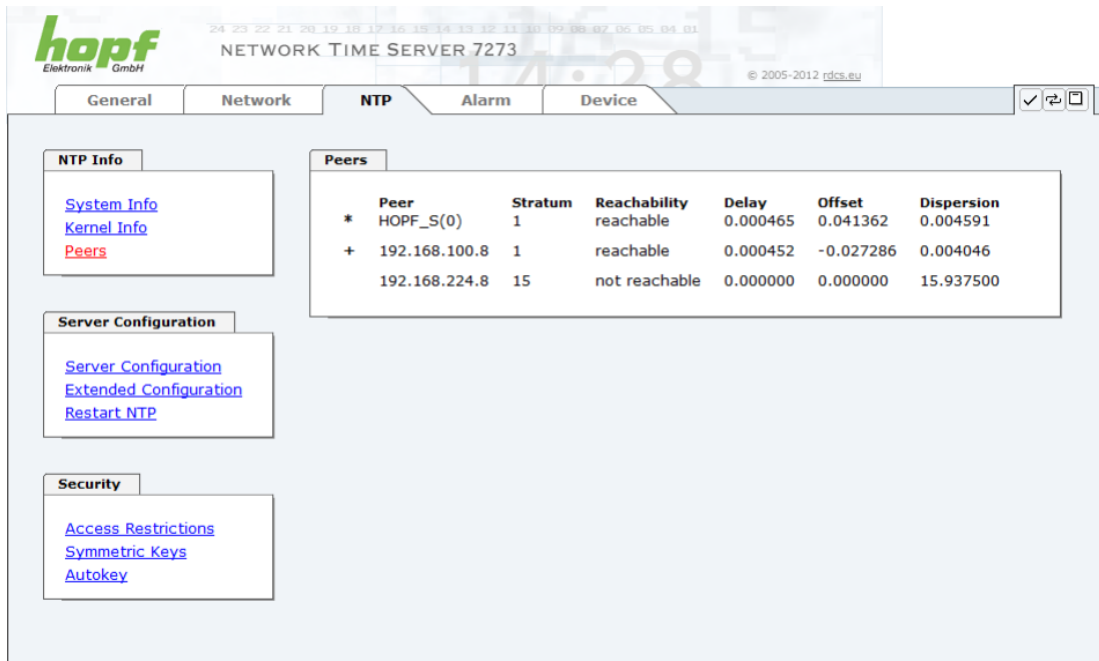
### 6.3.3.3 Peers

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).



Three lines can be seen in the above image. The first line is displays the **hopf - refclock ntp driver**, which gets its time information directly from the **hopf** Base System.
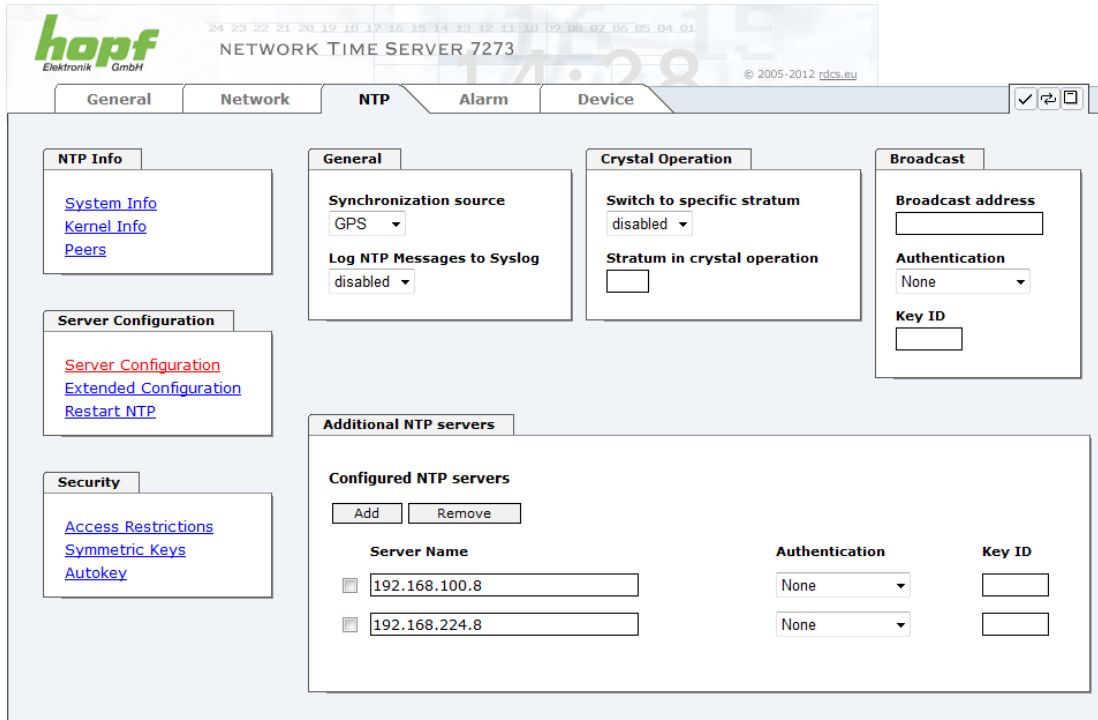
The second and third line display external NTP server that can be additionally added to the internal **hopf – refclock ntp driver** in the menu server configuration.

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 6.3.4.1 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 7273(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 7273(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 7273(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.

> ⚠ 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*.

> ⚠ 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.
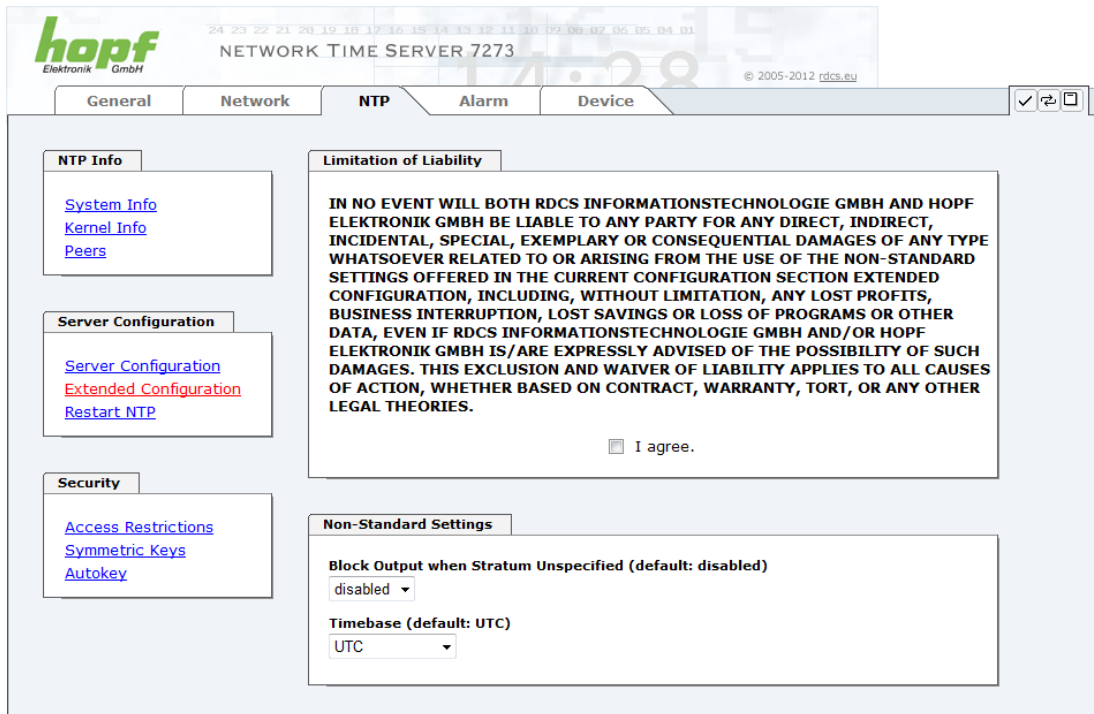
### 6.3.3.4.6 Additional NTP SERVERS

