MOUNTING AND INSTRUCTION MANUAL

DTS 4163.GRANDMASTER

PTP Grandmaster, PRTC with PRP and HSR

BE-801386.12 | 21.11.2025

Regulations and Certification

This product was developed and produced in accordance with the following EU directives:

EMC	Electromagnetic compatibility directive 2014/30/EU
LVD	Low voltage directive 2014/35/EU
RED	Radio equipment directive 2014/53/EU
RoHS	Restriction of the use of certain hazardous substances directive 2011/65/EU
REACH	Chemical substances directive 1907/2006/EC
WEEE	Waste electrical and electronic equipment directive 2012/19/EU
Railway Interop.	Interoperability of the rail system within the European Union directive 2016/797/EU
Railway Safety	Railway safety directive 2016/798/EU

See Conformity for the declaration of conformity of this specific product. This product may offer a CB test certificate for download at MOBATIME.COM/support/resources.

CE

Important Notes

This document was generated November 25, 2025 with the following disclaims:

1. Please read and follow the safety information in this document before operating the product. We cannot guarantee that no accidents or damage will occur due to improper use of this product. Please use this product with care and operate at your own risk.
2. We are not liable for any direct or indirect damage caused by the use of this document or the said product.
3. This product must be connected and installed by a qualified electrician who is familiar with the relevant regulations (e.g. VDE).
4. The information in this document is subject to change without notice. The latest version of this document is available for download at MOBATIME.COM/support/resources.
5. The product software is continuously being optimized and supplemented with new options. The latest firmware is available for download at MOBATIME.COM/support/resources.
6. This Instruction Manual has been composed with the utmost care to explain all the details to ensure a safe and stable operation of this product. Nevertheless, if questions arise or any errors appear, feel free to contact support.
7. **MOBATIME Two Years Limited Product Warranty.** MOSER-BAER AG and BÜRK MOBATIME GmbH warrant MOBATIME branded hardware product contained in the original packaging against defects in materials and workmanship when used normally in accordance with MOBATIME's guidelines for a period of TWO YEARS from the date of original retail purchase by the end-user purchaser.
8. No part of this document or the said product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from BÜRK MOBATIME GmbH, D-78026 VS-Schwenningen or MOSER-BAER AG - CH 3454 Sumiswald.
9.

Contents

1 Safety

Read the safety sections carefully and follow all the instructions. This ensures safe and reliable operation of this device.

1.1 Instructions and Symbols

Symbols used throughout this document and their meaning are as follows:

A note or important information.

Answer to a possible question. Contact information.

Keep away from children and people with limited physical, sensory, or mental capacities

Action needs to be taken.

Connect device to earth ground.

More information included in the manual.

Disconnect mains power before doing anything.

Attention of electrical shocks.

Attention of laser beam.

Surface may be hot.

Item is flammable.

A warning, be cautious.

Recyclable materials.

Do not put in trash.

1.2 General

For safety and licensing reasons, unauthorized modifications and/or changes to the product is prohibited. Maintenance, adjustments or repairs may only be carried out by the factory (copyright holder).

The product is not a toy; it does not belong in the hands of children. Mount or place the product so that it cannot be reached by children. Children may try to insert objects into the product. The product will not only be damaged, but there is also a risk of injury, as well as danger to life through electric shock.

Never open the housing of this product, for it poses mortal danger from electric shock or may even cause a fire.

- Keep packaging such as plastic films away from children. There is the risk of suffocation if misused.

Use caution with the product, knocks, blows, or even falls from a low height can damage it.

In industrial facilities, the accident prevention regulations of the trade associations for electrical systems and equipment must be observed.

- Do not use the product if it is damaged. It can be assumed that safe operation is no longer possible if:
  - the product has visible damage;
  - the product is not working properly (thick smoke or a burning smell, audible crackling noise, discoloration of the product or surrounding areas);
  - the product was stored under adverse conditions;
  - tough conditions during transport.

Improper handling of this product operated on the mains voltage can cause mortal danger from electric shock!

Interconnecting or combining equipment bearing a CE label does not inevitably result in a system that conforms with the safety regulations. Integrators will have to reassess the new product's compliance according to the locally valid directives. See section Conformity for more information on certification of this product.

1.3 Installation

- This product must be connected and installed by a qualified electrician who is familiar with the relevant regulations (e.g. VDE).

Never plug the product into voltage/power supply immediately after it has been moved from cold into warm environment (e.g. during/after transport/unboxing). The resultant condensed water may damage the product or may cause electric shock.

Allow the product to reach the ambient temperature. Wait until the condensation has evaporated, this can take a few hours. Only then can the product be connected to the voltage/current supply and put into operation.

This product may have screw terminal with open electrical contacts. It is essential to ensure that the connection is made only when no voltage/current is applied. Secure the power supply to prevent accidental reconnection. Verify the absence of voltage using an appropriate meter.

The power supply line must be protected with a residual current circuit breaker (RCCB) with a trip current <= 30 mA.

Always connect earth ground to the device at the indicated protective earth terminal (PE or earth symbol indication).

Always unplug a power plug from the socket only at the intended gripping surface, pull the power plug not the cord from a power outlet. Wires may rip out and pose danger to life through electric shock.

Maintain sufficient cooling of the product according to its specifications.

1.4 Operation

- Use the product in the specified environment. Use outside of the specifications can damage the product and/or stop any operation.
- The product may not be exposed to extreme temperatures, direct sunlight or strong vibrations. Protect the product from moisture, dust and dirt.

Operation in environments with excessive dust, flammable gases, vapours or solvents is not permitted. It may cause explosion or fire.

Depending on the cooling type, the product housing may reach temperatures above 60°C which can burn the skin.

- Do not overload the product. Note the input/output voltages and currents as well as output powers indicated on the product.
- Depending on the input currents and input voltages, suitable connecting cables with appropriate cable diameter must be used. Only use the plugs and connectors supplied in the original packaging with the product.

1.5 Maintenance and Cleaning

- If the product and/or the connecting cable is damaged, do not touch it: there is mortal danger from electric shock! First, turn off the power supply to all poles of the product (turn off associated circuit breaker or remove the fuse, then turn off GFCI). Verify the absence of voltage using an appropriate meter.
- For the end consumer, the product is maintenance free. Leave any maintenance to an expert. Repairs may only be done by the factory itself (copyright holder).
- Unplug all poles of the product from the operating voltage before cleaning.
- For external cleaning one can use a clean, soft, dry cloth. Dust can be easily removed with a clean, soft brush and a vacuum cleaner.
- Do not use aggressive chemicals or abrasive cleaners, as this may cause discoloration or even material changes.
- This product is equipped with fuses for protection against high voltage and high currents. Burned fuses may only be replaced by the factory itself (copyright owner).

Never bridge a fuse, it is a fire hazard and can cause a fatal electric shock.

Read the Troubleshooting section to find help to common mistakes, misbehavior and known issues.

1.6 Disposing

At the end of its lifecycle, do not dispose of this device in the regular household rubbish. Return it to the supplier who will dispose of it correctly.

This product was packed and stuffed with proper materials to protect it during transportation. Packaging materials can be recycled and should be disposed environmentally friendly.

2 Important Notes

After the first successful login over SSH the one-time password must be changed.

Prior the first SCP or SFTP connection, login via SSH to change the one-time password.

During a firmware update, do NOT reboot or cut power to the device.

To enable PTP probing, the profile parameters clientOnly and free_running must always be set to 1.

Use an appropriate SFTP/SCP capable client, such as FileZilla or WinSCP, for file transfers.

3 Introduction

High precision IEEE 1588v2.1 Precision Time Protocol (PTP) grandmaster and Primary Reference Time Clock (PRTC-A) with Parallel Redundancy Protocol (PRP) and High Availability Seamless Redundancy (HSR).

The DTS 4163 is built to distribute time and frequency synchronization in power plants, power distribution and industrial automation, as well as for testing and measuring of frequencies, time signals and time protocols. The built in enhanced redundant operation features increase availability, secure time distribution and protection against jamming and spoofing of GNSS signals.

4 Terms and Definitions

The following terms and definitions apply to this device:

Permanently connected equipment
Equipment that can only be electrically connected to or disconnected from the mains by the use of a tool.

Professional equipment
Equipment for use in trades, professions or industries and which is not intended for sale to the general public.

Indoor equipment
Equipment for indoor use only. All external circuits installed wholly within the same building structure. For installations where external circuits extend beyond the building structure, additional surge protection and grounding must be implemented by a skilled person according to applicable safety standards.

Class I equipment
Equipment with basic insulation used as a basic safeguard, and with protective bonding and protective earthing used as a supplementary safeguard.

Instructed person
Person instructed or supervised by a skilled person as to energy sources and who can responsibly use equipment safeguards and precautionary safeguards with respect to those energy sources (for installation and operation of the device inside a building).

Skilled person
Person with relevant education or experience to enable him or her to identify hazards and to take appropriate actions to reduce the risks of injury to themselves and others (for GNSS antenna installation outside of a building).

Normal operating condition
Mode of operation that represents as closely as possible the range of normal use that can reasonably be expected.

These terms may be used throughout the manual and instructions have to be followed in order to ensure safe operation of the equipment (device) and safety to the users. Since this is a professional and permanently connected equipment only an instructed person may operate this device. Further the normal operating conditions have to be ensured and maintained for safe operations (see environment for details).

Following abbreviations are used throughout the entire manual:

Abbreviation	Definition
AM	Amplitude Modulation
BCD	Binary Coded Decimal
BMCA	Best Master Clock Algorithm
CF	Control functions
CLI	Command Line Interface
CSV	Comma-Separated Value
DC	Direct Current
DCF-CL	DCF Current Loop
DCLS	DC Level Shift
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
E2E	End-to-End
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GNSS	Global Navigation Satellite System
GW	Gateway
HF	High Frequency
HSR	High Availability Seamless Redundancy

Abbreviation	Definition
HTTP(S)	Hypertext Transfer Protocol Secure
IRIG	Inter Range Instrumentation Group
ISO	International Organization for Standardization
L2	ISO/OSI Layer 2
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LDAP(S)	Lightweight Directory Access Protocol Secure
LED	Light Emitting Diode
MD5	Message-Digest algorithm
ms	Millisecond(s)
MTIE	Maximum TIE
NM	Network Manager
NMS	Network Management System
ns	Nanosecond(s)
NTP	Network Time Protocol
OSI	Open Systems Interconnection
P2P	Peer-to-Peer
PICS	Protocol Implementation Conformance Statement
ppb	parts per billion
PPS	Pulse-per-second
PRP	Parallel Redundancy Protocol
PRTC	Primary Reference Time Clock
PSU	Power Supply Unit
PTP	Precision Time Protocol
PWM	Pulse width modulation
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RTC	Real-Time Clock
RSA	Rivest-Shamir-Adleman (public-key cryptosystem)
S	Sample(s)
s	second(s)
S-FTP	Secure File Transfer Protocol
SBS	Straight Binary Seconds
SCP	Secure Copy Protocol
SFP	Small Form-Factor Pluggable (mini-GPIC)
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TE	Time Error
TIE	Time Interval Error
TLS	Transport Layer Security
TUI	Terminal User Interface
us	micro second(s)
USB	Universal Serial Bus

5 Quick Start Guide

Please read safety and mounting instructions before you set up this device.

5.1 Standard Setup

1. Connect GNSS Antenna
2. Connect network and/or serial
   - LAN1: DHCP
   - LAN2: Address 192.168.1.2/24
   - LAN3: DHCP
   - LAN4: Address 172.16.0.4/16
   - LAN5: DHCP (extension only)
   - Serial over USB C Port: speed 38’400, no parity
3. Connect power
   - Keep attention to the power ratings of your device.
   - Do not switch polarity of power supply (**P**: positive or phase, **N**: negative or neutral).
   - Please also connect protective earth to ensure your safety and correct operation of the device.
4. Login via network and/or serial
   - Login as dts.admin.
   - See section Login for default login.
5. Change configuration as desired
   - Network: use `nmtui` or `nmcli` from the command line interface (CLI) to configure the network.
   - Device: use dts `menu` to change other configurations.

5.2 Time Source Setup

Multiple time sources can be selected to synchronize this DTS or other devices with time and/or frequency signals (see Time Handling for details).

5.2.1 Client/Input Source

GNSS is set as default source to synchronize this device. In order to change the primary source or add another source as backup do as follows:

1. Set up the device as described in Standard Setup
2. In TUI navigate to *Configuration > Time > Source* and select *DCF* as an example.
3. Enable the source and set the cable delay according to the length of the cable from this device to the antenna (1ns delay = ~15cm of cable).
4. - *Save Changes* - and make sure you have the antenna connected.
5. Navigate back and into *Configuration > Time > Source > Priorities* and select *Priority 1* to change primary source or any of the other priorities as second, third and so on.
6. From the priority selector choose *DCF* and - *Save Changes* -.

5.2.2 Server/Output Source

This device may be server/master of many types of sources (see Time Sources for details). For example to operate as NTP server, do as follows:

1. Set up the device as described in Standard Setup
2. In TUI navigate to *Configuration > Time > Source > NTP > Server*.

3. Enable the server and add multicast/broadcast entries as needed.
4. - *Save Changes* - and your device will be reachable as NTP server.

5.3 Probing Setup

1. Set up the device as described in Standard Setup
2. Open the terminal user interface TUI if not opened automatically (enter `dtstui`, `menu`, or `tui` on the command line interface CLI)
3. Navigate to *Profiles > ptp > probe.cfg*
   - Verify Settings;
   - See section Create New Config File if different settings are needed.
4. Navigate to *Configuration > Probing > PTP*
   - Set *Enable* to *1/yes*;
   - Set *Log memory* to *SD*;
   - Select the LAN *Interface* on which to probe;
   - Set a *Name* for the measurement data file;
   - Set *Config file* to probe.cfg;
   - - *Save Changes* -.
5. As soon as the device is properly synchronized, probing will start.
6. The web server showing measurement data is accessible under any of the device's IP address' (for example: https://192.168.1.2).

For debugging issues, consult the probing logs in `log/ptp/*` and `log/dtsprobe/*`.

5.4 Output Setup

Your device offers a variety of generators, which can be configured to generate a certain signal; see Signal Generators for details.

1. Set up the device as described in Standard Setup
2. In TUI navigate to *Configuration > Outputs > Generators* and select 1 PPS, Frequency 1-3 or IRIG 1 or 2.
3. Configure the generator to match the signal you would like to output. Make sure *enable* is set to *1/yes*.
4. Navigate back and into *Configuration > Outputs > Output [1-5]* and select the generator you just configured. Also make sure *enable* is set to *1/yes*.
5. - *Save Changes* - and within 1-2 seconds, the configured output will show the signal from the selected generator.

Each generated signal is synchronous to the system time and only generated once the device has been synchronized to a time source.

6 User Interfaces

There are 2 available interfaces. A terminal user interface (TUI) and a command line interface (CLI). Both are accessible via serial or SSH connection. Depending on the logged in user and its associated privileges different interfaces are available.

User	Interface
dts.admin	CLI, TUI
dts.operator	TUI
dts.info	TUI

6.1 Login

6.1.1 First Login

DTS 4163 ships with a one-time password, which you will be requested to change directly after the first successful login. Devices with manufacturing date Q3 2025 and later, each have an individual password, a unique one-time password. This unique one-time password is printed on a label on the back of your device. Make sure to store this password somewhere save in case you need it later again (e.g. after a factory default).

By default, dts.operator and dts.info users are blocked from login. An administrator first has to unlock those users as described in the security chapter, section Lock and Unlock Users. Legacy devices (production date earlier Q3 2025) have set a default one-time password whereas all newer device ship each with a unique one-time password formed with 5 blocks of 4 capital letters each and numbers separated with a hyphen-minus.

User names	Factory state	Legacy password	Default one-time password
dts.admin	unlocked	dts.admin	####-####-####-####-####
dts.operator	locked	dts.operator	dts.operator
dts.info	locked	dts.info	dts.info

Right after the first successful login over SSH or serial terminal users will be asked to change their password. by entering their current (default) password again followed by a new password, which has to be entered twice to confirm.

Do not loose the dts.admin password for it can only be reset in the factory.

Resetting the entire device to factory defaults (not just the configuration) will also reset all the passwords and factory state of each user.

6.1.2 RADIUS and LDAP

Coming soon.

6.2 Terminal User Interface (TUI)

6.2.1 Overview

The TUI is developed with an intuitive menu structure in mind. When started the **Main Menu** is displayed on the left side of the terminal. On the top row are device specific information as well as the systems time displayed. On the bottom row of the TUI is the device status visualized. The central space is used to display further information based on the selection in the **Main Menu**.

Main Menu Entry	Description
Status	Current device status and state information.
Logs	Device log file reader
Profiles	Submenu to configure interfaces and Input/Outputs
Information	Current runtime states per application
Configuration	Section to configure the DTS device
Maintenance	DTS device maintenance operations
Help	Further information about the device and software
Exit	Entry to leave the TUI application

6.2.2 Status

Status is a directory/file browser menu, where you can find current status information on the following topics:

Topic	Description	Directory/Files
Alarms	Current state of all alarm and warning flags.	alarm.txt, warning.txt
Core	Core information such as temperature readings or watchdog states.	core.txt, led.txt, monitor.txt, startstop.txt, swwd.txt, syswd.txt
Network	Information about all network interfaces, routing and current state.	network.txt, eth0-4.txt, routing.txt
Probing	Current PTP probing state.	probing.txt
Time	Information about all sources, current samples and state.	source.txt, time.txt, dcf.txt, gnss.txt, ntp.txt, pim_. . . txt, ptp1/2.txt, servo.txt, signal1/2.txt, time.txt

6.2.3 Logs

The logs menu is also a directory/file browser menu, where logs from all entities of the system can be found:

Topic	Description	Directory/Files
Login	Who has logged in an when.	auth.log
System	System startup, errors and kernel messages.	dts.log, syslog, dbusd.log, kern.log, rcS.log, rcK.log, user.log
Services	Networking service logs such as SSH or SNMP.	netconf.log, nginx.log, nm.log, sshd.log
Alarm	Alarm and other system state history logs.	history/*.log
DTS	DTS related application logs.	dts.log, dtscore.log, dtstime.log, dtsprobe.log, dtstui.log
Time	Time related logs may originate from PTP, NTP or dtstime.	ptp/*.log, ntp.log, dtstime/*.log

6.2.4 Profiles

Profiles are basically configuration files for services, that require more complex configurations. In this menu you can browse and edit the following:

- **ptp** configurations may contain more than a 100 parameters and the underlying ptp4l requires these files to operate.
- **net**work configurations are highly individual and endless combinations of systems are possible, therefore users may use these system level configuration files.

6.2.5 Information

Information is mostly a copy of the status menu but in a different representational form, which is used for Web, SNMP or netconf services. Here you easily find device stratum or currently active alarms as well as device information such as serial number or current firmware versions.

6.2.6 Configuration

This is where the device behavior can be changed, outputs enabled or time source selected:

- **Alarming** allows to mask alarms or set the alive notifications interval.
- **General** offers device parameters such as hostname, location and timezone.
- **Time** contains all the possible time source settings such as GNSS, PTP and NTP.
- **Outputs** provide settings for the various signal generators and mapping to the physical outputs.
- **Network** allows to select an existing profile to apply to a LAN port or enable HSR/PRP.
- **Probing** offers monitoring capabilities for PTP servers.
- **Services** allows for enabling services such as syslog or SNMP.

6.2.7 Maintenance

This menu offers you to perform maintenance actions, which are performed almost always immediately, such as the following:

Action Group	Description
Device	Restart device, clean the logs or test alarm notification
Firmware	Update or restore the device
Configuration	Backup and restore configuration
Network	Reset network failure alarm (HSR/PRP)
Dump	Create log and support package dumps
Probing	Reset measurements and clean data
Service	Restart services such as SSH and SNMP

Maintenance actions are performed immediately on selection.

6.2.8 Help

Help is a file browser which contains help and information on the following topics:

Topic	Description	Directory/Files
Manual	A few man pages with details about HSR, SNMP, IRIG and so on	man-*
Product	Product information such as article or serial numbers, fabrication infos, revisions and MAC addresses	product*, ethernet-mac, hardware-revision
Versions	Firmware versions and release information	software-version, firmware-version, release-notes, hardware-revision

6.2.9 Exit

Exit allows to exit the menu and return to the CLI or terminate the session (depends on the user).

It is always possible to exit the TUI from anywhere issuing CTRL-C command. ;

6.2.10 Terminal Settings

To display the TUI the used terminal is required to have at least a size of 80 columns and 24 rows. If the terminal is resized during the use of the TUI application a restart of the TUI application may be necessary.

In order for the TUI to display correctly in PuTTY, enable VT100 line drawing (graphical characters): *PuTTY > Window > Translation > Enable VT100 line drawing. . .*

6.2.11 Usage

Menu Navigation

The menu navigation is as follows:

Key	Effect
Arrow up	Menu Entry up
Arrow down	Menu Entry down
Arrow left or Backspace	Back
Arrow right or Enter	Select
m (lowercase letter m)	Go back to Main Menu
h (lowercase letter h)	Help and Information

File or Parameter Interface Navigation

As there are different types of files and parameters, different interfaces are available. Each configuration interface has some individuality and not every function is supported in each. The general usage is:

Key	Effect
Arrow up	Scroll up, Field up
Arrow down	Scroll down, Field down
Arrow left	Field left
Arrow right	Field right
Page up	Page up
Page down	Page down
q or Backspace or Escape	Close and back to menu
Enter	Select
h (lowercase letter h)	Help and Information

6.3 Command Line Interface

For administrative tasks the command line interface is available and should be used. Network interfaces can only be configured via the available CLI programs `nmcli` and `nmtui`. Some available programs are:

Every command can be aborted by typing `CTRL-C` or `q` sometimes. For instance, if you have entered `thetime` a digital clock with showing the current time on the screen, it can be closed with `CTRL-C` or `q`. Also the TUI or any other command and application can be closed this way.

6.3.1 Basic Commands

Command	Arguments	Description
cat	<dir/file>	read entire <file> at <dir>
cd	<dir>	change directory to <dir>
clear	-	Clear entire terminal content
cp	-r <dir/file>	Recursively (optional -r) remove
exit, logout	-	logout from current session
head	<dir/file>	read the first 10 lines from <file> at <dir>
help	-	list bash command help
history	-	show last used commands
ls, ll	<dir>	list files in <dir>
mkdir	<path/name>	create a directory at <path> with <name>
mv	<from> <to>	move and/or rename a file or directory
pwd	-	show current directory path
tail	<dir/file>	read the last 10 lines from <file> at <dir>
tree	<dir>	list all files and directories recursively in a tree view
rm	-r <dir/file>	Recursively (optional -r) remove <dir/file> (permanent)
whoami	-	print current logged in user name

For more optional arguments type <command> -h.

6.3.2 Advanced Commands

Command	Arguments	Description
grep	<term>	filter e.g. a list output with <term>
lp	-	list currently running operational processes
more	<dir/file>	read a <dir/file> partially with scrolling
mem	-	show current memory usage
nano	<dir/file>	edit <dir/file>
ram	-	show current ram usage

6.3.3 Operational Commands

Command	Arguments	Description
dtstui, menu, tui	-	open DTS TUI (configuration menu)
date	-	show current system time/date
identify	-	lets PSU LEDs on device flash to identify the device among others
last, lastb	-	list successful last and failed lastb login attempts
modify_user	--help	lock/unlock other users, expire passwords
ntpq	<server>	get NTP time/date of <server>
update	-	trigger firmware update from FTP
restart	-	reboot the device
restore_factory_defaults	-	restore entire device inclusive password and configuration to factory defaults
status	stats/<dir/file>	display status information by selecting specific <file>
thetime	-	display a digital real-time clock (close by pressing q or CTRL-C)

6.3.4 Networking Commands

Command	Arguments	Description
arping	`-I <ethX> <destination>`	send arp ping (L2) over interface `<ethX>`
hostname	-	show device hostname
ip	-a, -h	show current ip information
ips	-	show IPs and link status of all 5 LAN interfaces
lan_bw	-	monitor inbound and outbound network bandwidth usage
nmcli	-h	configure network via CLI
nmtui	-	open network manager TUI to show/edit network connections
ping	`-I <ethX> <destination>`	send ping (L3) over interface `<ethX>`
route	-h	show, edit or add routes
scp	`<src:/dir/file> <dest:/dir/>`	secure copy `<file>` from `<dir>` of `<src>` to `<dir>` of `<dest>`
ssh	`<address>`	open secure shell to address
tracepath	`<destination>`	provides information alongside the path to the `<destination>`
traceroute	`<destination>`	trace the route to the `<destination>` using IPv4
traceroute6	`<destination>`	trace the route to the `<destination>` using IPv6

6.4 File Transfer

The DTS 4163 provides only secure file transfer via SFTP and SCP. Both protocols are configured to use the default port 22. File transfer can be used to:

- Copy log files out of the device;
- Copy signal/ptp profiles onto the device;
- Copy ptp probing measurement files out of the device;
- Copy firmware image onto the device.

Only secure-FTP is supported, FTP only is not supported.

SFTP connections are only possible via S-FTP capable clients such as FileZilla or WinSCP (the Windows file Explorer does not support S-FTP)

6.5 Network Management System - MOBA-NMS

MOBA-NMS or an NMS of your choice may use SNMPv3 to get and set configuration parameters. Support for DTS 4163 was added in MOBA-NMS version 2.12.1 or later. For instructions please read the manual or help included in MOBA-NMS. For information about SNMP users and credentials, see section SNMP below.

6.6 SNMP

6.6.1 Users

DTS 4163 ships with 2 default SNMP users. Those are needed by MOBA-NMS and should therefore not be removed nor the user names changed, except where NMS is not being used. However, you can freely change the

password, authentication and privacy settings by editing the file `/home/snmp/users`. Only administrators may edit this file.

A valid user entry requires at least a user name, password, authentication and encryption/privacy algorithm. The authentication pass-phrase is used as privacy pass-phrase if this is left empty. Make sure, each user entry is valid according to the following requirements:

user

- starts with a character
- may contain any character [a-z,A-Z] or numbers [0-9],
- no spaces or special characters allowed
- maximum 32 characters long

auth-pass/priv-pass

- minimum 8, maximum 128 characters long
- may contain any character [a-z,A-Z] or numbers [0-9],
- may contain special characters [-,.,_,+,*,=@]
- no spaces or hastags (#) allowed

auth

- any of MD5/SHA/SHA-512/SHA-384/SHA-256/SHA-224
- default is MD5

priv

- any of DES/AES
- default is DES

In order to apply changes, the device can either be restarted or SNMP as service disabled and re-enabled again. Check `snmp.log` in case you encounter issues after having changed the users file.

Make sure to restart SNMP in order to apply user changes.

6.6.2 MIBs

DTS 4163.grandmaster provides 3 MIBs downloadable via S-FTP from `home/snmp/mibs`. This directory contains:

1. MOBATIME-SMI-MIB.mib (Structure of Management Information)
2. MOBATIME-TC-MIB.mib (Textual Conventions)
3. MOBATIME-DTS-4163-MIB.mib (Device MIB)

For the use of SNMP communication tools or none-Mobatime NMS, it is important to load these files in the order presented above.

7 Alarming & Notifications

7.1 Alarming

This device is capable of detecting issues and notifying the user respectively. Issues are categorized into alarms and warnings:

- **Alarms**: System is degraded or becomes unusable if user does not intervene.
- **Warnings**: Irregularity detected, system is fully operational.

Untreated warnings may lead to alarms at some point, which would degrade the system. A degraded system may be for example:

- One of the two redundant power supplies failed: Another failure here would lead to no power to the system.
- Temperature critically high: Even more temperature increase could damage the device or lead to emergency shutdown.
- Synchronization failures, such as not available time source: The device cannot provide accurate time any longer (see holdover for more information).

Currently the following alarms can be set (depends on device firmware):

- POWER_SUPPLY_FAILURE: One of the redundant power supply failed (low or no voltage reading).
- NETWORK_FAILURE: No network link up or redundant network link failure.
- TEMPERATURE_CRITICAL: Temperature readings critically high.
- NO_AVAILABLE_SOURCE: No available synchronization source.
- SOURCE_FAILURE: Active or alternative synchronization source failure.
- SYNCHRONIZATION_FAILURE: Time or frequency synchronization failure.
- PTP_PROBE_TE_ALERT: TE of probed source over the configured limit.
- PTP_PROBE_MTIE_ALERT: MTIE of a probe over the configured limit.
- TEST: Test alarm enabled by user (no system degradation).

The following warnings can currently be set (depends on device firmware):

- RAM_ALMOST_FULL: RAM almost full (reboot suggested).
- CPU_HIGH_LOAD: High load on CPU detected (might by temporary from high network traffic or firmware update).
- PSU_1_NC: PSU 1 equipped but not connected or critically low voltage.
- PSU_2_NC: PSU 2 equipped but not connected or critically low voltage.
- ARBITRARY_TIMESCALE: System timescale is not UTC/TAI but arbitrary e.g. due to manual time set.
- TEMPERATURE_CRITICAL: One or more temperature reading too high/low.
- VOLTAGE_CRITICAL: One or more board voltage reading too low/high.
- SYSTEM_UPDATE_IN_PROGRESS: System update in progress.

7.2 Syslog (Log Server)

A common way to supervise or monitor a network connected device is by collecting and analyzing system log messages. This service is called syslog and can be configured as follows:

1. Set up the device as described in Standard Setup
2. In TUI navigate to *Configuration > Services > Log server 1/2* and set *Enable* to *Yes (1)*.
3. Set at least *Address* to an IP of your choice.
4. Make sure network settings are correct and the address is reachable, then - *Save Changes* -.

High setting for retry count may lead to high CPU usage and possible device failure when address is not reachable.

It is always possible to read the logs directly via CLI or download them via S-FTP.

7.3 SNMP Traps

Your DTS can generate SNMPv2 traps for any sort of event such as set/clear of alarms and warnings, state changes and startup/reboot triggers. Also, alive traps can be enabled to be sent in user defined intervals.

To enable SNMPv2 traps make sure to activate both SNMP as a service and SNMP traps. Also make sure to set a destination address:

1. Set up the device as described in Standard Setup
2. In TUI navigate to *Configuration > Services > SNMP* and set *Enable* to *Yes (1)*.
3. Navigate further into *Traps* and set *Enable* to *Yes (1)*.
4. Set *Destination address 1* or 1 + 2 to an IP of your choice.
5. Select - *Save Changes* - anywhere in the menu to save all the changes made.

In order to change the alive trap interval from default 60s to an interval of your choice, navigate to *Configuration > Alarming* and change *Alive interval* to a desired time in seconds.

Alive interval settings do apply to all notifications/supervision services, not just SNMP.

For more information on SNMP traps see alarming above or read the device MIB (see MIBs).

8 General

General device settings allow you to make system wide changes such as:

- Device name: This name is used as hostname for LAN communication, in syslog to identify the device and many more services.
- Device location and contact: Installation location and responsible technician of the device for user convenience only.
- Timezone: Offset to UTC time affects all time services and depending on your configuration also outputs.
- Redundant PSU mode: If your device offers redundant power supplies, an alarm is thrown when one fails.

System wide changes can only be fully applied after the device was rebooted. Without rebooting after changing the timezone for example, most applications will not realize the new UTC offset. For instance telegrams or time signals with localtime support would still emit UTC even after saving the changes.

Reboot your device after changing the device name or the timezone.

9 Time Handling

In order to synchronize this device properly an adequate time source is required. If a source does only provide a frequency, it cannot be used for initial synchronization. For highest precision and accuracy it is suggested to use GNSS or PTP as primary and secondary sources. Read section Time Source Setup to find out how to select a source.

The table below lists all time and frequency sources available. Server and client column denote this device's perspective as in server = output and client = input:

Source	Time	Frequency	Initial Sync	Server	Client
GNSS	yes	yes	yes	no	yes
PTP	yes	yes[1]	yes	yes	yes
NTP	yes	no[2]	yes	yes	no[3]
ToD In[4]	yes	yes	yes	no	yes
ToD Out[5]	yes	yes	no	yes	no
DCF-CL	yes	yes	yes	no	yes
IN 1+2	no	yes	no	no	yes
OUT 1-5	yes/no[6]	yes	no	yes	no
Oscillator	no	yes	no	no	yes

NTP does not provide precise time, hence a frequency derivation is instable and might be inaccurate. We suggest to not use it as primary time source, but it can act as backup source.

Input 1 and 2 can be used as backup source connected to a PRC such as a G.811 Caesium frequency normal.

Redundancy can be achieved by connecting two or more of this devices together using PTP and configuring one of the PTP master and client instances accordingly.

All the signal outputs and server side sources, such as NTp or PTP servers, are only activated after the device has properly synchronized to a valid time source.

9.1 Core

DTS 4163 core oscillator is a 50ppm TCXO, which represents the internal UTC time. It is constantly synchronized to one of the above mentioned input source via a PLL regulator. Each device ships with an RTC for dated logging during boot. Depending on the device type, your device may be equipped with an additional oscillator for improved holdover.

9.1.1 Oscillator (Holdover)

See device types to check, whether your device offers extended holdover capability. In the oscillator type section are also holdover performances specified.

If this additional oscillator is fitted, it can be used for holdover. Holdover is a mechanism that temporarily maintains a stable frequency of the internal clock, when no other source is available. That mechanism only works, when the device is synchronized to a primary reference time source. The oscillator will be trimmed to that primary reference time source.

[1] Frequency can be derived from time because PTP offers very precise time information.
[2] Frequency derivation from NTP time is very inaccurate which leads to instable signal outputs if used as synchronization source.
[3] Feature will be added in a future firmware release.
[4] Feature will be added in a future firmware release.
[5] Feature will be added in a future firmware release.
[6] Some signals may contain time in some format. See Signal Generators for details.

As soon as no other source is available but the oscillator, the time handler will select the oscillator as last priority to start holdover. As soon as a primary source is locked again, time handler will leave holdover and change back to the primary source to resynchronize.

Drift in holdover (Wander) greatly depends on the environment and synchronization prior holdover. Good and long synchronization (1 month and more) may reduce Wander by many factors. The change back to a primary source occurs in an instance at the moment. A future feature will allow you to choose the speed to get back on track.

The oscillator based holdover is enabled by default but can be disabled as follows:

1. Set up the device as described in Standard Setup
2. Navigate to *Configuration > Time > Core > Oscillator* and set *Enable* to *No (0)*.
3. Confirm your changes with *enter* on - *Save changes* -.