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 7273(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 7273(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 7273(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 7273.
>
> - 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 **without** 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

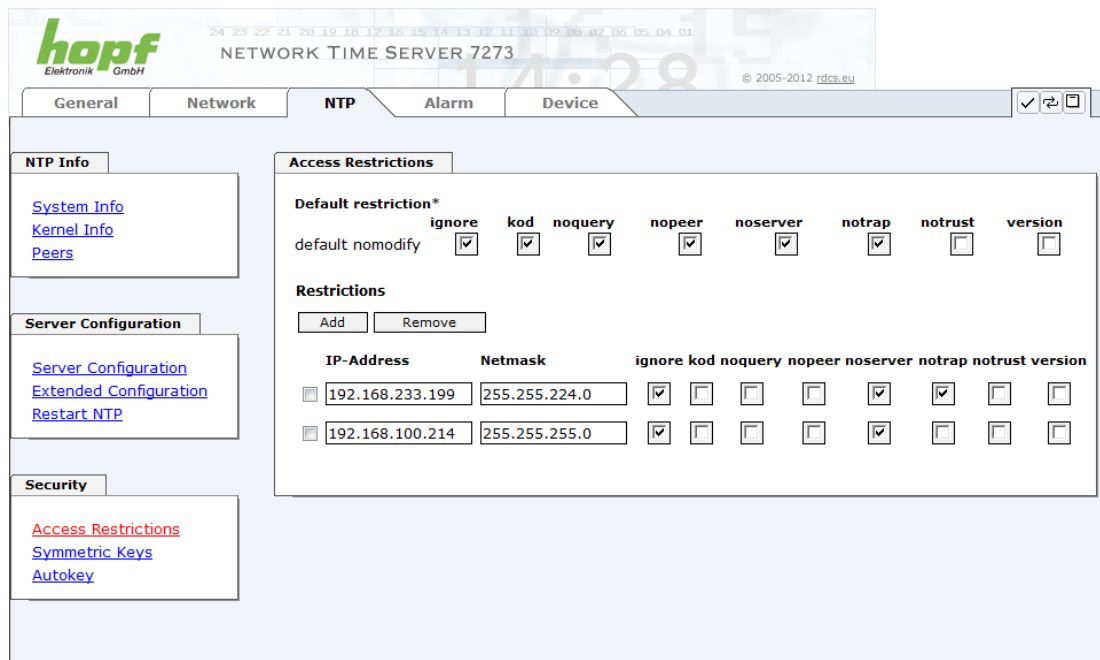The following screen appears after clicking on the Restart NTP option:



Restarting NTP Services is the only possibility of making NTP changes effective without having to restart the entire Board 7273(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 7273(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!

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.<br>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:<br><br>**ignore in the default restrictions**    ☑<br><br>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:<br>See *Chapter 6.3.3.7.6 Access Control Options*<br><br>**kod**<br><br>**notrap**<br><br>**nopeer**<br><br>**noquery**. | ☑<br><br>☑<br><br>☑<br><br>☑ |
| **Yes** | In this case select from the following standard restrictions:<br>See *Chapter 6.3.3.7.6 Access Control Options*:<br><br>**kod**<br><br>**notrap**<br><br>**nopeer**<br><br>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 .* | ☑<br><br>☑<br><br>☑ |

### 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.*<br><br>**kod**<br><br>**notrap**<br><br>**nopeer** | ☑<br><br>☑<br><br>☑ |

## 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.



 Unrestricted access of Board 7273(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* ).

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

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

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

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

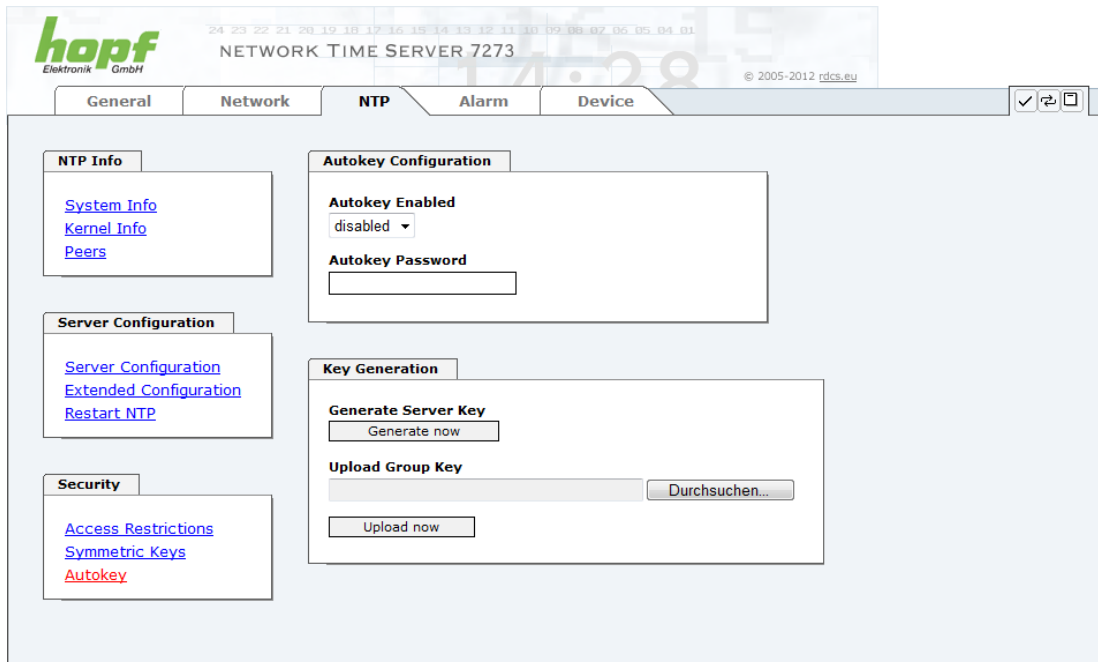### 6.3.3.8.4 How does authentication work?