9.1.2 Manual

For testing purposes DTS 4163 allows you to set a time by hand. This manual time set is helpful in situations where no synchronization source such as GNSS or PTP is available but some features or device behavior should be tested. Namely signal outputs will not be activated for as long as the device is not in sync with a primary source.

Once manual time setting is enabled, it overwrites the time handler source selection algorithm by selecting *Manual* as sole time source. Whatever time and source was set previously will be overwritten in an instance. The following steps enable setting time by hand:

1. Set up the device as described in Standard Setup
2. Navigate to *Configuration > Time > Core > Manual* and set *Enable* to *Yes (1)*, but do not save yet.
3. Set desired *Date* and *Time* in a valid format (see below).
4. Select - *Save Changes* - anywhere in the menu to save all the changes made.

By changing the values of *Nanoseconds* or *Frequency* parameters, the device will apply these to the core clock on - *Save Changes* -. This allows you to trim the device manually.

Once you have set the time manually, you cannot resynchronize to a real time source such as GNSS. Disable *Manual*, - *Save Changes* - and reboot the device to regain sync. It is suggested to even reset the device back to factory defaults after testing with manual time.

9.1.3 RTC

The internal RTC is used for dated logging during hot-starts and reboots. This allows for actual UTC timestamps in log messages generated during boot instead of an arbitrary time/date.

This feature cannot be disabled and does not affect the high precision system time. See backup battery for details on valid offline durations.

9.2 GNSS

GNSS is set as default source to synchronize this device. It usually offers best time accuracy with relatively low jitter. Find details about receiver and compatible antennas in the hardware chapter further below.

The receiver supports reception of multiple GNSS at time same time. This can be useful especially in situations, where reception or the opening to the sky is limited. By default, all the satellite systems are enabled and used to tracking time and position.

Settings coming soon.

In bad conditions, it is possible to take more than 10 minutes for a lock on time from a cold start. With the integrated super capacitor, a hot start is possible after about 30 minutes of operation. A hot start remains

possible within about 1 hour of no power delivery to the device. But keep in mind, that the longer the device is powered off, the longer it will talk to sync again.

9.3 PTP

Precision time protocol allows for very precise synchronization through non-deterministic networks.

A DTS 4163 may run multiple PTP instances at the same time, but not on the same interface. It is, however, possible to configure multiple instance on the same interface, but this may in the worst case crash the device. Supported are:

- 4 PTP server instances,
- 2 PTP client instances,
- each on LAN 1-4.

9.3.1 Server

PTP server instances are disabled by default. Each instance has to be used on another LAN port. The following parameters can be set using TUI at *Configuration > Time > Source > PTP > PTP Server X*:

- Enable: 1/yes, 0/no;
- Config file: configuration file located on your device at `profiles/ptp/`;
- Profile: none or one of the supported PTP profiles;
- Interface: LAN 1-4.
- Log level: per instance log level (use Debug with caution, because it increases CPU and flash usage significantly)

Some profiles are not yet fully supported.

Set log level Debug for maximum 1 instance, due to high CPU and flash usage.

The configuration file tells the ptp4l instance what to do (static). But the profile is more of a runtime matter and changes the default behavior acc. to the definition in the standard.

Running multiple PTP instances on the same interface may cause a critical system failure.

Server instances are only started, after the device has been synchronized to a valid time source. Make sure to match the configuration and the profile to ensure correct operation. To debug issues consult the logs at `log/ptp4l/serverX.log`.

Restart the server instance after changing any PTP parameter in the menu or the configuration file.

9.3.2 Client

PTP client instances are disabled by default. Each instance has to be used on another LAN port. The following parameters can be set using TUI at *Configuration > Time > Source > PTP > PTP Client X*:

- Enable: 1/yes, 0/no;
- Stratum: 0-16;
- TE alarm: time error limit to set the alarm in ns;
- Config file: configuration file located on your device at `profiles/ptp/`;
- Profile: none or one of the supported PTP profiles;

- Interface: LAN 1-4.
- Log level: per instance log level (use Debug with caution, because it increases CPU and flash usage significantly)

The stratum value basically imposes a stratum to the server at the other end. So if the DTS 4163 as NTP server should have a stratum of 1, the client stratum value needs to be 0. A stratum 0 source should directly be connected to GNSS.

Some profiles are not yet fully supported.

Set log level Debug for maximum 1 instance, due to high CPU and flash usage.

The configuration file tells the ptp4l instance what to do (static). But the profile is more of a runtime matter and changes the default behavior acc. to the definitions in the standard.

Running multiple PTP instances on the same interface may cause a critical system failure.

Client instances may be used for initial device synchronization and therefore start up immediately after system finished its boot sequence. Make sure to match the configuration and the profile to ensure correct operation. To debug issues consult the logs at `log/ptp4l/clientX.log`.

Restart the client instance after changing any PTP parameter in the menu or the configuration file.

9.4 NTP

Network time protocol version 4 is supported in server and client mode, however it is not recommended to use NTP as time source for its inferiority in accuracy and stability compared to GNSS and PTP.

9.4.1 Server

NTP server is disabled by default. It can be enabled in TUI at *Configuration > Time > Source > NTP > Server*. It is also possible to register 4 multicast/broadcast entires. Without one of these entries set, NTP server only answers to unicast requests on all LAN ports.

NTP multicast mode can be used to extend the scope using IPv4 multicast or IPv6 broadcast with defined span. The IANA has assigned IPv4 multicast address `224.0.1.1` and IPv6 address `FF05::101` (site local) to NTP, but these addresses should be used only where the multicast span can be reliably constrained to protect neighbor networks. In general, administratively scoped IPv4 group addresses should be used, as described in RFC 2365, or GLOP group addresses, as described in RFC 2770.

- IP address: a site local multicast address;
- Interval: 0=auto, $2^{(1-16)}s$;
- Time to live (TTL): number of hops the packet may pass through.

9.4.2 Client

Coming soon.

9.5 ToD

Coming soon.

9.6 DCF-CL

Extension A and B include a DCF-77 current loop input which can be used to connect a GNSS antenna with DCF-CL output, such as the Mobatime GNSS 4500. This source is disabled by default. Following parameters can be set:

- Enable: yes (reception enabled), no (reception disabled);
- TE alarm: time error limit to set the alarm;
- Delay: length of the wire in ns (1ns delay = ~15cm of cable).

LED 4 will indicate received DCF pulses directly from the wire. Make sure you have perfect reception and undisturbed wiring, otherwise the synchronization may fail entirely or fail spontaneously.

9.7 Signal IN

Signal input may be used as backup to a regular time source. A frequency source does not contain time information and therefore cannot be used for initial synchronization. A suitable frequency source would be a ITU-T G.811 capable cesium clock. The following settings can be made per input:

- Stratum: this parameter is used to impose a stratum of the source. The device will have +1 if this source was active.
- TE alarm: limit between source and internal clock to set time error alarm.
- Frequency: input frequency (set this before connecting an input signal).
- Wire delay: to compensate any delay caused be the connected wire; add 1ns for each 15cm of wire.

If the input was deactivated (see `stats/time/signalX.txt`), make sure the frequency configuration matches the actual signal and disable then enable the input again.

A wrong input frequency setting may force the input to deactivate to prevent CPU overload.

10 PTP

The precision time protocol allows for device synchronization with a time accuracy of below 100ns over a LAN. Each node of that LAN needs to be PTP capable, therefore it has to support PTP hardware time stamping. The standard defines multiple types of clocks and mechanisms. DTS 4163 operates as ordinary clock (OC) and supports all mechanisms:

- **Network transport**
  - **L2**: ISO/OSI layer 2 communication (no IP configuration required);
  - **UDPv4**: ISO/OSI layer 3 communication (correct IPv4 configuration required);
  - **UDPv6**: ISO/OSI layer 3 communication (correct IPv6 configuration required);
- **Sync mode**
  - **2-step**: response and delay measurements in separate packets;
  - **1-step**: response and delay measurements in the same packet;
- **Delay mechanism**
  - **E2E**: delay measurements are done between both ends;
  - **P2P**: delay measurements are done between every peer;
- **Message Contracts**
  - **Multicast**: default operation with master detection and BMCA;
  - **Unicast**: allows unicast message contracts based on predefine master table.

For detailed information on PTP operation and mechanisms consult IEEE 1588:2019.

This device is equipped with 4 individual PTP capable network ports (LAN 1-4), all of which support L2 hardware time stamping. Supported is the latest PTP version 2.1 (IEEE 1588:2019, partially supported) and version 2.0 (IEEE 1588:2008, fully supported) in compatibility mode.

10.1 Configuration

This device runs with the latest version of ptp4l. In order for PTP to work, a configuration file is required which may contain all of the parameters described in the ptp4l documentation. Users are advised to read said documentation for help on this topic. Some of the parameters take no effect, because they are managed by the device or set to a fixed value.

Most important parameters to change the mechanics of PTP (synchronization mechanism and layer) are the following:

- **delay_mechanism**: P2P, E2E
- **network_transport**: UDPv4 (default), UDPv6, L2
- **twoStepFlag**: 0 (one-step), 1 (two-step)
- **domainNumber**: 0-255

For additional help and references read the factory configs included on your device.

10.1.1 Create New Config File

On the device

To create a new ptp config, log in as user dts.admin. Multiple ways are available to create a new config:

- Copy and edit an existing config using CLI commands.

- Create new config from default profile via menu.
- Copy and edit a file via S-FTP.

To copy and edit an existing as a custom config, execute these steps:

```
cd /profiles/ptp
cp Default_E2E.cfg custom.cfg
nano custom.cfg
```

The newly created config can also be edited and selected via the menu TUI.

On a PC

- Create a plain text file on the host machine.
- Create the configuration as desired. See section Sample Configuration for details.
- Copy the file onto the device into `profiles/ptp`. See section File Transfer for details.

The new configuration file can now be selected from the menu.

10.1.2 Sample Configuration

```
#
# Default P2P configuration (multicast, 2-step)
#
[global]
domainNumber            0
twoStepFlag             1
network_transport       L2
delay_mechanism         P2P
```

10.2 Profiles

The configuration file tells the ptp4l instance what to do (static). But the profile is more of a runtime matter and changes the default behavior acc. to the definition in the standard. Currently, the following profiles are supported:

- Default PTP (IEEE 1588)
- Default E2E (IEEE 1588)
- Power Utility (IEC 61850-9-3:2016)
- Power (C37.238:2011+2017)

Profile specifics usually include parameter range limitations or even fixed values for some parameters and profiles may also define different operational behavior compared to default IEE 1588 definition. When a power profile is selected apart from the parameter re-definitions, it will append the power TLVs mentioned in said standard. Some details about profile specific configuration parameters can be found in the factory PTP configuration files provided with the device.

More supported profiles follow soon:

- Enterprise
- IEEE 802.1AS:2011
- ITU-T G.8265.1:2014
- ITU-T G.8275.1:2016
- ITU-T G.8275.2:2016

10.3 Probing

Your device offers a PTP probing functionality acc. to ITU-T G.8273 Annex B. A PTP probing instance operates as free-running client and uses GNSS as reference to measure the maximum time interval error MTIE based on dynamic time error dTE (low-pass filtered TE) samples.

Probing only work using GNSS as primary and active synchronization source.

10.3.1 Configuration

For successful probing the device and PTP configuration have to be set correctly.

Use an existing or create a new configuration acc. to Create New Config File in the PTP section. Parameters for a probe could for example be as follows:

[global]	
clientOnly	**1**
free_running	**1**
twoStepFlag	0
logAnnounceInterval	1
logSyncInterval	-7
operLogSyncInterval	-7
logMinDelayReqInterval	-2
network_transport	L2
delay_mechanism	E2E

Make sure parameters clientOnly and free_running are always set to 1.

Once the configuration file is correct, set and enable the probe in the TUI as follows:

1. Navigate to *Configuration > Probing > PTP*
2. Set *Log memory* to *SD*
3. Select the LAN *Interface* to probe on (LAN 1-4)
4. Set a *Name* for the measurement data file
5. Set *Config file* to the desired profile configured before
6. Set State = 1
7. Save Changes

As soon as the device is synchronized probing will start and MOBA-NMS provides a visualization of the measurement data. The measurement data can be accessed via MOBA-NMS or downloaded via S-FTP as described in section File Transfer.

Log memory type can only be set to SD card if your device is equipped with extended storage.

10.3.2 Alarming

It is possible to set |*dTE*| and *MTIE* limits which are continuously monitored and if overstepped, an alarm is set until the measurements are within limits again.

10.3.3 Data Records and Visualization

File Records

Depending on the used PTP configuration/profile, a huge amount of data needs to be collected. Due to limited memory, only devices with an additional integrated memory may use long term probing. The high-resolution probing data is preprocessed in real-time and provided for visualization. This high-resolution data is limited to 10k samples and is not stored permanently in any record. Permanently recorded data offers 1 sample per minute and is CSV formatted as follows:

```
System time [s since UNIX-Epoch], System time [us],
dTE(60s), TEmax(60s) [ns], TEmin(60s) [ns],
MTIE(1s) [ns], MTIE(2s) [ns], MTIE(4s) [ns],
MTIE(8s) [ns], MTIE(16s) [ns], MTIE(32s) [ns]
```

The system time is accurate within a few microseconds, it allows to identify each samples. TEmin(60s) and TEmax(60s) allow for subsequent calculation of MTIE of arbitrary length using Excel or similar tools. The dTE(60s) denotes a mean value of the effective dTE. When your device is equipped with additional memory for probing, it is capable of recording data acquired from at least 1 year of continuous probing.

MOBA-NMS

The Mobatime Network Management System (MOBA-NMS) provides data visualization for the current probing data. It also offers easy accessible data export/download features for any of the probing data files.

In order for NMS to communicate to this device, both SNMP (v3) and SSH need to be enabled. By default, SSH is enabled but SNMP is not. To enable SNMP open TUI and navigate to *Configuration > Services > SNMP* and set enable to yes (1) then - *Save Changes* -.

For more information on the usage of NMS, please consult the help pages in NMS itself.

Webpage [deprecated]

The probing webpage is no longer maintained and will be removed soon, use MOBA-NMS instead.

The measurement data are visualized on a web page. The webpage is available on the local network with the IP address of the device. The web server for this specific webpage provides a self-signed TLS-certificate. Since the certificate is self-signed, the web browser will ask for a confirmation to access the page.
It may be necessary to indicate a tls connection when accessing the webpage as follows:
`https://IP-address`
For more information about the certificate see section Certificates.

10.4 IEC 61850 Conformance

Currently, only the PTP portion of 61850 required protocols is implemented. Others, such as GOOSE or SV will follow soon.

10.4.1 PICS (61850-9-3/8-1/9-2)

Protocol Implementation Conformance Statement (PICS) specifies which IEC 61850 communication services (MMS, GOOSE, SV, etc.) a device supports.

PICS proforma reference	Capability	Value range	Base	Cond.	Support (see Note)
CLOCK_TYPE_OC	clock is OC according to this base	True, False	m	c.1	True
CLOCK_TYPE_TC	clock is TC according to this base	True, False	m	c.1	True

PICS proforma reference	Capability	Value range	Base	Cond.	Support (see Note)
CLOCK_TYPE_BC	clock is BC according to this base	True, False	m	c.1	True
NR_PORTS	number of clock ports (total)	integer > 0	m	-	4
PORTS_STEP	1: all ports support 1-step on egress2: all ports support 2-step on egress3: all ports support both 1-step and 2-step on egress	1..3	m	-	{3}
SLAVE_ONLY	all ports of the clock are slave-only	True, False	m	c.2	False
TIME_TRACEABLE	connectable to a time reference outside of PTP (e.g., GPS)	True, False	m	c.3	True
FREQ_TRACEABLE	connectable to a frequency reference outside of PTP (e.g., GPS)	True, False	m	c.3	True
DAC	doubly attached OC	True, False	o	-	True
PORTS_PAIRED	paired clock ports for redundancy (e.g., 3-4)	identifier pair	o	c.4	{1,2}
REDBOX_DATC	Redbox as TC	True, False	o	c.5	N/A
REDBOX_SLTC	Redbox as Stateless TC	True, False	o	c.5	N/A
REDBOX_TWBC	Redbox as three-way BC	True, False	o	c.6	N/A
REDBOX_DABC	Redbox as DAC BC	True, False	o	c.6	N/A
MIB_SNMP	supports MIB of IEC 62439-3:2016, Annex E	True, False	m	c.7	False
MIB_61850	supports IEC TR 61850-90-4 Clock Objects	True, False	m	c.7	False
MIB_OTHER	clock supports fixed values or a mechanism defined by the manufacturer (if True, this list is appended to this PICS)	True, False	m	c.7	True, void list.
ATOI	supports ATOI TLV as specified in IEC 61588:2009/IEEE Std 1588-2008, 16.3	True, False	o	-	True
PPS	clock has a 1 PPS output	True, False	o	-	True
ACCURACY	Design value of clockAccuracy	nano-seconds	o	-	100 ns
DEVIATION	Design value of Allan deviation	nano-seconds	o	-	4 ns
HOLDOVER	The length of time the clock is expected to stay in clockClass 7, if it is the grandmaster and no longer synchronized to its time reference signal	seconds	o	-	60

Remarks

- Holdover time for clockClass 7 highly depends on the oscillator stability and environment.
- 60s in clockClass 7 is based on a 5ppb oscillator.
- By choosing a Rubidium oscillator, clockClass 7 may be held for more than one hour.

Notes:

- **c.1:** At least one shall be supported (CLOCK_TYPE_OC and CLOCK_TYPE_TC may be both True).
- **c.2:** Only if CLOCK_TYPE_OC = True.
- **c.3:** Only if SLAVE_ONLY = False.
- **c.4:** Shall be “m” (>1) if DAC = True.
- **c.5:** Support shall only be declared if CLOCK_TYPE_TC = True and DAC=True.
- **c.6:** Support shall only be declared if CLOCK_TYPE_BC = True and DAC=True.
- **c.7:** At least one shall be supported.

11 Outputs

11.1 Output 1-5

Outputs 1 through 4 can be individually connected to one of the internal signal generators. Output 5 can only provide analog IRIG-B signals, why it is always connected to the second IRIG generator. Available signal generators are:

- 1 PPS generator (1Hz)
- Frequency generator 1 (2Hz - 10MHz)
- Frequency generator 2 (2Hz - 10MHz)
- Frequency generator 3 (2Hz - 10MHz)
- IRIG generator 1 (IRIG-B/Gxyz)
- IRIG generator 2 (IRIG-B/Gxyz)

Further more, you can select pass-through signals from the following sources:

- GNSS PPS pass-through (PPS output of the internal GNSS receiver)
- IN 1 pass-through (signal input 1 of 1Hz to 10MHz)
- IN 2 pass-through (signal input 2 of 1Hz to 10MHz)
- DCF-CL pass-through (1Hz DCF-CL signal from the DCF-CL input)
- Oscillator 10MHz pass-through (10MHz frequency of the internal backup oscillator)

Signal generators can be configured independently of the outputs themselves. The output has only the possibility to invert the signal from the generator or be disabled/enabled. For generator settings see signal generators section below.

Each output signal can individually be inverted. Default setting (not inverted) will output a rising edge on the 0s crossing. Inverting the output changes this to a falling edge.

11.2 Signal Generators

This device has built in signal generators that can be configured to your needs. Each generator can be assigned to none or any number of outputs 1 to 4. The following generators and signal configurations are available:

Generator	Signals	Parameters	Outputs
1 PPS	1Hz Pulse	enable, pulse width, polarity, cable delay	Out 1-4
Frequency 1-3	2Hz to 10MHz frequency	enable, frequency, polarity, cable delay	Out 1-4
IRIG 1+2	IRIG-m00c [m=B,G; c=0,1,2,3,6,7]	enable, mode, code	Out 1-4
IRIG 2	IRIG-B00c [c=0,1,2,3,6,7]	enable, mode, code	Out 5

IRIG 2 generator is always mapped to output 5. Output 5 can only output analog IRIG-B time codes. So if IRIG generator 2 was set to IRIG-G mode, output 5 will not be able to output any useful signal. Further IRIG knowledge can be found in section IRIG time codes.

Each generator triggers its output signal synchronous to the internal high-resolution clock (accuracy <1n). The different frequencies are generated using numerical dividers. Therefore, the time accuracy is very high, however the signals show higher jitter compared to a real frequency sources such as output from oscillators. Due to the finite nature of computation numbers, e certain frequency error may result when choosing non-twos-complement numbers such as 1’234’567Hz.

The stability and precision of each signal generator/output greatly depends on the active synchronization source.

11.3 IRIG Time Codes

Commonly used codes are:

- IRIG-B007/B127
- IRIG-B004/B124

IRIG codes consists of 1 letter and 3 digits:

- Letter: Rate designator
- 1st digit: Modulation type
- 2st digit: Carrier frequency
- 3st digit: Coded expressions

11.3.1 Rate designator

This device supports only rate B which means 100 PPS and G which is 10’000 PPS.

11.3.2 Modulation type

- 0: DC level shift (DCLS, PWM)
- 1: Sine wave carrier (AM)

11.3.3 Carrier frequency

- 0: no carrier (modulation type 0)
- 1: 100Hz (10ms resolution)
- 2: 1kHz (1ms resolution)
- 3: 10kHz (100us resolution)
- 4: 100kHz (10us resolution)
- 5: 1MHz (1us resolution)

11.3.4 Coded expressions

- 0: BCD, CF, SBS
- 1: BCD, CF
- 2: BCD
- 3: BCD, SBS
- 6: BCD, BCD_Year
- 7: BCD, BCD_Year, SBS

BCD contains:

- day of year
- year
- hours
- minutes
- milliseconds

11.3.5 Usage

This device supports most of these time codes. However, only the coded expression (digit 3) can be configured. Modulation type 0 (DCLS) never has a modulation type (digit 2 = 0) and modulation type 1 (AM) can only be set to output 5, which is optionally available on some extension boards.

11.4 SIMATIC Time

SIMATIC time is a proprietary layer 2 network synchronization protocol by Siemens. It can be enabled on each LAN interface configured in different modes. Currently, only send always is supported.

12 Events

12.1 Switches

Event switches 1 and 2 are smart low-side power switches and are operated on one of the following user selectable triggers:

- Pulse: one pulse-per-second (1PPS) up to a user defined multiple of a second interval; a common signal would be a PPm (pulse-per-minute, 60s interval).
- DCF-77: 1PPS signal with pulse width modulation encoded DCF telegram.
- Flags: user selectable alarm and warning flags that trigger the switch (alarm relay function).
- User: manually set switch state (useful for testing).

Pulse and DCF triggers rely both on the PPS generator. Therefore, enable the PPS generator to have working switches. Both low-side switches are normally open but you can set *invert* parameter to *1/yes* for normally closed operation. Please keep in mind, that an inverted PPS generator also inverts the operation of pulse and DCF triggered event switches.

Event switch triggers 'Pulse' and 'DCF' require the PPS generator to be enabled.

12.1.1 Pulse Trigger

A pulse is made by switching twice, at the start of a second and after a defined pulse width. That switching pulse is repeated in an interval. The pulse can be parametrized as follows:

- Pulse interval: interval in seconds between one and the next start of a pulse (xPPS, where $x \geq 1s$ and $x \leq 86400s$).
- Pulse width: length of the pulse in milliseconds ($10ms \leq \text{width} \leq interval - 10ms$)

Shortest pulse possible is one pulse per second and longest pulse possible is one pulse per day. Pulse activation is synchronized to the start of each minute and always synchronous to the second.

12.1.2 DCF-77 Trigger

Both event switches are capable of outputting a DCF current loop (DCF-CL) signal. DCF is a 1 PPS signal where a single data bit is encoded in the pulse width. The DCF telegram can either include UTC or localtime.

It is not possible to set one switch to DCF localtime and the other to UTC. Switch 2 localtime setting overrides switch 1.

12.1.3 Flags Trigger

DTS 4163 extension features on alarm relay contact. If you need more than one alarm relay, both event switches may be configured to trigger on a specific, all or multiple alarms and warnings.

12.1.4 User Trigger

Use this trigger with the *user state* parameter to close or open the switch manually.

12.2 Time Stamper

An event time stamper can be used for high-precision event logging. Time stamps are triggered by every rising and falling edge detected on the input. Each edge is timestamped with a user define log level and message. Key

features of such a time stamper are:

- Accurate time stamps (time event error < 10us)
- Custom start and stop log messages
- Custom start and stop message severity levels

If the start and stop logic should be inverse, set *invert* parameter to *1/yes*. Log messages will primarily be printed to `log/dtstime/event/event.log` and if log level (severity) was set to at least *Notice*, message will be forwarded to `log/dts.log` and `log/syslog` as well as to a remote syslog server (if configured). Messages are of the form:

```
<DATE/TIME/ORIGIN> <START/STOP SEVERITY>: event: ...
   ...<START/STOP MESSAGE> at <START/STOP EVENT TIMESTAMP>
```

Make sure to configure the time stamper after connecting any wire.

13 Network

All network interfaces may be used for management and are pre-configured with different settings to cover a wide range of situations during initial commissioning (see Standard Setup above for default settings).

When a network cable is plugged in, the speed should be auto-negotiated, if both parties support this feature. In case this fails, the DTS prefers to select 1Gbps full-duplex. Link properties currently cannot be set manually. Using SFP (GBIC) modules, even 100Mbps ones, require auto-negotiation enabled and the speed set to 1Gbps.

Special circumstances may cause a faulty link. In this case, unplug and reconnect the cable or even reboot the device.

Network configuration is based on connection files. To edit or create new connections, you may use a terminal (SSH connection) or any sort of editor on your PC and transfer the file to the device. You may also conveniently use `nmtui` or `nmcli` to edit, create or delete a connection (recommended). Read the Linux man page on `nmcli` for help. Instead of a text editor, you can also edit existing connection files in the menu (save under a different file name to create a new file). If you change a connection file, say `default_lan1`, using `nmtui`, the changes you made are not back ported to the network profiles which are displayed in `dtstui` (this is a future feature).

Using nmcli or nmtui to activate or deactivate a connection supersedes the dtstui settings.

Network configuration is subject to change. Read the Release Notes for noted changes about network configuration.

make sure to use either ‘nmcli‘/‘nmtui‘ or the menu (‘dtstui‘) for network configuration, not both.

Each LAN port maps to an Ethernet device as follows:

Port	Device
LAN 1	eth1
LAN 2	eth2
LAN 3	eth3
LAN 4	eth4
LAN 5	eth0

Note that LAN 5 (available on some extensions) is mapped to *eth0*.

13.1 Hostname

The device’s hostname could be configured using `nmtui` however, please use `dtstui` for that, because otherwise it will not be set persistently. Steps to change the hostname, i.e. the device name, are as follows:

1. Login as `dts.admin` via terminal through SSH or serial connection, type `dtstui` and press the enter key.
2. In the menu navigate to *Configuration > General* and select *Device name*.
3. Enter a valid hostname (see requirements below) and select *Set* to confirm.
4. Select - *Save Changes* - and restart your device by selecting *Maintenance > Device > RESTART_ACTION*.

If a set device name is not valid, LAN configuration, communication and other this may fail. A valid hostname follows these rules:

- 1 to 63 characters long;

- letters from *a* to *z*;
- digits from *0* to *9*;
- hyphens -.

Make sure the hostname (device name) does not contain your domain. Therefore, a valid hostname is *my-time-server* but not *my-time-server.example.com*.

13.2 Create and Activate a Connection

Steps to create a new static IPv4 connection for LAN 1 (eth1) using `nmtui`:

1. Login as `dts.admin` via terminal through SSH or serial connection, type `nmtui` and press the enter key.
2. Select *Edit a connection* and then *<Add>* using the arrow and enter keys.
3. In the *New Connection* wizard select Ethernet and then *<Create>*.
4. Give the connection an appropriate name
5. Navigate down once to *Device*, where you type *eth1* to select LAN 1.
6. Navigate further down to *<Automatic>* of *IPv4 CONFIGURATION* and press the enter key, then select *Manual*.
7. Navigate right to *<Show>* to display the settings.
8. Fill in one or more Address by selecting *<Add...>*, then type an IP with subnet as prefix in the form *192.168.1.1/24*.
9. If necessary add also *Gateway* and *DNS servers*.
10. Navigate down and select whether this connection should *Automatically connect* when a cable is plugged in.
11. Navigate to *<OK>* to save the connection.

Make sure, that only 1 single connection is selected to automatically connect, otherwise the wrong connection might be applied.

See further below for help on ethernet device mapping and IP subnet prefixes.

Steps to do using `nmtui` to activate the newly created connection on LAN 1 (eth1):

1. Login as `dts.admin` via terminal through SSH or serial connection, type `nmtui` and press the enter key.
2. Select *Activate a connection* and then *Ethernet (eth1)* using the arrow keys.
3. Select *Activate* for the connection you just created.
4. Select *<Deactivate>* if an existing connection is already active and should be deactivated.

Newly created or edited connections using ‘nmtui‘ are not yet visible in the dtstui or via file access. This will be implemented in a future release.

13.3 IPv4 Subnet Prefix

IPv4 network masks on this device follow the prefix (bits) syntax:

Class	Prefix	Network mask	Usable hosts per subnet
-	/1	128.0.0.0	2,147,483,646
-	/2	192.0.0.0	1,073,741,822
-	/3	224.0.0.0	536,870,910
-	/4	240.0.0.0	268,435,454
-	/5	248.0.0.0	134,217,726
-	/6	252.0.0.0	67,108,862
-	/7	254.0.0.0	33,554,430

Class	Prefix	Network mask	Usable hosts per subnet
A	/8	255.0.0.0	16,777,214
A	/9	255.128.0.0	8,388,606
A	/10	255.192.0.0	4,194,302
A	/11	255.224.0.0	2,097,150
A	/12	255.240.0.0	1,048,574
A	/13	255.248.0.0	524,286
A	/14	255.252.0.0	262,142
A	/15	255.254.0.0	131,070
B	/16	255.255.0.0	65,534
B	/17	255.255.128.0	32,766
B	/18	255.255.192.0	16,382
B	/19	255.255.224.0	8,190
B	/20	255.255.240.0	4,094
B	/21	255.255.248.0	2,046
B	/22	255.255.252.0	1,022
B	/23	255.255.254.0	510
C	/24	255.255.255.0	254
C	/25	255.255.255.128	126
C	/26	255.255.255.192	62
C	/27	255.255.255.224	30
C	/28	255.255.255.240	14
C	/29	255.255.255.248	6
C	/30	255.255.255.252	2
C	/31	255.255.255.254	0

Search the web for "ip subnet calculator" if you have trouble with subnet prefixes.

13.4 HSR/PRP (Redundancy)

High-Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) are hardware based network redundancy features. Compared to LACP/LAG, HSR/PRP do not just move communication to the inactive link when the primary one is down, they operate permanently on two links, hence seamless switchover is possible. Here you find some insights mainly into configuration and limitations of these network operation modes.

13.4.1 Availability

Normal mode, HSR and PRP are mutually exclusive and available on the network pair LAN 1 + 2.

- **Normal**: Normal/regular network mode active on LAN 1 + 2. Both links can be individually configured as any other LAN port.
- **HSR**: Ring mode is active on LAN 1 + 2. Network configuration and MAC address of LAN 1 are used for both links. HSR frames are sent. PTP operation limited (see below).
- **PRP**: Parallel mode is active on LAN 1 + 2. Network configuration and MAC address of LAN 1 are used for both links. PTP operation limited (see below).

When HSR or PRP is active some features are not available or limited. See limitations further below.

13.4.2 Potential Risks

Configure HSR and PRP in a test environment or with LAN 1 + 2 physically disconnected to prevent any failures.

- Enabling HSR or PRP in any network might disconnect your session. Make sure to use one of the other ports as management interface.
- Enabling HSR in a regular/normal network will loop every single packet which causes the network to be flooded and most if not all service will stop working (similar to a DoS attack).
- Enabling HSR in a PRP network will essentially connect the two very independent networks completely together an destroy the purpose of PRP. Some services or systems may fail.
- Enabling PRP in a regular network might cause strange behavior of this device (services may fail entirely).
- Enabling PRP in a HSR network will break the HSR ring (no redundancy anymore).

Be very cautious when enabling HSR or PRP. Especially HSR is capable of bringing entire networks down.

13.4.3 Network Operation Mode

LAN 1 + 2 operation **mode** can be selected from:

- **Normal/redundancy off**: both LAN 1 + 2 can freely and individually be configured as usual.
- **HSR**: LAN 1 configuration will be used for both links, LAN 2 configuration is ignored.
- **PRP**: LAN 1 configuration will be used for both links, LAN 2 configuration is ignored.

In redundant operation, IP configuration from LAN 1 will continue working as before, however, only the first LAN configuration is operational. Configuration 2 will also be applied to LAN 2 (eth2) but due to the redundancy core, LAN 2 will be bridged and is thus not operational. Link status information from LAN 1 + 2 will be indicated but not accurate nor reliable. Consult the redundant link status instead. Further, the MAC address from LAN 1 will be used also for LAN 2. Hence, all packets sent by this device over LAN 1 + 2 will show the same source Ethernet address (MAC of LAN 1).

Make sure LACP/LAG (IEEE 802.3ad) is deactivated for LAN 1 + 2 before enabling HSR/PRP.

Make sure that LAN 1 + 2 configurations have default routes deactivated (are configured right) if you use LAN 3 or 4 as management port.

Changing network operation mode may require a reboot.

13.4.4 Supported PTP Profiles

The redundant network link may only handle one single PTP instance, server or client. Therefore, only the first PTP instance configured for LAN 1 will be used. All other instances with interface set to LAN 1 or 2 will be ignored.

HSR and PRP redundancy was built for energy and power industry, therefore the PTP power profiles are fully supported, but most other profiles are not supported.

HSR/PRP supported profiles are:

- Default E2E
- Default P2P
- IEC 61850.9.3:2016

- IEEE C37.238:2011
- IEEE C37.238:2017

Not supported profiles are:

- IEEE 802.1AS:2011
- ENTERPRISE
- ITU-T G.8265.1:2014,
- ITU-T G.8275.1:2016,
- ITU-T G.8275.2:2016

Make sure to enable PTP **after** HSR/PRP was enabled.

13.4.5 Limitations

- HSR/PRP operation is not supported using copper GBIC modules (SFP to RJ45).
- Only one single PTP instance may be used on LAN 1 + 2.
- Internally operates always as PTP transparent clock (according to standard)
- PTP configuration parameters are limited (see PTP configuration above for details).
- Network link status must be ignored; consult redundant link status instead.
- LACP/LAG cannot be combined with HSR or PRP.
- Only LAN 1 IP configuration is used, LAN 2 configuration is ignored.
- Allows frame size up to 2044 bytes, but no support for jumbo frames (according to standard).
- Frames are sent independent of the physical link status.
- No QuadBox support or coupling with other HSR or PRP networks.
- Only one VLAN supported.
- LAN 1 + 2 have to have the same link speed.
- The maximum roundtrip time is limited to 400ms; redundant operation will only work with shorter roundtrip times.
- The frame table length is 16’384; redundant operation will only work as long as this table is not full.