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 NTS board 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   ALARM Tab

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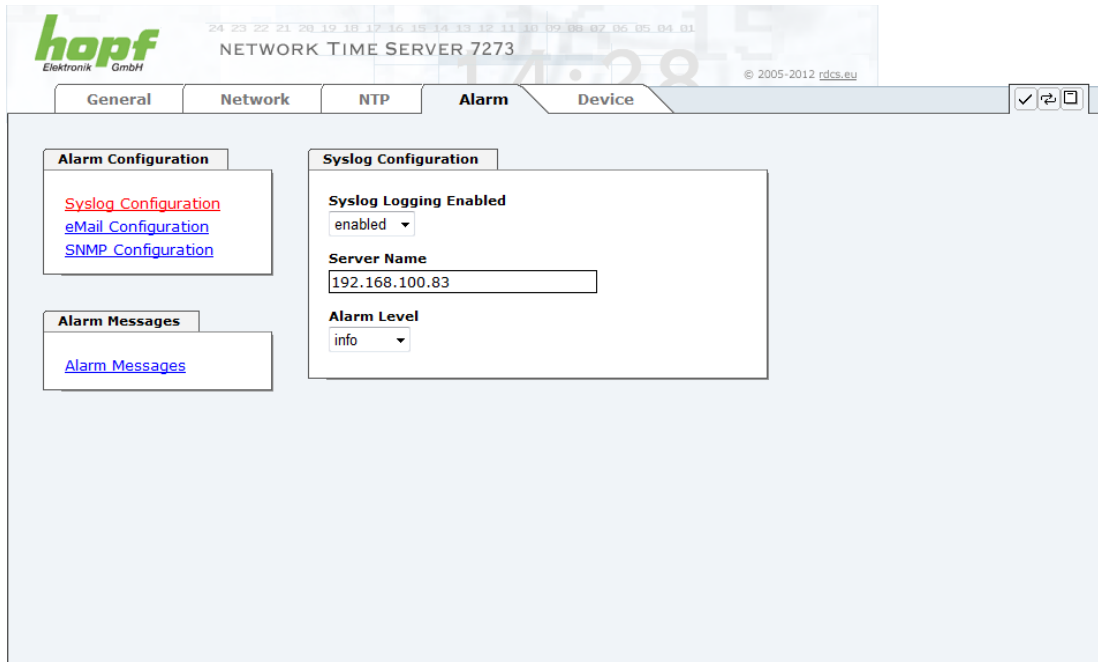
### 6.3.4.1  Syslog Configuration

It is necessary to enter the name or IP 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!
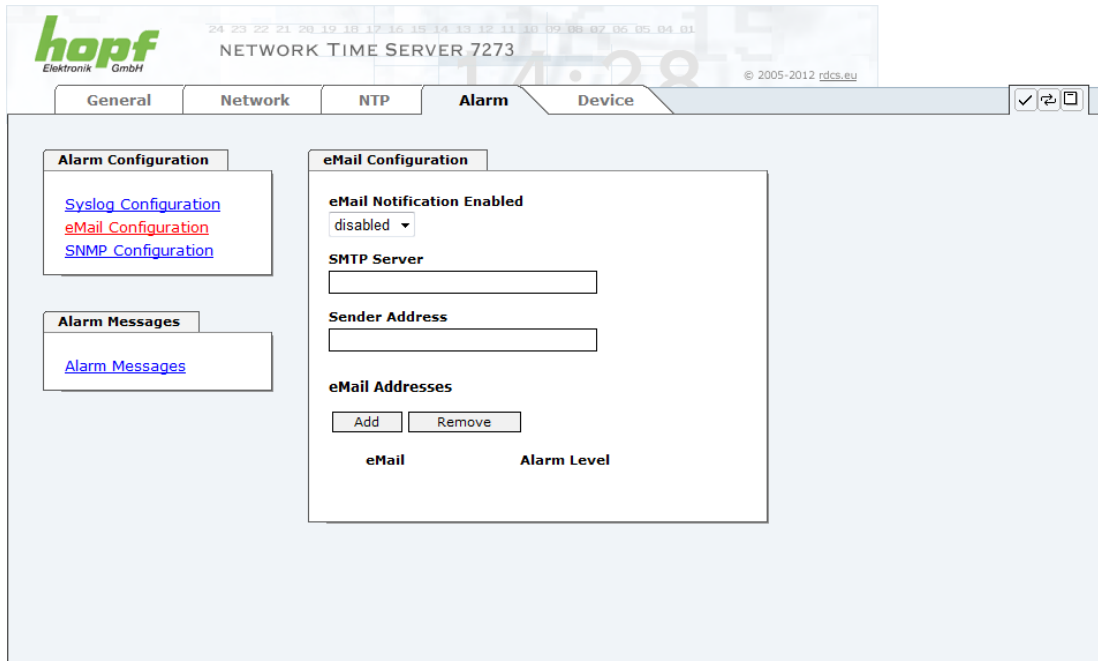


The alarm level designates the priority level of the messages to be transmitted and the level from which transmission is to take place (see **Chapter 6.3.4.4 Alarm** ).

| 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 7273(RC) are described in **Chapter 10.5 Syslog Messages**.

## 6.3.4.2 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.
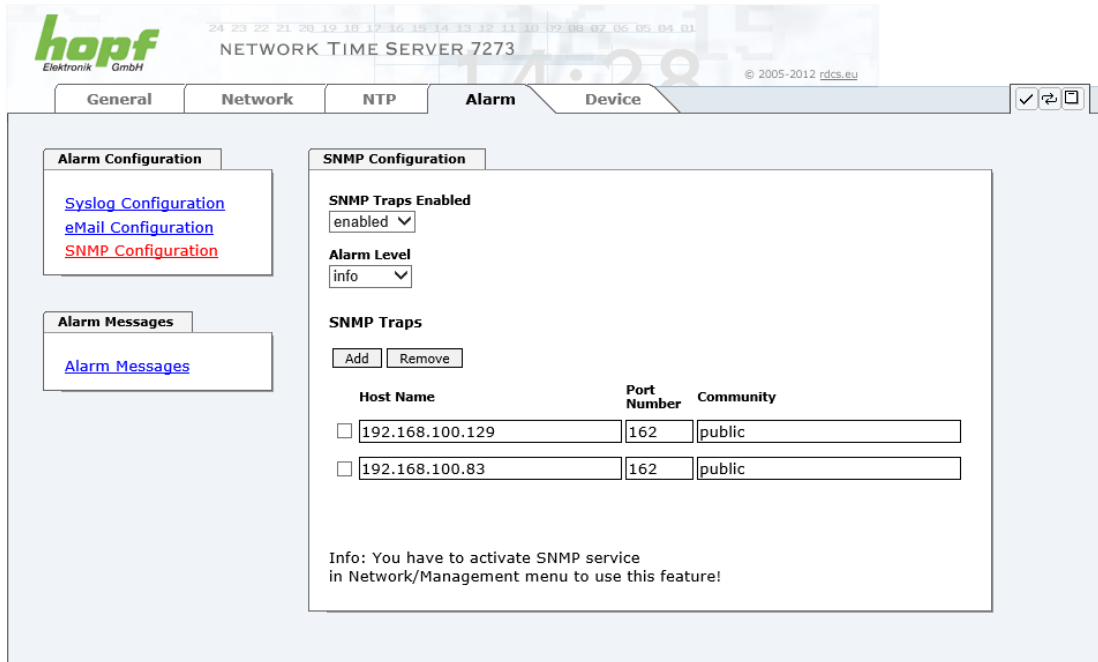
Some E-mail servers only accept messages if the sender address entered is valid (spam protection). This can be inserted in the "Sender Address" field.