Relationship between roundtrip time and frame table length: The longer the roundtrip time and the higher the frame rate, the faster the frame table fills up and redundant operation will not work reliably.

$$roundTripTime = \frac{frameTableLength}{frameRate_{max}}$$

For example, the maximum allowed round trip time in ms for a gigabit per second link speed with an average packet size of 256Bytes would be:

$$16'384 frames * \frac{8 bit/Byte * 256 Byte/frame}{1'000'000'000 bit/s} = 33.55 ms$$

13.4.6 Deviation from Standard

The deviations below apply however, the core is fully compatible with IEC 62439-3:

- No duplicate detection for frames looping in the ring more than once.
- No duplicate accept mode, only duplicate discard.
- No special SAN handling for PRP, sending always to both ports tagged.
- No supervision counters and error counters.
- No node table for supervision.
- No padding between RCT and CRC for PRP allowed.
- No padding of frames when frames are less than 64 bytes after un-tagging or before tagging.
- No wait after reboot.

- No priority queues.
- No bridging mode for PRP.

13.4.7 Frame Size Restriction

According to IEC 62439-3 regarding PRP frame sizes, we read that frame sizes may exceed the MTU settings of an IEEE 802.3 Ethernet device:

> Hence, it is expected that every network component in the LANs supports oversize frames up to the maxValidSize foreseen by ISO/IEC/IEEE 8802-3:2014 plus 6 bytes of RCT (1528 octets).

If you encounter connection establishment issue for example with SSH in PRP mode after a successful key-exchange, an issue with the MTU might be the cause. Your NIC might start the SSH connection establishment with an MTU size smaller than 1500. After the key-exchange the secured connection over the redundant network might include packet sizes beyond 1500 bytes which could then be rejected by your NIC. This is caused by the PRP/HSR redundancy header added to the regular packets. Therefore the “normal” protocol sizes are bigger in a redundant network.

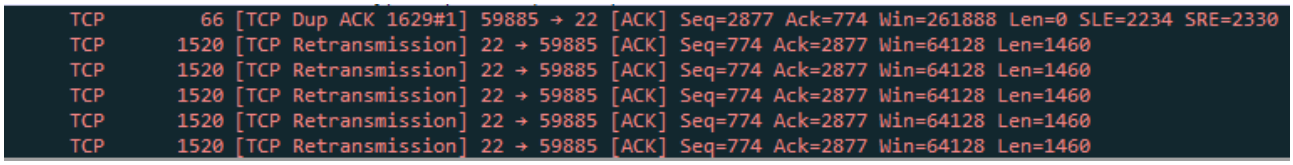

Figure 1: MTU issue over PRP

In the Wireshark record above you see that the packets with sizes exceeding 1500 bytes are rejected by the NIC and then retransmitted by the time server. Using PowerShell on Windows or Shell/Bash on Linux shows us the MTU setting:

```
# Show MTU sizes in Windows PowerShell
PS C:\Windows\system32> netsh interface ipv4 show subinterfaces
   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
  1500                1  855955376  138207911  Ethernet
# Change MTU size of Ethernet in Windows PowerShell
netsh interface ipv4 set subinterface "Ethernet" mtu=1480 store=active

# Show MTU size in Linux Shell
~$ ip link show
eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group de
    link/ether 01:02:03:04:05:06 brd ff:ff:ff:ff:ff:ff
# Change MTU size of eth0 in Linux Shell
~$ sudo ip link set dev eth0 mtu 1480
```

By decreasing the MTU size on the client side, the server will send smaller packets. Typically, the overhead added by redundancy is only 6 bytes (might be greater because it depends on many factors), so it would be enough to reduce the MTU size to 1494 instead of 1480, but it is wise to include some margin.

Instead of reducing the NICs MTU size, you can also simply enable jumbo frame support.

In PRP mode a NIC ought to have jumbo frame support enabled.

13.4.8 Alarm Handling

The “Network failure” alarm indicates that something is not right with your network. Depending on the operation mode, the meaning differs:

- **Normal**: Alarm is active when none of the 5 LAN ports have link status UP.
- **HSR**: Alarm is active when LAN 1 or 2 have link DOWN, different link speed or HSR supervision failed.
- **PRP**: Alarm is active when LAN 1 or 2 have link DOWN, different link speed or PRP supervision failed.

In normal mode the alarm is cleared automatically as soon as any one link is up. In HSR or PRP mode, an admin or operator user has to clear it manually via *Maintenance > Network > RESET_RED_SUPERVISION_FRAMES* or if the automatic supervision frame reset is enabled under *Configuration > Network > Redundancy > Auto reset SVF*, the alarm is cleared automatically after a few seconds given the redundancy is fully restored.

13.5 Protocols and Used Ports

13.5.1 Synchronization Protocols

Protocol	Port	Transport	Notes
NTP (Network Time Protocol)	123	UDP	For regular time sync
SNTP (Simple NTP)	123	UDP	Lightweight version of NTP
PTP (Precision Time Protocol)	319 (event), 320 (general)	UDP	Used in high-precision environments
SyncE (Synchronous Ethernet)	Various	TCP	Typically uses port 990

13.5.2 Secure Shell and File Transfer

Protocol	Port	Transport	Notes
SSH (Secure Shell)	22	TCP	Remote shell access
SCP (Secure Copy Protocol)	22	TCP	Uses SSH
SFTP (SSH File Transfer Protocol)	22	TCP	Uses SSH

13.5.3 Management and Logging

Protocol	Port	Transport	Notes
DHCP (Dynamic Host Configuration Protocol)	67 (server), 68 (client)	UDP	IP address assignment
DNS (Domain Name System)	53, 853	UDP/TCP	Name resolution
LACP (Link Aggregation Control Protocol)	L2 (no port)	n/a	Used with LAG
SNMP (Simple Network Management Protocol)	161 (query), 162 (trap)	UDP	Used for network monitoring
NETCONF	830	TCP	XML-based network config
RESTCONF	443	TCP	REST over HTTPS
HTTPS	443	TCP	Encrypted HTTP
Syslog	514	UDP/TCP	Centralized logging system

13.5.4 Authentication

Protocol	Port	Transport	Notes
RADIUS (default)	1812 (auth), 1813 (acct)	UDP	Default modern ports
RADIUS (legacy)	1645 (auth), 1646 (acct)	UDP	Older implementations
RadSec (Secure RADIUS)	2083	TCP	RADIUS over TLS
LDAP (Lightweight Directory Access Protocol)	389	TCP/UDP	Directory queries
LDAPS (LDAP over SSL)	636	TCP	Secure version of LDAP

14 Security

14.1 Secure by Design

The DTS 4163 is designed from the ground up with a strong focus on security. It meets at least Security Level 2 as defined by IEC 62443-4-2, ensuring robust protection against a wide range of threats.

Key security features include:

- **Secure Boot**: Ensures that only authenticated and trusted firmware is executed, preventing the execution of malicious code at startup.
- **Encrypted Memory**: Protects sensitive data against unauthorized access, even in cases of physical intrusion using advanced tools.
- **Firmware Integrity**: The entire firmware image is both encrypted and digitally signed to prevent tampering. Firmware downgrades are prohibited to avoid reintroducing known vulnerabilities.
- **Protocol Hardening**: Only secure communication protocols are supported; all non-secure protocols are disabled by default.
- **Interface Availability**: Each hardware interface can be disabled to be non-functioning.
- **Regulatory Compliance**: The device is fully compliant with EU Cyber Resilience Act (CRA) requirements.

These measures make the DTS 4163 a secure and reliable choice for modern industrial applications and critical infrastructures.

14.2 Security Updates and Reports

Mobatime offers a service level agreement (SLA) to all end-users, that register their device(s), to establish a way of communicating immediate security threats, security updates and security reports.

14.3 Secure Access

Any remote access method considered unsecure is disabled by default or even not provided at all. Some of the well known remote access methods are as follows:

Method	Secure	Available
SSH	yes	yes
SCP	yes	yes
S-FTP	yes	yes
HTTPS	yes	available soon
SNMP v3	yes[7]	yes (disabled)
SNMP v2 traps	no	yes (disabled)
SNMP v2	no	yes (disabled)
SNMP v1	no	yes (disabled)
FTP	no	no
Telnet	no	no

disabled access methods are available but have to be enabled fist via a secure access method such as SSH. SSH denotes the primary access interface.

A serial terminal (serial over USB) is available as well even though technically not secure, it is enabled by default because physical access to the device is required.

[7] Depends on the chosen authentication and privacy algorithms.

14.4 Certificates

This device provides a self-signed certificate for the webpage with the following credentials:

Parameter	Value
Common Name	www.mobatime.com
Organization	Moser-Baer AG
Organization Unit	Mobatime
Key Type	RSA
Key Size	2048

Your web browser will ask for your confirmation to access the webpage, because a self-signed certificate is used.

A future release will allow dts.admin users to install own certificates.

14.5 Change Password

This devices ships with a one-time password which has to be changed after the first login. Except for `dts.admin` user, all other users have to request a password expiration from an admin. Administrators themselves are able to change all the passwords directly using the command `modify_user`.

14.5.1 dts.admin

1) Login as `dts.admin` with your current password over an SSH connection or the serial terminal.
2) On the CLI type `modify_user` followed by the `tab` key or type `--help` for instructions.
3) To change your password type `modify_user --name dts.admin --password` followed by the desired password.
4) If you choose to expire the password instead, during the next successful login, you will be prompted to enter a new password.

Administrators can change the password of any of the dts users.

14.5.2 dts.operator, dts.info

dts.operator user currently has the possibility to expire all the passwords via *Maintenance > Device > EXPIRE_PASSWORDS*. This feature will either be changed or removed in the future. *dts.info* user has no means to change the password, however, administrator can set a new one or force it expired as follows:

1) Login as `dts.admin` over an SSH connection or the serial terminal.
2) On the CLI type `modify_user --name dts.info --expire`.
3) Type the `enter` key to provoke a password change request for *dts.info* during the next login.

14.6 Lock and Unlock Users

Users can be locked (disabled) or unlocked (enabled) by administrators. By default the device ships with `dts.operator` and `dts.info` users locked. The `dts.admin` user is always enabled. To lock or unlock a user, follow these steps:

1) Login as `dts.admin` over an SSH connection or the serial terminal.
2) On the CLI type `modify_user --name <username> --lock` to lock a user or `modify_user --name <username> --unlock` to unlock a user.
3) Type the `enter` key to confirm the action.

14.7 Audit

Security audits allow administrators to track anything that is done on the system or done to the system. Mobatime offers timely firmware updates, which offer more audit functions. Currently, the security audit contains the following:

- **Logging**: Local log files contain a wast amount of information about what has happened (files in `/var/log`).
- **Status**: A variety of status information shows what is currently happening (command `status`).
- **Syslog**: Two remote syslog servers can be configured to forward log messages to.
- **Login**: Every login attempt is logged, succeeded logins as well as failed ones (command `last` and `lastb`).
- **Notifications**: NMS can be notified about alarms, warnings, status and configuration changes.

15 Maintenance

15.1 Firmware Update

Each stable firmware is released and published on the website mobatime.com. Every firmware comes with these files:

- **133814_DTS4163_MOBA_Vx.y.z_n_date_time_IMG.zip**: firmware archive, contains encrypted images.
- **133814_DTS4163_MOBA_Vx.y.z_n_date_time_IMG.sig**: firmware signature, contains the signature the archive (zip), to make sure no faulty or malicious firmware is installed.
- **Release-Notes-x.y.z.pdf**: a pdf document that contains the release notes for this firmware version.

The release notes you should read prior updating the device, because special update instructions or actions may apply. It contains the following information:

- **Update instructions** for information and changes to the update procedure.
- **Added** for new features.
- **Changed** for changes in existing functionality.
- **Deprecated** for soon-to-be removed features.
- **Removed** for now removed features.
- **Fixed** for any bug fixes.
- **Security** in case of vulnerabilities.
- **Known issues** for bugs that are known but not yet fixed.

Generally, we suggest to perform regular updates for security and stability reasons. However, if your system demands very low down-times it is wise to only perform an update when really necessary. So if a release would only contain new features and minor changes, that are irrelevant to your system, it is probably best to not apply such an update. In terms of security update, we encourage you to apply them as soon as possible, because they may contain fixes for critical vulnerabilities. Also, it is not possible to skip a major release (e.g. jump from 1.x to 3.x) without applying the intermediate releases (e.g. 2.x). This is due to the fact that some settings may change and therefore the device needs to be updated step by step.

To update the device firmware perform the following steps:

1) Copy the new firmware zip and its signature with the same name onto the device using S-FTP or SCP as described in section File Transfer.
2) Ensure the firmware and signature are of the form `133814_DTS4163_MOBA_Vx.y.z_n_date_time_IMG.zip|sig` and stored in directory `home/firmware/`.
3) Open the menu and navigate to *Maintenance > Firmware > Update from FTP*. See section TUI for more information about the menu.
4) After selection the update starts directly and status information is indicated in the status bar of the menu. Also, an `update.log` is written during this process. Do not alter any device configuration while an update is in progress.
5) After a successful update, the device will automatically restart. It may be necessary to restart the terminal for a new session as well.
6) Some device settings may be overridden to default by the update. Make sure to check all relevant settings.

A successful device update takes about 2 minutes to write and 2 minutes to reboot.

It may be necessary to restore device configuration from factory after a firmware update, in order to resolve all bugs and enable all features from a specific firmware update (check release notes for more information).

15.2 Actions

Maintenance actions allow you to actively control the device outside of the configuration. For example, if a service such as SNMP does not react properly or some parameters have changed, you can trigger the SNMP

service restart action which stops SNMP, reapplies the configuration and starts it again. The full list of maintenance actions is the following:

Group	Action	Description
Device	Restart	Reboots the device
Device	Identify	Lets the PSU LEDs blink to identify one among multiple DTS
Device	Clean logs	Removes all log files from the memory (persistent)
Device	Expire passwords	Expires all dts users passwords to enforce choosing of a new password
Device	Test alarm	Set a test alarm flag to test notification services or the relay
Firmware	Update from FTP	Start update process with a firmware provided through FTP or SCP in `home/firmware` directory
Firmware	Update from USB	Start update process with a firmware provided from USB drive in `dts4163/firmware` directory
Configuration	Backup internal	Backup the configuration to internal memory
Configuration	Backup USB	Backup the configuration to an USB drive to `dts4163/<name>/backup`
Configuration	Backup FTP	Backup the configuration to FTP location `home/backup`
Configuration	Restore internal	Restore the configuration and profiles from internal backup location
Configuration	Restore USB	Restore the configuration and profiles from backup location on a USB drive from `dts4163/<name>/backup`
Configuration	Restore FTP	Restore the configuration and profiles from backup location FTP `home/backup`
Configuration	Restore config only	Restore only the configuration from backup location FTP `home/backup`
Configuration	Restore factory	Restore the factory configuration
Network	Reset red. sv. frames	Reset the HSR/PRP redundancy supervision frames to clear network failure alarm
Network	Reset red. frame stat.	Reset the HSR/PRP redundancy frame statistics (RX/TX packet count etc.)
Dump	Logs to USB	Dump all log files to USB drive to directory `dts4163/<name>/dump`
Dump	Support package to USB	Dump all logs, configuration, profiles etc. as archive to `dts4163/<name>/dump`
Dump	Support package to FTP	Dump all logs, configuration, profiles etc. as archive to `home/dump`
Probing	Reset measurement	Reset the current measurement (clean MTIE graph)
Probing	Clean measurement data	Clean all current measurement data (CSV files)
Probing	Clean all	Cleans all measurement data (also CSV files from previous measurements)
Service	Restart SSH	Stops and restarts SSH service (if enabled)
Service	Restart SNMP	Stops and restarts SNMP related services (if enabled)

16 Device Types

The different oscillators, PSUs and interfaces can be distinguished by the device type code which is of the form: 123.456.78

Each digit represents a variation in hardware.

Digit 1: Oscillator
Actual stability may vary depending on the factory date and availability of parts.

Code	Type	Stability	Holdover	Wander[8]
A	TCXO	50 ppm	no	< 5s/d
B	TCXO	2.5 ppm	yes	< 0.3s/d
C	TCXO	500 ppb	yes	< 0.05s/d
D	MEMS	5 ppb	yes (G.813)	< 500μs/d
E	OCXO	1 ppb	yes (G.813)	< 100μs/d
F	DOCXO	0.05 ppb	yes (G.812)	< 5μs/d
G	Rb	0.05 ppb	yes (G.811)	< 1.2μs/d

Drift in holdover (Wander) greatly depends on the environment and synchronization prior holdover. Good and long synchronization (1 month and more) may reduce Wander by many factors.

If holdover duration of a full day is likely in you application, use at least oscillator option D.

Digit 2+3: PSU 1 + 2

- Digit 2: PSU 1
- Digit 3: PSU 2

Code	Nominal Voltage
0	not equipped
A	12-130V DC
B	12-48V DC
C	24-48V DC
D	24-130V DC
E	48-130V DC
G	110-250V DC / 100-240 V AC 50/60Hz

All PSUs are rated for 30W, but the average power consumption is about 15W.