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 6.3.4.4 Alarm** ).

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

### 6.3.4.3 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 6.3.5.13 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 6.3.4.4 Alarm** ).
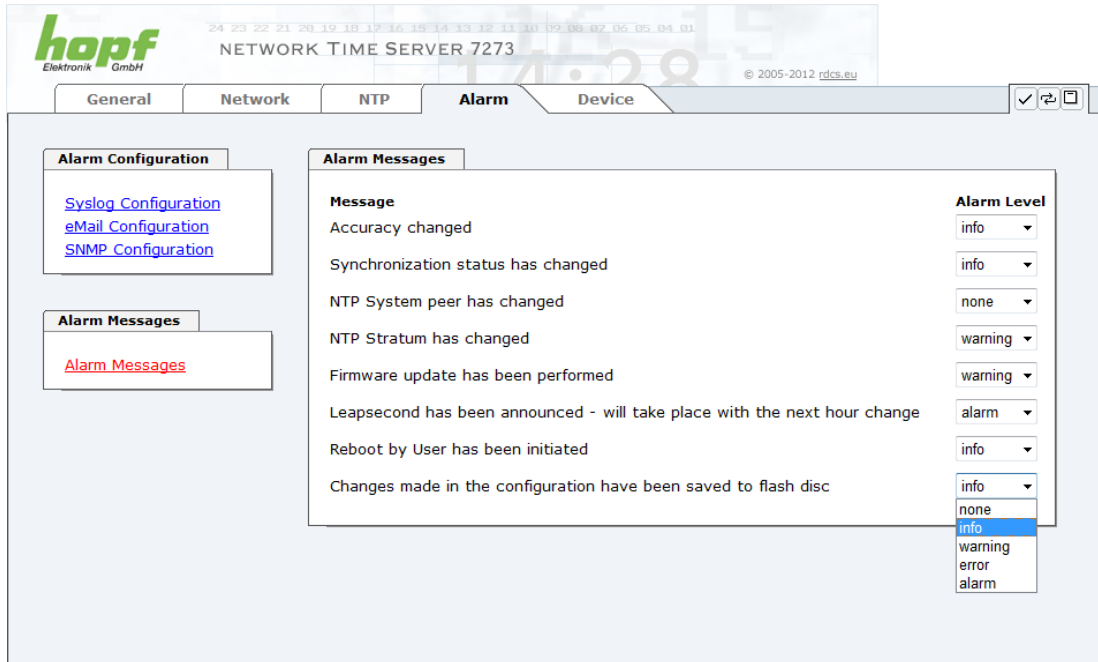
| Alarm Level | Transmitted Messages |
|---|---|
| none | no messages |
| info | info / warning / error / alarm |
| warning | warning / error / alarm |
| error | error / alarm |
| alarm | alarm |

SNMP protocol must be enabled in order to use SNMP (see **Chapter 6.3.2.4 Management-Protocols – HTTP, SNMP**).

## 6.3.4.4 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.

## 6.3.5 DEVICE Tab

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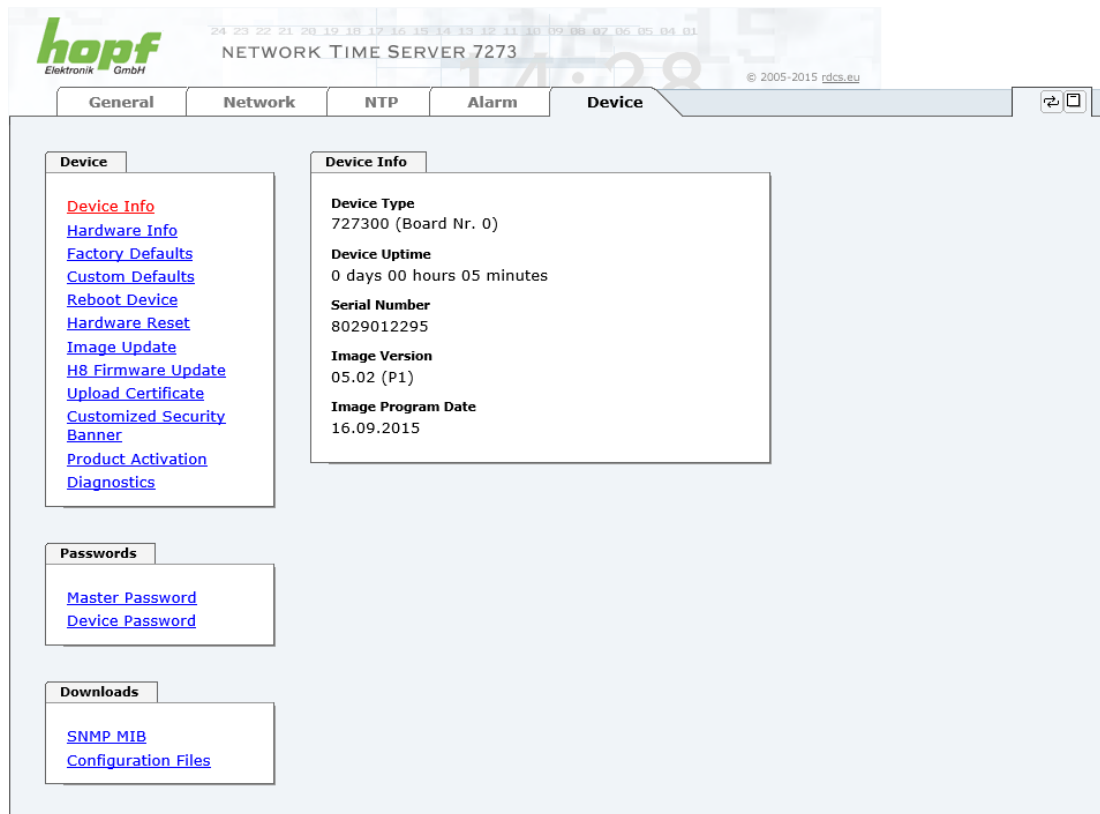