Digit 4: LAN

Code	Interface
C	Copper gigabit Ethernet, RJ45
F	Fiber gigabit Ethernet, SFP

Digit 5: Signals

Code	Interface
C	Copper, BNC 50Ω
F	Fiber, ST 820nm

Digit 6: Cooling

Code	Cooling method
A	Active, long life fan
B	Active, 2x long life fan[9]
C	Passive
D	Passive[10]

Digit 7: Storage

Code	Storage
0	internal memory
S	additional SD card

Digit 8: Extension

Code	Extension
A	Extension with copper output 4
B	Extension with fiber output 4

Apart from output 4, extension A and B include output 5, LAN 5 and the MISC socket (relay, DCF-CL, serial, events).

[9] Optional extended temperature range of -20° to +70°C.
[10] Optional extended temperature range of -20° to +70°C.

17 Hardware Interfaces

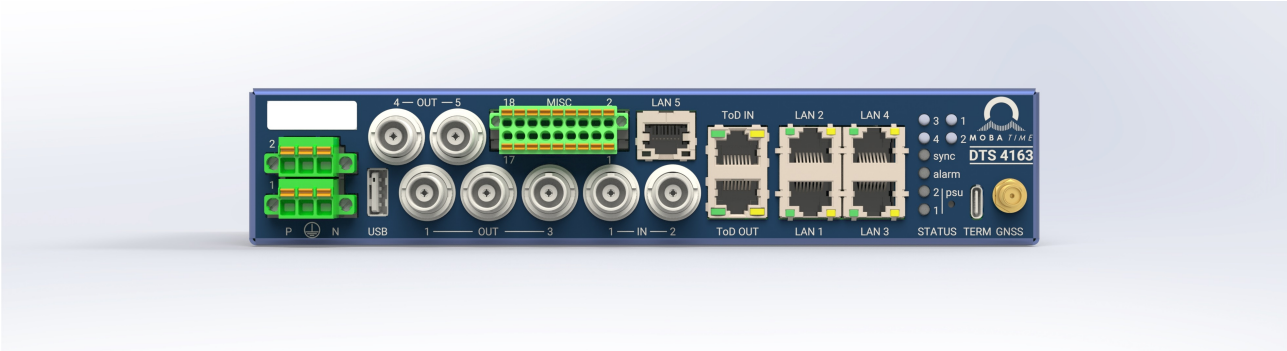

Figure 2: Front view of DTS 4163 with copper interfaces

This section describes all hardware interfaces, their functions and behavior. Not all devices are equipped with the same interfaces, see Device Types for details about your device. Electrical specifications and maximum ratings can be found further below.

Interface	Variants	Availability
PSU 1+2	yes, see device types	always
USB	no	always
OUT 1-3	BNC or ST	always
OUT 4	BNC or ST	extension A/B
OUT 5	no	extension A/B
IN 1+2	BNC or ST	always
MISC	no	extension A+B
ToD IN	no	always
ToD OUT	no	always
LAN 1-4	RJ45 or SFP	always
LAN 5	no	extension A+B
STATUS	no	always
TERM	no	always
GNSS	no	always

The 4 STATUS LED labeled 1-4 are only available with extension A and B.

17.1 Power (PSU)

This device may be equipped with one or two power supply units (see Device Types for details).

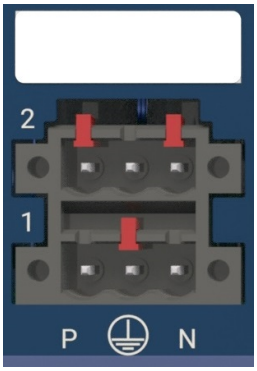

Figure 3: PSU socket of DTS 4163

For pin assignment and maximum ratings read section Power Plug.

Only one PSU with a rated output power of at least 25W needs to be connected for the device to work. It is not allowed to connect 2 too weak PSUs to match the power requirements, because of the featured redundancy mode.

Power supply redundancy mode can be enabled via TUI *Configuration > General > Red. PSU mode*. It offers the following features:

- enables an additional alarm, which is set as soon as one of the PSUs does not deliver enough power;
- enables even wear and tear of the internal supplies by using power of both supplies;
- enables operation in higher environment temperatures (>50°C).

17.2 USB

This USB type A socket supports only USB version 2.0 and can be used for:

- Update: Firmware image upload;
- Backup: Configuration and profiles;
- Dump: Logs, support package;
- External display (optional accessory).

You may plug in a USB memory stick into this USB type A socket. Inserting a USB HDD or similar will not work due to the very limited output power.

USB type A socket is always disabled and when actively used.

17.3 OUT 1-5

Outputs 1 through 4 are digital signal outputs that can be attached to any one of the internal signal generators. Output 5 is an analog signal output which is hard-wired to the IRIG generator 2 and only available with certain extensions (see device type).

Output 5 signal level may be adjustable by the user in a future release. Currently, the output voltage is at a higher level than specified by the standard. Make sure your input device (sink) can handle the voltage. The levels are different depending on the hardware revision:

- Rev. 0 to 1: the level is 10Vpp (+/-5V).
- Rev. 2 and later: the level is 5Vpp (+/-2.5V).

Output 5 signal level may exceed 5Vpp and potentially destroy a sensitive input device.

17.4 IN 1-2

Both signal inputs can be used as backup source for the scenario, where the primary time source would not be available such as due to jammed GNSS reception. Input signals need to meet the following requirements:

- Signal: frequency only (not modulation of data, square or sine wave);
- Frequency: 1Hz up to 10MHz;
- Level difference ($\Delta V = V_{high} - V_{low}$): >1V at 50Ω;
- Resolution: time stamping accuracy of these inputs is 4ns.

17.5 ToD OUT+IN

Coming soon.

17.6 MISC

This socket hosts the following miscellaneous interfaces, which are only available with an extension:

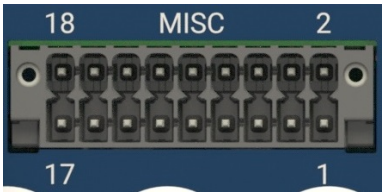

Figure 4: MISC socket of DTS 4163

Interface	Pins (DMC Socket)	Description
EVT SW 2	1 (+), 2 (-/CASE)	Configurable event switch
24V DC	3 (+), 4 (-/CASE)	24V DC output
DCF-CL	5 (+), 6 (-/CASE)	DCF77 current loop input
EVT SW 1	7 (+), 8 (-/CASE)	Configurable event switch
EVT TS	9 (+), 10 (-)	Event timestamper
CASE	11, 12	PE/Case ground
NC	13, 14, 16, 17	Not connected, leave open
ALARM	15 (rel A), 18 (rel B)	Alarm relay contacts, normally open

See section device type for details about available extensions and other hardware configurations.

For a visual pin assignment and maximum ratings read the MISC plug section.

17.6.1 ALARM

Critical infrastructure and legacy systems often use a hardware based alarming and redundancy management, which is often built using relay contacts. This normally open relay contact indicates an alarm when open and no alarm when closed. It is directly coupled to the alarm LED on the front and is triggered by the alarm state of the device.

Altering the alarm mask via TUI, it is possible to disable switching for certain alarms. But keep in mind, that the entire device will ignore a masked alarm, also it would not be logged when masked. For more custom alarm indicators use one of the event switches.

For maximum ratings read the section about the MISC plug. Nominal ratings of the relay:

- DC: 250V, 0.12A (continuous current)

- AC: 250V, 0.12A (continuous current)

17.6.2 24V DC

Extension A and B come with an integrated 24V DC power supply to deliver power to an active DCF-CL antenna such as the Mobatime GNSS 4500. It can also be connected to the event switches to output for example a 24V DCF signal.

Make sure not to add to much load, because it is a week power supply designed to output maximum 100mA (see MISC plug for maximum power ratings).

17.6.3 DCF-CL

Extension A and B include a DCF-77 current loop input, which can be used to connect an active DCF-CL antenna such as the Mobatime GNSS 4500. It is also possible to connect a DCF 4500 antenna, it is however not recommended due to the high jitter of the DCF-77 signal.

Connect the GNSS 4500 antenna to output DCF timecode in UTC time.

The Mobatime GNSS 4500, GPS 4500 and DCF 4500 should all be connected as follows:

Wire	Pin
yellow	3 (+24V DC)
green	4 (GND/PE)
white	5 (DCF-CL+)
brown	6 (GND/PE)

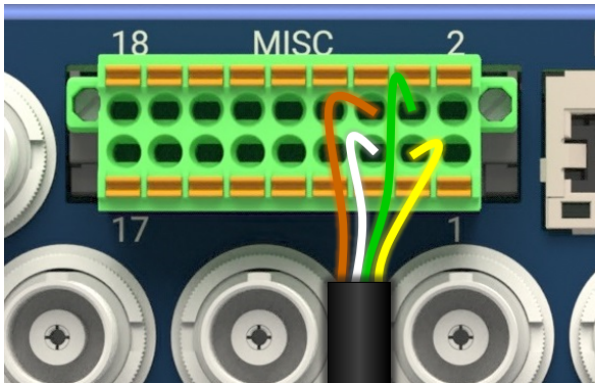

Figure 5: Connection of a GNSS/DCF 4500 receiver

LED 4 will indicate received DCF pulses directly from the wire. Therefore, 59 long and short pulses are visible per minute. If you see a flicker or more pulses than 1 pulse per second, check the cabling and antenna.

For the Mobatime GNSS 4500 antenna, *no reception* will be indicated by single long pulses.

17.6.4 EVT SW 1 + 2

Extension A and B include two event switches which can be used as alarm relay or to create current loop signals such as PPm and DCF. Both are normally open low-side switches and can be connected as follows:

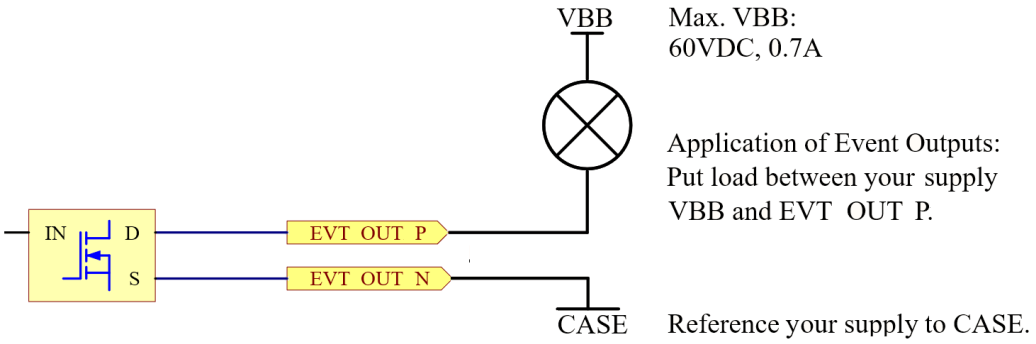

Figure 6: Low-side switch load connection

Normally closed operation can be set by inverting the logic via the menu. Electrical limits, see MISC Interfaces section.

For a powered down device, the switches are always normally open, equal to the alarm relay.

17.6.5 EVT TS

Extension A and B include an event time stamper, which creates a system log message for each detected significant voltage level change. Nominal voltage levels are:

- Low-level: -0.7 to +0.7V
- High-level: > |0.7V|

That timestamper input is built using a full-bridge rectifier. Therefore, it is positive and negative voltage tolerant and not referenced to case ground. Maximum ratings see electrical specifications.

17.7 LAN 1-5

Each LAN port is capable of handling 100Mbps and 1Gbps in full-duplex mode. Link speed auto-negotiation is also supported, but this feature may not succeed with every possible switch available on the market. If it would fail, the port usually choses 1Gbps, full-duplex. All available LAN ports can be used for management (configuration). Following features are supported:

Feature	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
Management	yes	yes	yes	yes	yes
DHCP	yes	yes	yes	yes	yes
NTP server	yes	yes	yes	yes	yes
PTP server	yes	yes	yes	yes	no
PTP client	yes	yes	yes	yes	no
HSR	yes	yes	no	no	no
PRP	yes	yes	no	no	no
LAG	yes	yes	yes	yes	no
VLAN	yes	yes	yes	yes	yes
SyncE	yes	yes	yes	yes	no

LAN port 5 is only available with an extension (see device type).

For details on configuration please read network configuration.

17.8 STATUS

DTS 4163 is not equipped with a display to show status, time or network information. However, an optional USB connected display may be available on request. 4 dual-color LEDs plus 4 optional LEDs (included with extensions) are mounted, which indicate status as follows:

Interface	Description
LED sync	green: synchronized, yellow: time source failure
LED alarm	yellow: waring active, red: alarm active
LED psu 1	yellow: voltage NOK, green: voltage nominal
LED psu 2	yellow: voltage NOK, green: voltage nominal
LED 1	green: event TS indicator
LED 2	green: multipurpose LED
LED 3	green: multipurpose LED
LED 4	green: DCF-CL pulse reception indicator

Some LEDs may also indicate further information by flashing such as the PSU LEDs may alternate colors when you select the device identification action from the maintenance menu.

17.9 RESET

A reset button (not labeled) is available between the STATUS and TERM label, directly underneath the “psu” label. Use a sharp pen or office clip to push the button.

Figure 7: Reset of DTS 4163

This button cannot be used to restore factory defaults, delete or change anything in the device. Pushing the button does cut the power to the entire device for as long as the button is pressed. This comes in handy, if for some reason the device does not behave as it should (for example, if it would not react to a restart command). Be aware that resetting the device by cutting power may corrupt persistent memory. It is possible, however unlikely, that some log files or the user configuration is corrupted by this action. The latter would automatically be fixed during boot, by replacing it with a auto-backup or an internal user backed configuration. In the event, that non of these are available, the default configuration would be loaded instead.

Never press the reset button during a firmware update or while saving any file or configuration changes.

17.10 TERM

The USB type C connector is a serial over USB 2.0 terminal connector. It can be used for adjusting initial configuration or to simply connect when no LAN (SSH) connection is available. Use PuTTY or a similar terminal with the following settings:

- USB Serial Port (COM port on Windows, ttyUSB on Linux)

- Baud rate: 38400
- Data bits: 8
- Stop bit: 1
- Parity: none
- Flow control: XON/XOFF
- VT100 line drawing: enable (PuTTY: *Window > Translation > Enable VT100...*)

Only use an USB 2.0 cable for devices with hardware revision 0. With newer devices you may also use an USB 3.x cable. To read the hardware revision login as any user and find device information via TUI at *Information > Device > HW revision*. `dts.admin` users may also use the CLI by typing `cat help/hardware-revision`.

17.11 GNSS

GNSS is designed to be used as the primary time source. It is also the only source, which is configured to work from factory settings out of the box. This SMA type connector supports only HF antennas and was tested to work with the following antennas:

- PCTEL GPSGL antenna with integrated lightning protection (article 102386)
- Tallysman GNSS antenna (article 126552)
- Tallysman anti-jamming GNSS antenna (article 138203)

Other antennas might also work but are not guaranteed to work. In any case, this GNSS connector always outputs a 5V DC voltage to feed the active antenna.

Since a GNSS antenna usually is mounted outside of a building, always connect the inside of the building using a surge/lightning protector and properly installed earthing cables. Proper mounting terminals, cables, lightning protectors and other accessories are available; please ask your Mobatime sales contact.

We take no responsibility for any damage to life or material caused by your installation.

Working on antenna systems poses risks to life from getting shocked by close high-voltage installations or lightning strokes.

Only a skilled person may install the GNSS antenna, proper Earth ground and the mandatory surge/lightning protection due to the risk of electric shocks.

Ensure adequate safeguards to prevent falling of the building.

Improper use of signal amplifiers may cause damage to the GNSS receiver. Make sure antenna gain of the supported bands are sufficient but do not exceed maximum ratings. The receiver has the following specifications and maximum ratings:

Parameter	Rating
Socket	SMA, female
Rate impedance	50Ω
Output power	5V DC, <100mA
RF input power	13dBm
PPS accuracy	30ns RMS
Sensitivity cold start	-148dBm
Sensitivity tracking	-167dBm
Position accuracy	2m CEP
GPS/QZSS constellation	L1C/A (1575.42MHz)
Galileo constellation	E1-B/C (1575.42MHz)

Parameter	Rating
GLONASS constellation	L1OF (1602MHz + k*562.5kHz, k=-7,. . .,6)
BeiDou constellation	B1I (1561.098MHz)
Receiver type	92 channel u-blox M9 engine

For antenna and cable specifications ask your Mobatime sales or support contact.

18 Mounting Instructions

This equipment is intended to be fastened in place. Instructions on securely fasten the device are given in subsection DIN Rail and 19" Rack below.

Make sure protective earthing is used as a safeguard.

This device is designed for connection to GNSS antennas, which may be installed outside a building. It is the responsibility of the user (skilled person) to ensure appropriate overvoltage protection is implemented according to applicable standards (e.g. IEC 62305). Some countries (like the US and Canada) have additional requirements regarding telecom and antenna connections. The installation shall comply to these requirements.

This equipment is not suitable for use in locations where children are likely to be present.

18.1 Safety Considerations

To comply with the IEC 62368-1 safety standard, the cooling holes must not be oriented upwards. They must be positioned horizontally (sideways), as upward-facing ventilation may increase the risk of electrically induced fires.