This tab provides the basic information about the Board hardware and software/firmware. Password administration and the update services for the Board are also made accessible via this website. The complete download zone is also a component of this site.
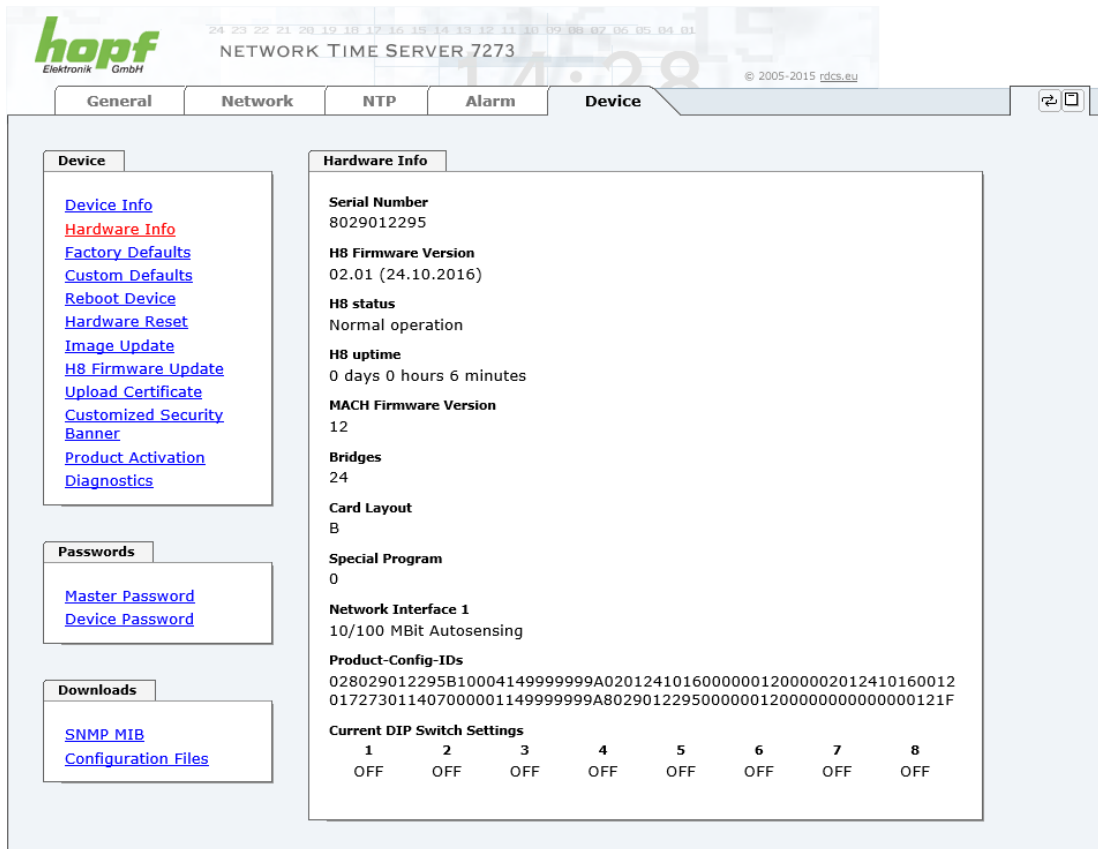
### 6.3.5.1 Device Information

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.

## 6.3.5.2 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 7273(RC) will be shown under the point "Current DIP Switch Settings"

### 6.3.5.3 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).
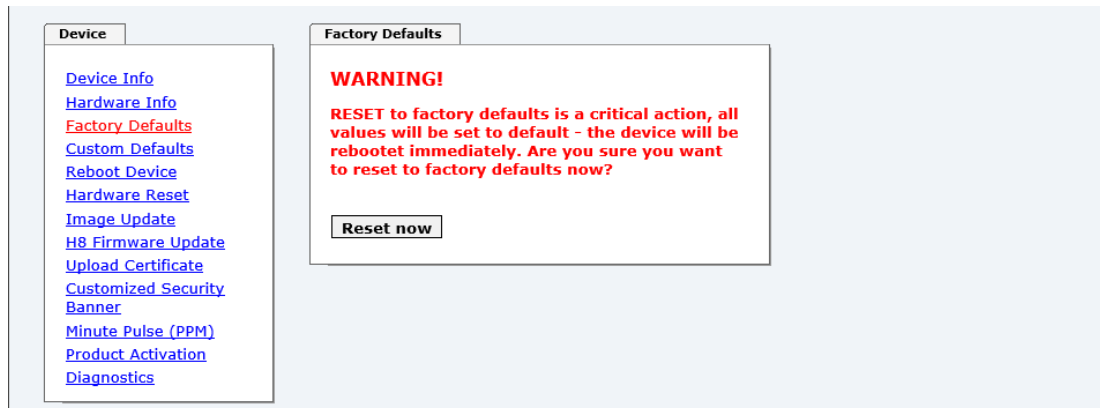


This function serves to restore all values in the flash memory to their default values. This also includes passwords (see **Chapter 9 Factory Defaults of Board 7273(RC)**).

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.

### 6.3.5.4 Restoring saved Customer Settings (Custom Defaults)

This function allows to save a current configuration as CUSTOM DEFAULTS.

The current configuration is saved. It is irrelevant whether the configuration has already been saved with "**SAVE to FLASH**" or just activated by "**Apply**".

```
┌─────────────────┐  ┌────────────────────────────────────────────────┐
│ Device          │  │ Reset to Custom Defaults                       │
│                 │  │ ┌──────────────────────────────────────────────┐│
│ Device Info     │  │ │ No Custom Defaults available. They can be saved││
│ Hardware Info   │  │ │ below based on the current configuration.    ││
│ Factory Defaults│  │ └──────────────────────────────────────────────┘│
│ Custom Defaults │  │                                                │
│ Reboot Device   │  │ Save Custom Defaults                           │
│ Hardware Reset  │  │ ┌──────────────────────────────────────────────┐│
│ Image Update    │  │ │  ┌──────────────────────────┐                ││
│ H8 Firmware Update│  │ │  Save Custom Defaults now │                ││
│ Upload Certificate│  │ │  └──────────────────────────┘                ││
│ Customized Security│  │ └──────────────────────────────────────────────┘│
│ Banner          │  │                                                │
│ Minute Pulse (PPM)│  │                                               │
│ Product Activation│  │                                               │
│ Diagnostics     │  │                                                │
└─────────────────┘  └────────────────────────────────────────────────┘
```

In order to activate a CUSTOM DEFAULTS a configuration has to be saved initially.

Saving is only processed via the button "**Save Custom Defaults now**". A successful saving is confimred with a text message underneath the button.

> ⚠ If the user saves **no** CUSTOM DEFAULT via the WebGUI, a FACTORY DEFAULT via dthe Reset-(Default) button is triggered instead.

With this function the saved configuration is written back into the flash memory.

> ⚠ The settings for activation keys (e.g. an entered activation key) are neither deleted nor restored by the CUSTOM DEFAULTS.

## 6.3.5.5 Restarting the Board (Reboot Device / Hardware Reset)

> ⚠ The restart concerns Board 7273(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.

## 6.3.5.6 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**.

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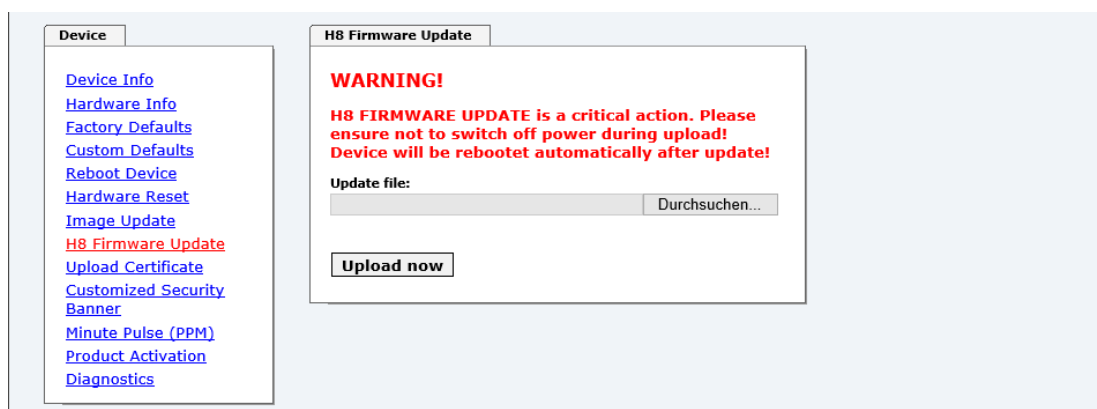
In order to carry out an update, enter the name and the folder in which the update / firmware image is located in the text field or open the file selection dialogue by pressing the "Browse" button.

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

H8-7273(8029)_v0114_128.**mot**    for the **H8 firmware**
(update takes approx. 1-1.5 minutes)

upgrade_8029gen_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.

## 6.3.5.7 Upload SSL-Server-Certificate

This offers the possibility to encrypt the https connections to the board 7273 (RC) with a user-provided SSL server certificate.

## 6.3.5.8 Customized Security Banner

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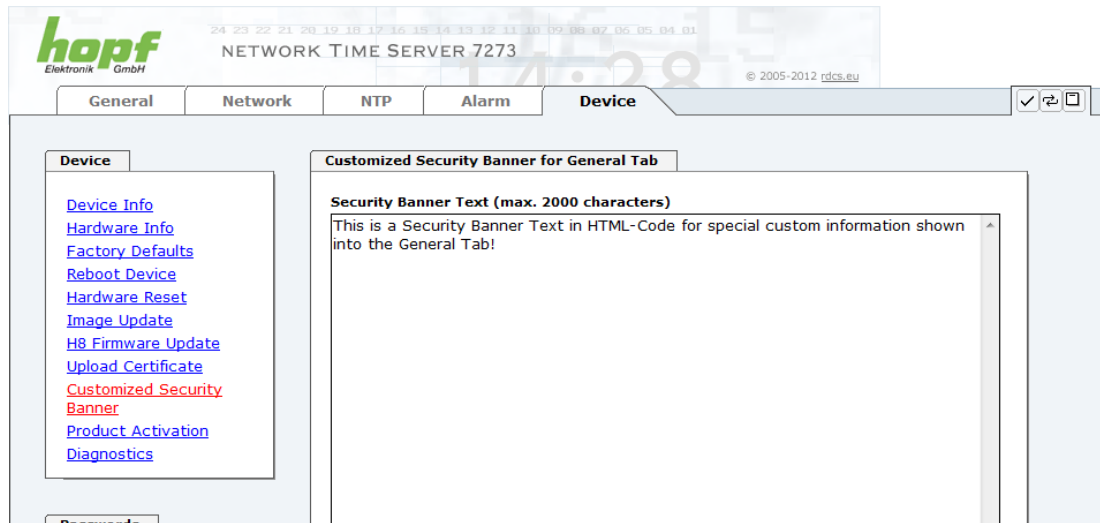


The security information can be written as 'unformatted' text as well as HTML formatted text. 2000 characters are available to write failsafe into the board 7273(RC).
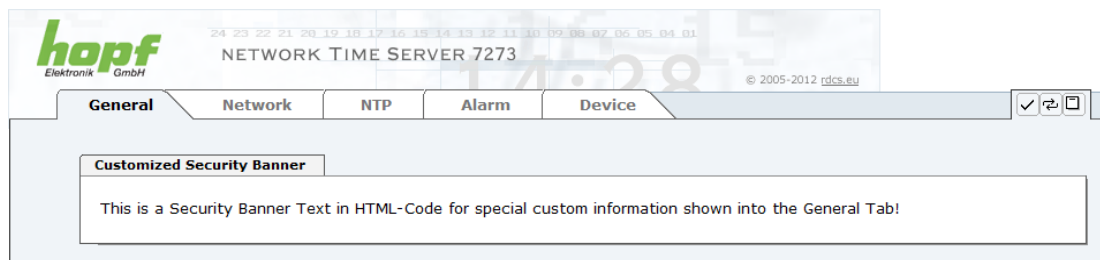


After a successful storage the "Customized Security Banner" with the saved security information is displayed in the General-Tab.

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

### 6.3.5.9 Option FG7273/PPM: Minute Pulse Length (PPM)

With this option FG7273/PPM a high active isolated minute pulse (high active) of +12V DC is distributed on the 3 pole screw terminal. Further technical data can be found in **Chapter 8 Technical Data**.

The output is an "open collector" with a current limiter. For further information see **chapter 1.3.1.7 Option: Active 12V DC PPM (Minute Pulse)**.

> **i** This minute pulse is fully compatible to the minute pulse of the **hopf** board 7270/7271 (the electrical properties as well as the adjustable parameters).

> **i** The menu item Minute Pulse (PPM) is only indicated in WebGUI if this function is also available for the board.

> **i** Both boards 7273 and 7273RC are available with the option FG7273/PPM. A subsequent upgrading of this option is not possible by the customer.