To use vertically orientated mounting (cooling holes top to bottom) enclose the device in a certified chamber/housing as a safeguard against flammable materials for protection against electrically caused fires acc. to IEC 62368-1. Make sure the enclosure is vented well enough to prevent overheating (consider device operating temperature).

Regarding the PSU and MISC plug wires: avoid stripping wires in a way that could lead to contact with other components. Install strain reliefs where necessary. Any resulting damage or hazards are not covered by our responsibility.

18.2 DIN Rail

Your device can be clipped to a DIN rail using the optional available DIN rail mounting adapter. Please only use the screws provided with the adapter. The wrong screws, especially too long ones may damage your device internally. This optional DIN rail mounting kit may come with two sets of screws, make sure you use the right (green) ones!

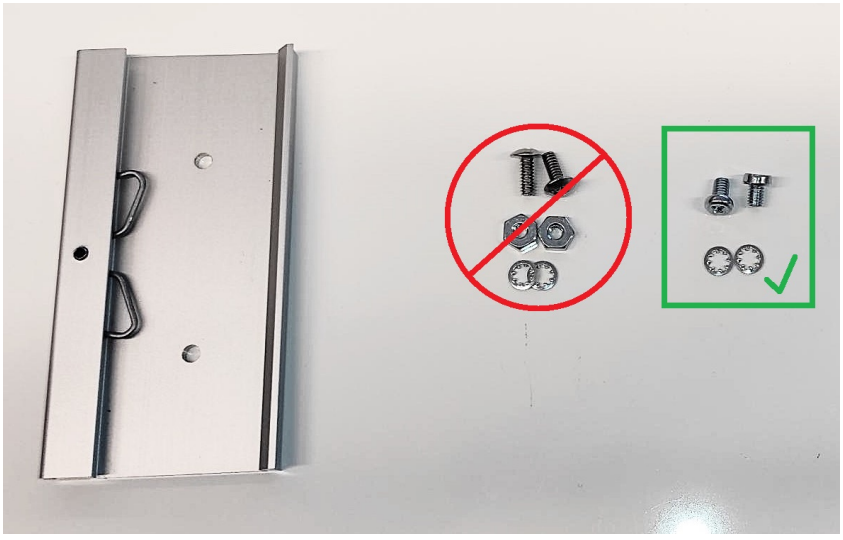

Figure 8: DIN rail mounting kit

Use the following screws and serrated lock washers to mount the adapter to the bottom of your device.

Figure 9: Correct screws to mount DIN rail adapter

When orientating the cooling holes facing upwards (top to bottom), this device does not meet the safety requirements acc. to IEC 62368-1.

The adapter can be rotated in 90° steps. It is **not allowed** to mount this device vertically (green screw holes, cooling holes top to bottom) without adequate safety precautions. Use either pair of the marked holes (green or yellow pair) to screw the adapter to, the green marks are to prefer:

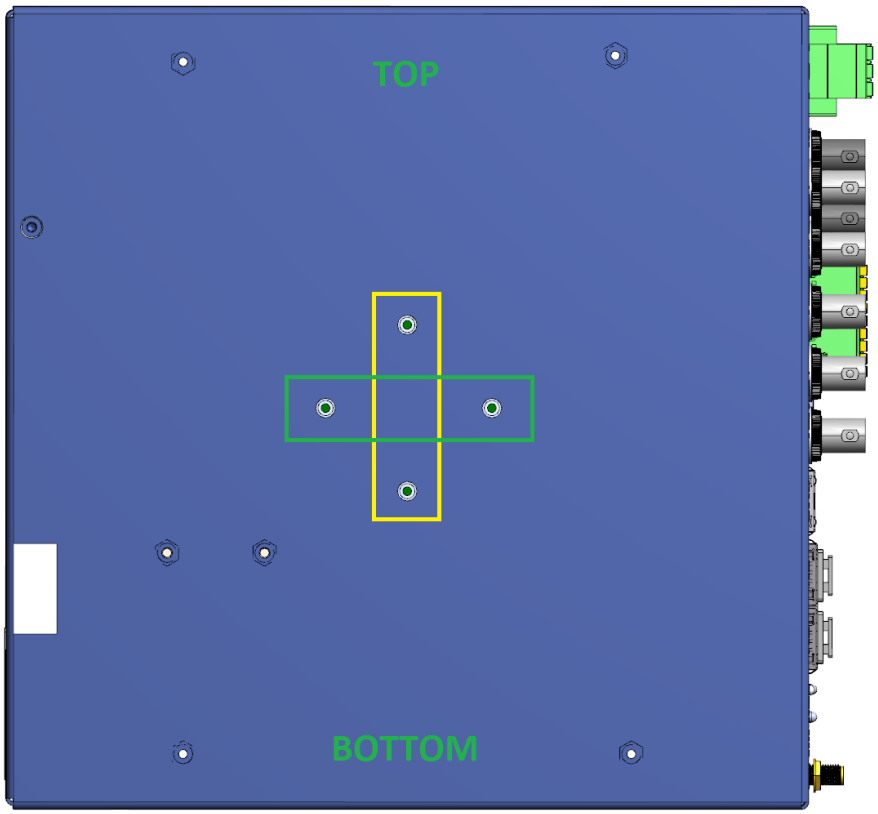

Figure 10: Mounting holes for DIN rail adapter

For passive cooled devices (no fan) it is important to have the cooling holes orientated vertically and not horizontally. For best cooling performance we suggest to orient the device with PSU sockets in upper position as depicted above (green marks) and below:

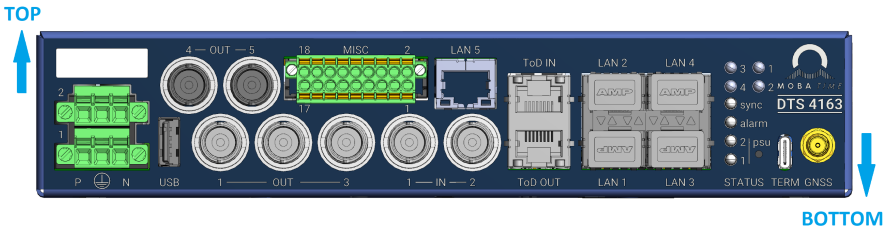

Figure 11: Cooling optimized device orientation, front view

To comply with the safety regulatory (IEC 62368-1) use the yellow marked mounting holes only and read section safety considerations above.

18.3 19" Rack

Your device can be screwed into a regular 19" server rack using the optional available 19 inch rack ears. Please only use the screws provided with the rack ears. The wrong screws, especially too long ones may damage your device internally.

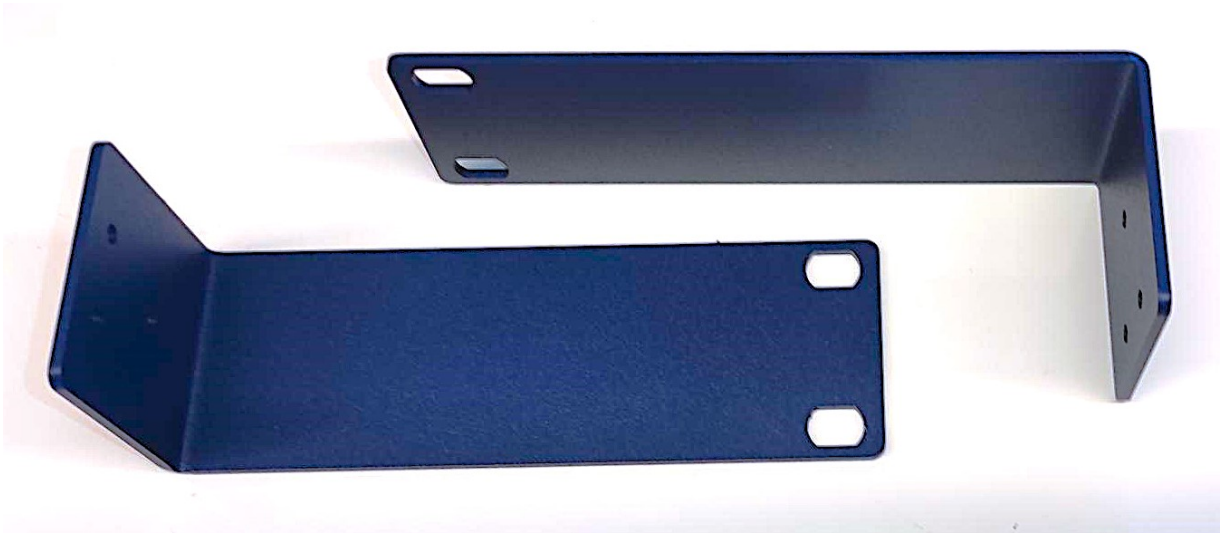

Figure 12: 19inch Rack mounting kit

A rack-mounted DTS 4163 should be equipped with active cooling (option A or B). While the device can operate without fans (options C or D) when installed in a rack, this is not recommended because cooling performance is significantly reduced without proper airflow. However, if you leave one height unit (HU) empty above and below the device and ensure adequate ventilation, the DTS 4163 can still operate within its specified temperature range.

For passive cooled device (option without fan), make sure to leave one HU empty above and below the device.

18.4 Power Plug

This device is a permanently connected equipment that can only be electrically connected to or disconnected from the mains by the use of a screwdriver. Also, an all-pole switch is not provided with the device, therefore and

according to the safety requirements (IEC 62368-1 Annex L), an all-pole switch shall be incorporated in the electrical installation of the building.

An all-pole switch shall be incorporated in the electrical installation of the building.

Required power connectors are provided with the device and comes with the following terminals:

- AC: P=phase, N=neutral
- DC: P=positive, N=negative
- PE: protective Earth terminal

The wires need to be connected as follows:

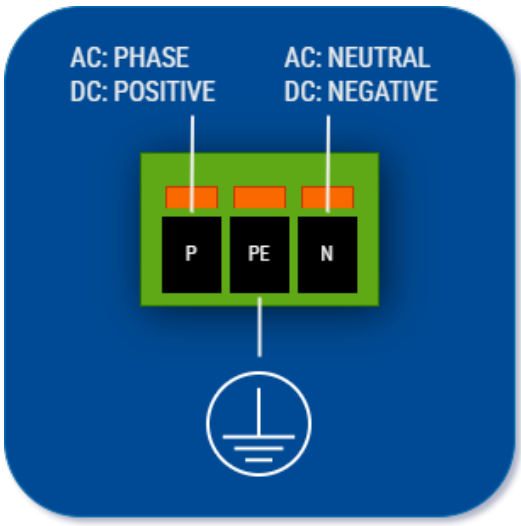

Figure 13: Power Plug

Connecting mains to a DC power supply or the phase/positive pole to the neutral/negative contact may permanently break the device.

The rated power is indicated on the front of your device.

Your device ships with the necessary plugs, but you may choose to use an alternative type matching the socket. Please be advised that only original plugs may be used (vendor is Phoenix Contact):

- Socket: CCDN 1734452
- Plug: FKCN 1732975

Avoid stripping wires in a way that could lead to contact with other components. Make sure to attach strain reliefs to relieve the connection points of cables and lines from mechanical stress. The plug should be screwed tight to the socket to lock it in place, which is important to prevent accidental loosening of the plug.

We accept no responsibility for any damage to persons or property resulting from the use of plugs other than those provided, or from faulty or unsafe wiring.

Make sure all wires are disconnected from live voltage before handling them.

Always connect the protective Earth terminal as a safeguard.

18.5 GNSS Antennas

Two sockets for GNSS antennas are available:

- GNSS: SMA terminal for a HF GNSS antenna;
- MISC (pins 3-6): MISC socket (see below) for a GNSS/GPS antenna with DCF-CL output.

This device is designed for connection to GNSS antennas, which may be installed outside a building. The installation of external circuits must be carried out by a skilled person in accordance with applicable safety and grounding standards.

To ensure safe operation and compliance with IEC 62368-1, surge protection and grounding must be implemented.

Working on antenna systems poses risks to life from getting shocked by close high-voltage installations or lightning strokes.

Only a skilled person may install the GNSS antenna, proper Earth ground and the surge (lightning) protection due to the risk of electric shocks.

Ensure adequate safeguards to prevent falling of the building.

We take no responsibility for any damage to life or material caused by your installation.

18.5.1 Surge Protection

Appropriate over-voltage and lightning protection must be installed to protect the device and connected equipment from transient over-voltages, including those caused by lightning strikes.

The surge protection equipment should comply with IEC 62305 (Protection Against Lightning) and other relevant standards. Some countries (like the US and Canada) have additional requirements regarding telecom and antenna connections. Make sure to follow your local safety requirements and standards.

Proper surge (lightning) protectors are available; please ask your Mobatime sales contact.

18.5.2 Grounding

Proper grounding of the antenna system must be ensured to prevent potential differences and hazardous voltages on connected cables. Make sure to follow your local safety requirements and standards.

18.6 MISC Plug

This device may be equipped with extension A or B (see Device Types for details), which offer a multipurpose connector. Pin assignment for this plug is as follows:

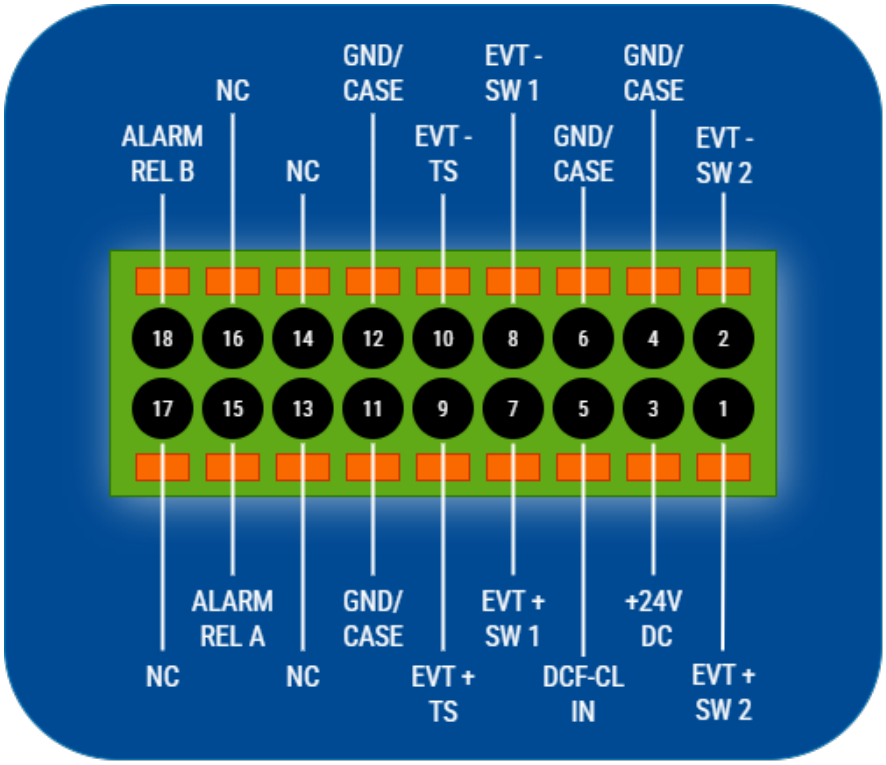

Figure 14: Misc Plug Rev02

Some features may not be functional or function differently, depending on the revision of your device.

Your device ships with the necessary plug, but you may choose to use an alternative type matching the socket. Please be advised that only original plugs may be used (vendor is Phoenix Contact):

- Socket: DMC 1787085
- Plug: DFMC 1790360

Avoid stripping wires in a way that could lead to contact with other components. Make sure to attach strain reliefs to relieve the connection points of cables and lines from mechanical stress. The plug should be screwed tight to the socket to lock it in place, which is important to prevent accidental loosening of the plug.

We accept no responsibility for any damage to persons or property resulting from the use of plugs other than those provided, or from faulty or unsafe wiring.

Make sure all wires are disconnected from live power before handling them.

Always connect the CASE pins to protective Earth terminal as a safeguard.