The length of the pulse can be adjusted in 4 steps.
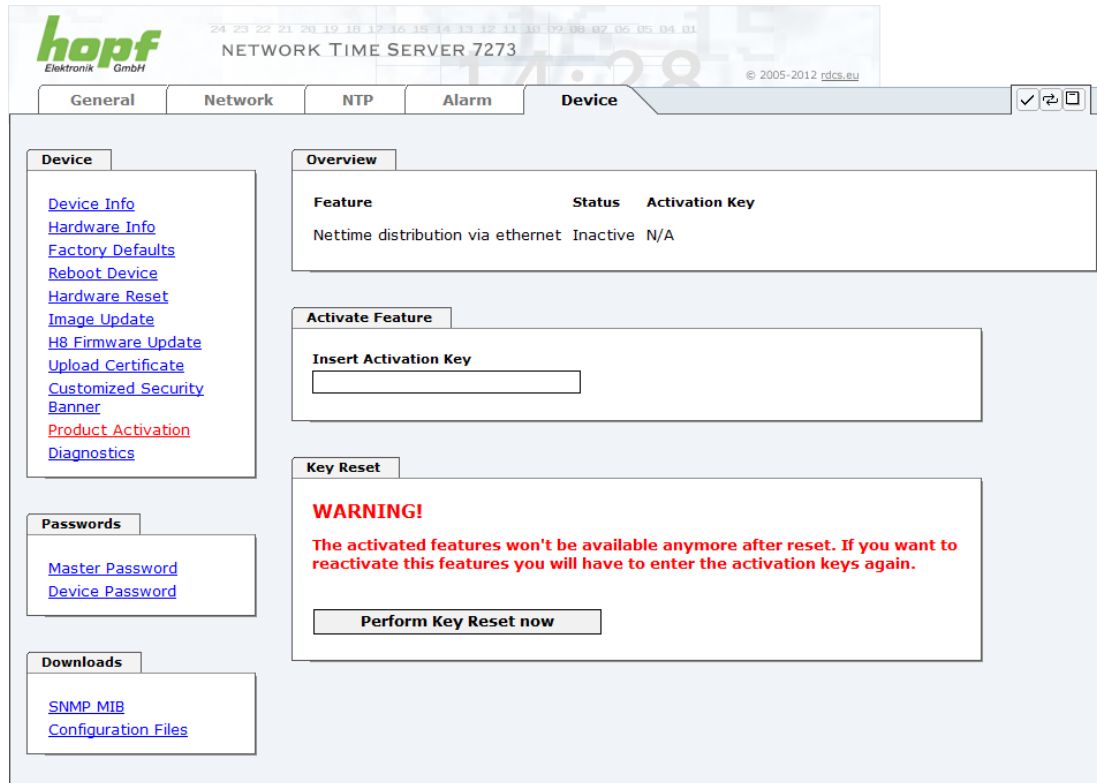
| Pulse Length of the Minute Pulse (high active) |
|---|
| 10 msec |
| 100 msec |
| 500 msec |
| 1000 msec |
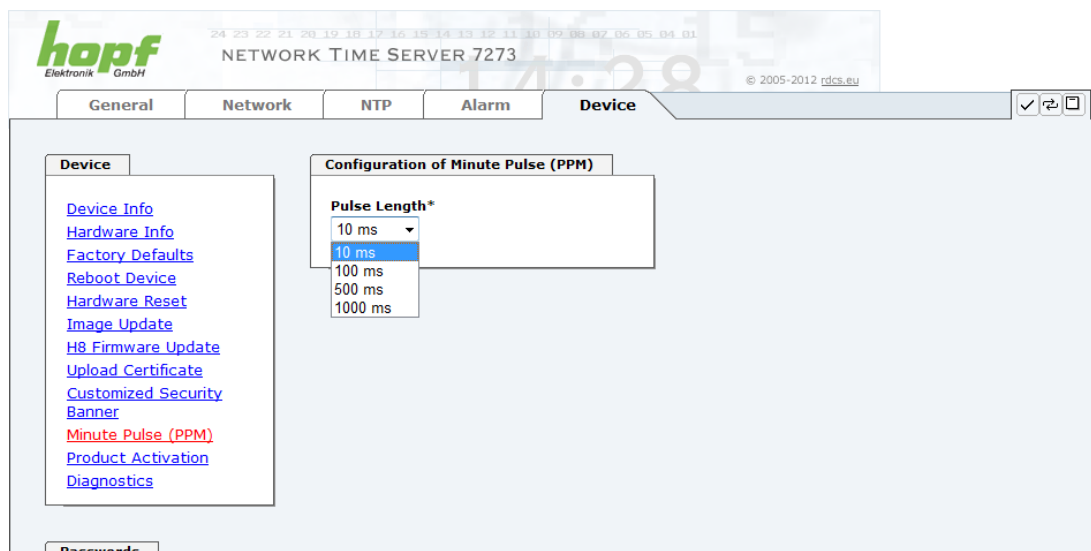
### 6.3.5.10    Product Activation

Optional features (e.g. net frequency output via ethernet) 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.



**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.

## 6.3.5.11 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.

### 6.3.5.12 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*)

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

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

## 6.3.5.13 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.



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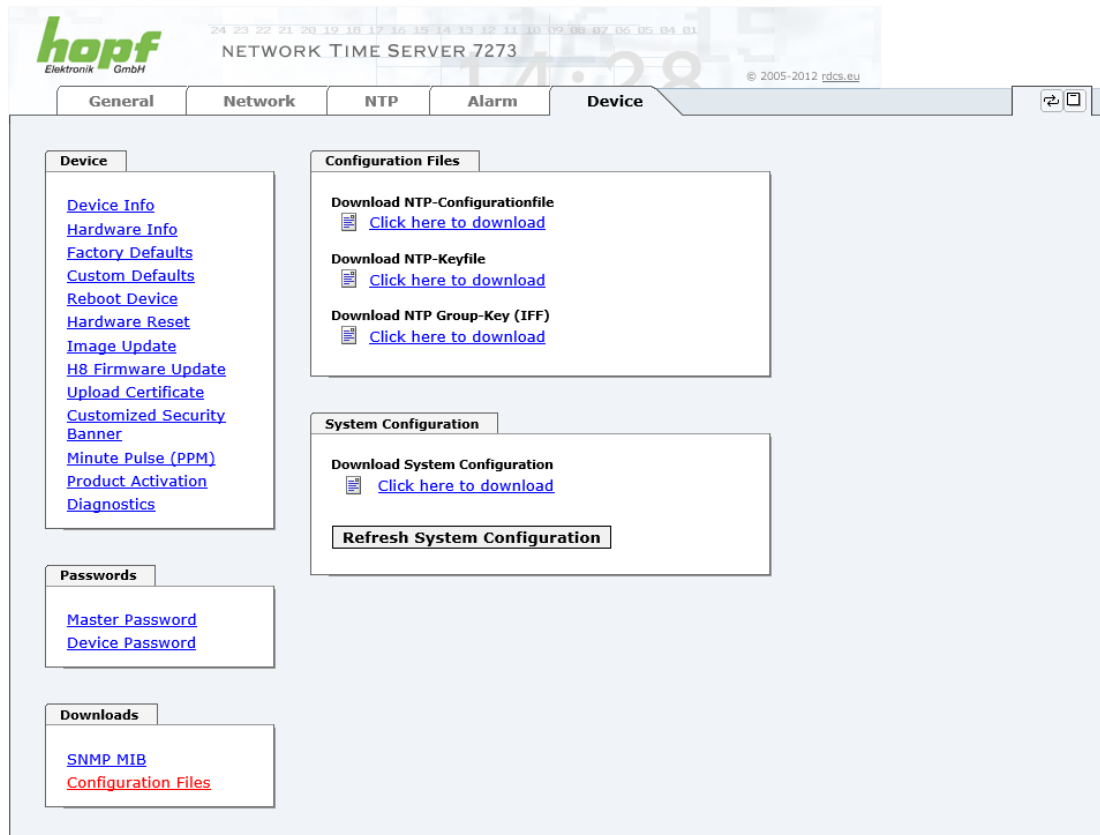
| | |
|---|---|
| **i** | The loaded file **System Configuration** from the board is only used for support purposes and cannot be reloaded for adjusting the settings. |

| | |
|---|---|
| **!** | 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.



---
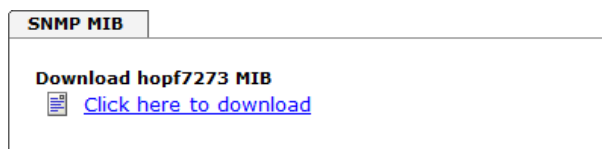
# 7    SSH and Telnet Basic Configuration

> ⚠ Only basic configuration is possible via SSH or Telnet. The complete configuration of Board 7273(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 6.3.5.12 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 6.3.2.4 Management-Protocols – HTTP, SNMP**)

```
192.168.100.184 - PuTTY                              _  □   ×
login as: master
master@192.168.100.184's password:


      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 727300 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 7273(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
- SNMPv2 / 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 | |
|---|---|
| Normal operation | Typical: 230 mA (max. 300 mA) |
| Boot phase | Typical: 230 mA (max. 300 mA) |
| **LAN** | |
| Network Connection | Via a LAN cable with RJ45 plug (recommended cable type CAT5 or better). |
| Requests per second | max. 1000 requests |
| Number of connectable clients | Theoretically unlimited |
| **Network interface ETH0** | 10/100 Base-T |
| **Ethernet compatibility** | Version 2.0 / IEEE 802.3 |
| **Isolation voltage** (network to system side) | 1500 Vrms |
| **MTBF** | |
| MTBF | > 900,000 hours |

### Board 7273 with Option FG7273/PPM (Output Minute Pulse)

| **Minute Pulse** | **12V DC, potential isolated via an 'open collector unit'** |
|---|---|
| As Current Source | typical: 20mA (max. 30 mA) The output load should be ($R_L$ < 600 Ohm), because of a too small edge steepness. |
| Output logic | high active |
| | |
| Active output voltage | 12V DC, max. 100mA, potential isolated |
| Isolation voltage | min. 1000V DC |

# 9 Factory Defaults of Board 7273(RC)

The default delivery status of the Board 7273(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 factrory-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 Presentation |
|---|---|---|
| Hostname | hopf7273 | hopf7273 |
| Default Gateway | No change | --- |
| DNS 1 | Blank | --- |
| DNS 2 | Blank | --- |
| **Network Interface ETH0** | **Setting** | **WebGUI** |
| Use Custom Hardware Address (MAC) | Disabled | disabled |
| Custom Hardware Address (MAC) | Blank | --- |
| DHCP | Enabled | enabled |
| IP | No change | no change |
| Netmask | No change | no change |
| Operation mode | Auto negotiate | auto negotiate |
| **Routing** | **Setting** | **WebGUI** |
| 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 | Blank | --- |
| Read/Write Community | Blank | --- |
| Security Name | Blank | --- |
| Access Rights | Readonly | Readonly |
| Authentication Protocol | MD5 | MD5 |
| Authentication Passphrase | Blank | --- |
| Privacy Protocol | DES | DES |
| Privacy Passphrase | Blank | --- |
| Read/Write Community | Blank | --- |
| **Time Protocols** | **Setting** | **WebGUI** |
| NTP | Enabled | enabled |
| DAYTIME | Disabled | disabled |
| TIME | Disabled | disabled |
| SINEC H1 time datagram | Disabled | disabled |
| **SINEC H1 time datagram** | **Setting** | **WebGUI** |
| Send Interval | every second | 1 second |
| Timebase | UTC | UTC |
| Destination MAC Address | 09:00:06:03:FF:EF | 09:00:06:03:FF:EF |
| Minimum Accuracy | LOW | low |
| **DIP-Switch DS1 SW6** | **Setting** | **WebGUI Presentation** |
| Transmission point of the SINEC H1 time datagram | off (same second) | off |

## 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    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 |

## 9.4    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 |
| **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<br>http://de.wikipedia.org/wiki/User_Datagram_Protocol |
| **ToD** | Time of Day |
| **UDP** | User Datagram Protocol<br>http://de.wikipedia.org/wiki/User_Datagram_Protocol |
| **UTC** | Universal Time Coordinated |
| **WAN** | Wide Area Network |
| **msec** | millisecond ($10^{-3}$ seconds) |
| **µsec** | microsecond ($10^{-6}$ seconds) |
| **ppm** | parts per million ($10^{-6}$) |

## 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.

## 10.5  Syslog Messages

Description of the Syslog messages of the board 7273(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 854-861)

- SNMPv2 (RFC 1213, RFC1901-1908)

- SNMPv3 (RFC 3410-3418)

- SYSLOG (RFC 5424)

- SMTP (RFC 5321)

# 12 List of Open Source Packages used

Third Party Software

The *hopf* network TimeServer 7273(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 | License | License details | Patches |
|---|---|---|---|---|
| boa | 0.94.14rc21 | GPL | v1+ | No |
| busybox | 1.18.5 | GPL | v2 | No |
| eeprog | 0.7.6 | GPL | v2+ | No |
| ethtool | 2.6.39 | GPL | v2 | No |
| i2c-tools | 3.0.3 | GPL | v2 | No |
| libatomic_ops | 1.2 | GPL | v2 | No |
| libdaemon | 0.14 | LGPL | v2.1 | No |
| libelf | 0.8.12 | LGPL | v2 | No |
| libevent | 1.4.12 | 3-clause BSD | http://libevent.org/LICENSE.txt | No |
| libgcrypt | 1.5.0 | GPL | v2 | No |
| libgpg-error | 1.8 | GPL | v2 | No |
| libsysfs | 2.1.0 | LGPL | v2.1 | No |
| libupnp | 1.6.6 | BSD | http://pupnp.sourceforge.net/LICENSE | No |
| libusb | 1.0.8 | LGPL | v2 | No |
| linux | 2.6.38.8 | GPL | v2 | No |
| ltrace | 0.5.3 | GPL | v2 | No |
| lzo | 2.05 | GPL | v2 | No |
| mii-diag | 2.11 | GPL | | No |

| Package name | Version | License | License details | Patches |
|---|---|---|---|---|
| **mini_httpd** | 1.19 | | Copyright © 1999,2000 by Jef Poskanzer <jef@mail.acme.com>. All rights reserved.<br><br>Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:<br>1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.<br>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.<br><br>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 |
| **mtd** | 1.4.6 | GPL | v2 | No |

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

| Package name | Version | License | License details | Patches |
|---|---|---|---|---|
| **ncurses** | 5.7 | Permissive free software licence | Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.<br><br>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, 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:<br><br>The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.<br><br>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.<br><br>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. | No |
| **netsnmp** | 5.6.1 | BSD (more) | http://net-snmp.sourceforge.net/about/license.html | No |
| **ntp** | 4.2.8p2 | NTP | Copyright (c) University of Delaware 1992-2011<br><br>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. | Yes (6) |
| **openssh** | 5.8p2 | BSD | | No |
| **openssl** | 1.0.0d | Dual | http://www.openssl.org/source/license.html | No |
| **readline** | 6.2 | GPL | v3 | No |
| **setserial** | 2.17 | GPL | | No |
| **strace** | 4.5.20 | BSD | | No |
| **sudo** | 1.7.6p2 | ISC-style | http://www.sudo.ws/sudo/license.html | No |

7273 and 7273RC NTP/SINEC H1 LAN Board - V05.01

| Package name | Version | License | License details | Patches |
|---|---|---|---|---|
| uboot | 2010.06 | GPL | v2 | No |
| uboot-tools | 2011.03 | GPL | v2 | Yes (1) |
| uClibc | 0.9.32 | LGPL | v2.1 | No |
| usbutils | 003 | GPL | v2 | No |
| util-linux | 2.19.1 | GPL | v2 | No |
| which | 2.20 | GPL | v3 | No |
| zlib | 1.2.5 | Permissive free software licence | http://www.gzip.org/zlib/zlib_license.html | No |