18.7 Other Plugs

All other sockets but the power and MISC sockets carry only logical signals with low-voltage and low-power. Those sockets may be connected and disconnected at any time, even when the device is powered already. Use cables with the following minimal requirements as applicable:

Interface	Cable
USB	none (USB memory stick only)
OUT 1-5	RG58 (or similar) cable with BNC male plug
IN 1-2	RG58 (or similar) cable with BNC male plug
ToD IN/OUT	straight CAT5 (or higher) Ethernet cable with RJ48/RJ45 plugs
LAN 1-5	straight CAT5e (or higher) Ethernet cable with RJ45 plugs
TERM	USB 2.0 cable with USB-C to USB-A or to USB-C type plugs
GNSS	RG58 (or better) cable with SMA male plug

19 Electrical Specifications

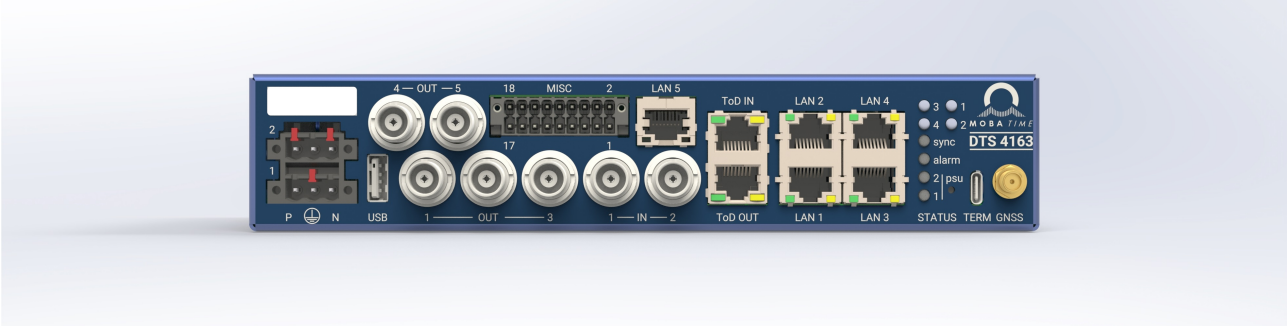

Figure 15: DTS 4163 interfaces

19.1 Interfaces

Below table shows the maximum ratings of each featured interface:

Interface	Socket	Voltage	Current	Length
PSU 1+2	CCDN	see PSU ratings	input	N/A
USB	USB-A, 2.0	+5V DC	<350mA output	<5m
OUT 1-4	BNC, 50Ω	TTL 5V DC	<50mA output	<30m
OUT 5	BNC, 50Ω	<10V DC	<50mA output	<30m
IN 1+2	BNC, 50Ω	TTL 5V DC	<50mA input	<30m
MISC	DMC	see MISC Interfaces	-	<30m
ToD IN	RJ48	<7.0V DC	<8mA input	<30m
ToD OUT	RJ48	<5.5V DC	<150mA output	<30m
LAN 1-4	RJ45, SFP/GBIC	+/-2V diff.	<20mA output	<100m, <10km
LAN 5	RJ45	+/-2V diff.	<20mA output	<100m, <10km
TERM	USB-C, 2.0	+5V DC	<10mA input	<5m
GNSS	SMA, 50Ω	+5V DC	<100mA output	>30m [11]

Some of the listed interfaces may only be available with an extension. Fiber based networks may extend in length to about 10km. Do not use stronger GBIC modules due to the power limit. RJ45 Ethernet connections with speed lower than 1Gbps may exceed distances of 100m but operation over such distances is not guaranteed.

19.2 MISC Interfaces

Your device may be equipped with extension A or B (see Device Types for details), which offers a multipurpose connector. Its interfaces ratings are as follows:

Interface	Pins (DMC Socket)	Voltage rating	Current rating	Length
EVT SW 2	1 (+), 2 (-/CASE)	<60V DC	<0.7A switch	<30m
24V DC	3 (+), 4 (-/CASE)	24V DC, +/-2%	<250mA output[12]	<100m
DCF-CL	5 (+), 6 (-/CASE)	<24V DC	<100mA output	<100m
EVT SW 1	7 (+), 8 (-/CASE)	<60V DC	<0.7A switch	<30m
EVT TS	9 (+), 10 (-)	<+/-60V DC	<150mA input	<30m

[11] depends on the HF antenna and cable used. Cable may also be shorter, but make sure maximum signal strength does not exceed 15dBm.
[12] Extension A/B revision 0-1 offer 2W and revision >1 6W power.

Interface	Pins (DMC Socket)	Voltage rating	Current rating	Length
CASE	11, 12	N/A	N/A	N/A
NC	13, 14, 16, 17	N/A	N/A	N/A
ALARM	15 (rel A), 18 (rel B)	<250V AC/DC	<0.12A constant	<30m

Some features may not be functional, depending on the revision of your device.

19.3 Power Supply Ratings

The required voltage and power/current for the specific variant of the DTS 4163 is indicated by a sticker on the device above the power plug. See also Device Types for nominal power ratings.

Nominal ratings are as follows:

Code	Nominal Voltage	Allowed Voltage Range	Power Rating
A[13]	12-130V DC	+/- 10%	30W (<2.5A)
B[14]	12-48V DC	+/- 10%	30W (<2.5A)
C	24-48V DC	+/- 10%	30W (<1.3A)
D[15]	24-130V DC	+/- 10%	30W (<1.3A)
E	48-130V DC	+/- 10%	30W (<0.7A)
F	110-250V DC / 100-240V AC 50/60Hz	+/- 10%	30W (<0.3A)

Inrush currents will exceed the rated current in the power rating column.

Power supply units may fail permanently if operated outside of the nominal voltage ratings.

19.4 Backup Battery

DTS 4163 is not equipped with a backup battery, however it is equipped with a super capacitor to allow hot-starts (short time until operational).

Hot-starts are possible at least during the first 20 minutes after power loss, but depending on the environment hot-starts may be possible far beyond.

19.5 Interface Protection

Every interface is adequately protected against common faults, user caused or environmentally caused.

- The entire device offers **thermal** protection; for more information see section environment.
- **Shielded** interfaces usually offer good signal protection due to high electromagnetic immunity (EMI).
- **ESD** protected interfaces can be touched by the user in a non electrostatic discharge (ESD) protected environment.
- Outputs are usually **overload** and **short circuit** protected to allow user manipulation errors.
- **Overvoltage** protection for continuous faults. It is limited to usually 4 times the nominal input voltage.

[13] PSU option has internal certification only.
[14] PSU option has internal certification only.
[15] PSU option has internal certification only.

Interface	Thermal	Shielded	ESD	Overload	Short circuit	Overvoltage
PSU 1+2	yes	no	yes	n/a	n/a	yes
USB	yes	yes	yes	yes	yes	no
OUT 1-4	yes	yes	yes	yes	yes	no
OUT 5	yes	yes	yes	yes	yes	no
IN 1+2	yes	yes	yes	n/a	n/a	no
ToD IN	yes	yes	yes	n/a	n/a	no
ToD OUT	yes	yes	yes	no	yes[16]	no
LAN 1-5	yes	yes	no[17]	yes	yes	no
TERM	yes	yes	yes	n/a	n/a	no
GNSS	yes	yes	yes	yes	yes	no
24V DC	yes	no	yes	yes	yes	no
DCF-CL	yes	no	yes	n/a	n/a	no
EVT SW 1+2	yes	no	yes	n/a	n/a	yes
EVT TS	yes	no	yes	n/a	n/a	yes
ALARM	yes	no	n/a	n/a	n/a	no

Inputs and bidirectional interfaces should be used and connected with special care.

Interface protections should not be stress tested, because your device may take permanent damage.

[16] partial short circuit protection (1 driver at a time)
[17] robust design offers partial protection

20 Technical Specifications

20.1 Boot Time

Action	Time to login	Time to sync (GNSS)	Time to sync (PTP)[18]
Factory start	~4min	>7min	>5min
Cold-start	~2min	>5min; <16min	<3min[19]
Hot-start	~2min	~3min	<3min
Restart	~3min	~4min	~4min

Hot-starts are available after about 10 to 30 minutes of continuous synchronization to GNSS or PTP. With each minute passes while the device is powered off, synchronization (hot-start) time increases. Best hot-start performance shows a reboot.

Never interrupt a factory boot, otherwise your device may permanently fail.

20.2 Mechanical Data

Dimensions housing (W x D x H)	221.5 x 222 x 44mm
Dimensions rack (W x D x H)	484 x 222 x 44mm
Dimensions DIN rail (W x D x H)	221.5 x 222 x 52mm
Weight (fully featured)	~2.5kg

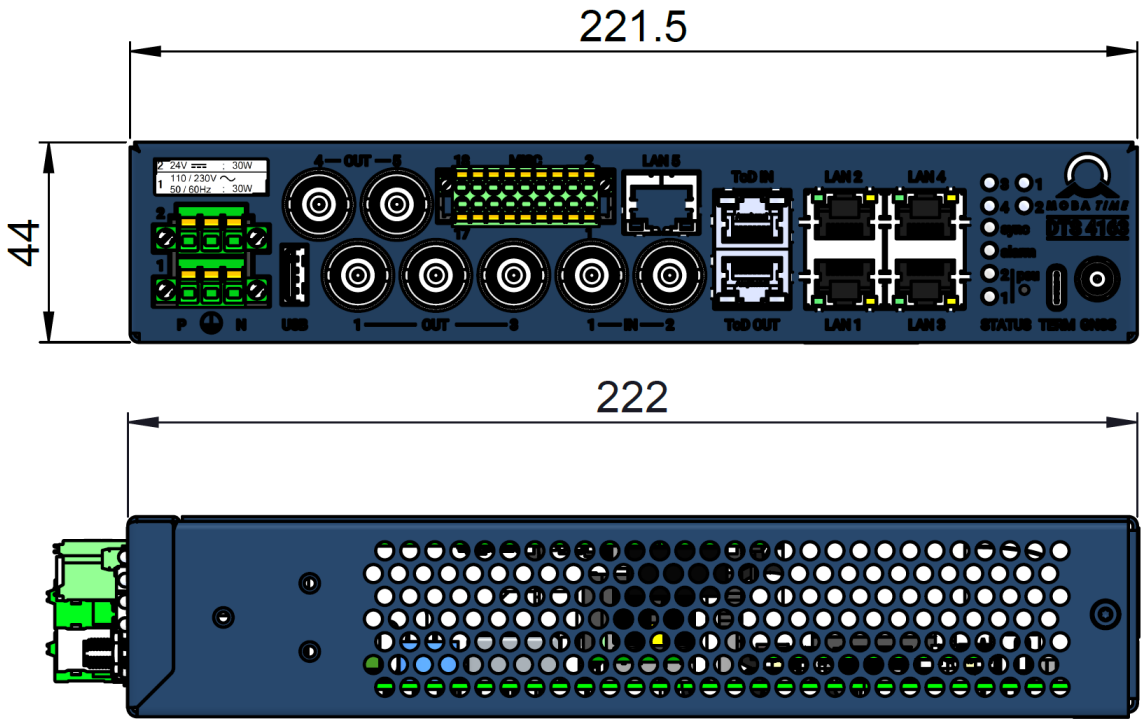

Figure 16: Housing dimensions without mounting adapters

[19] Cold-start time to sync for passive cooled device may take several minutes longer depending on the temperate of the device.

20.3 Environment

Storage temperature	-20° to +90°C
Operation temperature	0° to +50°C[20]
Relative humidity	5 to 95% (non-condensing)
Operation altitude	<2000m above sea level

Your device is equipped with protective circuitry to prevent overheating. This system ensures the longevity and safe operation of internal components. Most electronic parts are rated for a maximum operating temperature of 85°C, while internal device temperatures typically exceed external temperatures by at least 15°C. As a result, the device may function at ambient temperatures above 50°C.

If any critical temperature reading exceeds 85°C, the device will enter over-temperature mode until temperatures return to a safe range. In this mode, power is cut to all major components, including the CPU and interfaces, while only the protective circuitry and cooling system remain active.

High device temperatures decrease MTBF and may even permanently damage components.

Make sure your device is sufficiently cooled.

20.4 Operation

MTBF	250’000h
Expected lifetime	>10 years

Both MTBF and expected lifetime are estimates and expect a temperature regulated (22°C) and low-level radiation contaminated environment in a altitude below 2000m a.s.l.. For harsher environments the numbers likely decrease, especially when operated in high temperatures (>35°C).

[20] Optional extended temperature range is -20° to +70°C.

21 Compliance

21.1 EMC and Safety

Your device is compliant to following standards and EMC certified[21] as well as safety certified[22]:

- IEC 61000-6-2:2016 (EMC)
- IEC 61000-6-4:2018 (EMC)
- IEC 61000-3-2:2018 (EMC)
- IEC 61000-3-3:2013 (EMC)
- IEC 61000-3-3:2013/AMD1:2017 (EMC)
- IEC 62368-1 (safety)

This device fulfils the **IEC 61850-3:2013** requirements for an in-field IED, which are coved by the following IEC standards:

- IEC 61850-3:2013
- IEC 61000-3-2:2018/AMD1:2020
- IEC 61000-3-2:2018/AMD2:2024
- IEC 61000-3-3:2013/AMD2:2021

This device also fulfils the **national differences** for the following countries:

- CH
- AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SI, SK
- UK
- AU, KE, NZ, MY
- IL, IN, RS, SG
- AR, CL, CN, ID
- RU, TH, TR, UA
- UY, ZA, HK
- KR, SA, PE
- US, CA
- TW, CO
- JP
- BR, MX

National differences were tested and the device is compliant with the following standards:

- EN 61000-6-2:2005*
- EN 61000-6-2:2005/AC:2005*
- EN IEC 61000-6-2:2019
- EN 61000-6-4:2007*
- EN 61000-6-4:2007/A1:2011*
- EN IEC 61000-6-4:2019
- EN 61000-3-2:2014*
- EN IEC 61000-3-2:2019
- EN IEC 61000-3-2:2019/A1:2021
- EN IEC 61000-3-2:2019/A2:2024
- EN 61000-3-3:2013*
- EN 61000-3-3:2013/A1:2019
- EN 61000-3-3:2013/A2:2021
- EN 61000-3-3:2013/A2:2021/AC:2022-01
- ETSI EN 301 489-1 V2.2.3 (CENELEC)

[21] EMC certificate number is DE-6-G5241599.
[22] Safety certificate number is DE-6-T2501100.

- ETSI EN 301 489-19 V2.2.1 (CENELEC)
- 47 CFR Part 15 Subpart B (US)
- ICES-003 Issue 7 (CA)

21.2 Time

Time related services, signals and general time handling comply with:

- ITU-T G.8271 (time and phase synchronization)
- ITU-T G.8272 (timing of PRTC)
- ITU-T G.813 (timing of slave clocks)
- ITU-T G.812 (timing of slave clocks)
- ITU-T G.703 (1PPS)

Specifically PTP services are compliant with:

- IEEE 1588:2008/2019 (PTP)
- IEEE C37.238:2011/2017 (power profiles)
- IEC 61850-9-3:2016 (power utility profile)
- IEC 62439-3:2021 (HSR+PRP)
- ITU-T G.8261-64 (timing and synchronization)
- ITU-T G.8273 Annex B (PTP probing)
- ITU-T G.8275.1 (telecom profile)
- ITU-T G.8275.2 (telecom profile)
- ITU-T G.8265.1 (telecom profile)

21.3 Networking

Implemented LAN related standards are the following:

- IEEE 802.1ad/Q (VLAN/bridging)
- IEEE 802.1p (QoS)
- IEEE 802.3ad (LACP)
- RFC 2865 (RADIUS)
- RFC 6020 (YANG model)
- RFC 6241 (Netconf)
- RFC 7950 (Yang)
- RFC 5424 (syslog)

21.4 Others

- RoHS

22 Specification Summary

Time and Frequency Reference Inputs

Interface	Reference (as client)	Summary
GNSS	Multi GNSS RF antenna	GPS, Galileo, GLONASS, BeiDou, 92 channels, -167dBm tracking sensitivity
LAN 1-4	PTP 2.0 and 2.1	E2E, P2P, 1-step, 2-step, multicast, unicast, power utility, telecom
LAN 1-5	NTP	coming soon
DCF-CL	GNSS-4500 receiver	GPS, Galileo, GLONASS
IN 1+2	Frequency signal	1 PPS, 2Hz to 10MHz, square wave
ToD IN	1 PPS and serial telegram	coming soon

Time, Frequency and Signal Outputs

Interface	Reference (as server)	Summary
LAN 1-4	PTP 2.0 and 2.1	E2E, P2P, 1-step, 2-step, multicast, unicast, power utility, telecom
LAN 1-4	SyncE master	coming soon
LAN 1-5	NTP	stratum 0 server, multicast, unicast, 8s interval
OUT 1-4	Frequency and time signal	1 PPS, 2Hz to 10MHz, IRIG-B/G, square wave
OUT 5	Time signal	IRIG-B AM, IRIG-B127, IRIG-B124
ToD OUT	1 PPS and serial telegram	coming soon
Serial 1+2	Serial telegram	coming soon
EVT SW 1+2	Frequency and time signal	pulse-per-minute, 1 PPS, DCF-CL

Management, Alarms and Notifications

Interface	Protocol	Summary
LAN 1-5	SSH, SNMPv1-3, HTTPS, NETCONF, Syslog	Device management, supervision, data transfer
TERMINAL	USB-Serial	Device management, 38400/8/1/none, VT100 line drawing
ALARM	LED, Relay	Device alarm indication
EVT TS	Log, Syslog	Precision fault detection and logging

Protocol and Signal Accuracies

Signal/Protocol	Accuracy	Precision
GNSS	<+/-50ns	4ns
PTP	<+/-50ns	4ns
NTP	<+/-50μs	100μs
DCF-CL	>+/-100ns	100ns
1 PPS	<+/-50ns	4ns
2Hz-10MHz	<+/-50ns	4ns
IRIG-B/G	<+/-50ns	4ns
IRIG-B AM	<+/-100μs	100ns
ToD	<+/-50ns	4ns
EVT TS	<+/-10μs	10μs

Signal/Protocol	Accuracy	Precision
EVT SW	<+/-10μs	10μs

Clock Stability and Wander

Type	Stability	Wander
A (TCXO)	50 ppm	< 5s/d
B (TCXO)	2.5 ppm	< 0.3s/d
C (TCXO)	500 ppb	< 0.05s/d
D (MEMS)	5 ppb	< 500μs/d
E (OCXO)	1 ppb	< 100μs/d
F (DOCXO)	0.05 ppb	< 5μs/d
G (Rb)	0.05 ppb	< 1.2μs/d

23 FAQ - Common Issues

Q: SSH connection establishment fails over the redundant LAN?
A: Maximum MTU size of your NIC might reject the packets because their size is increased with a redundancy overhead to more than the MTU size. See network redundancy chapter above for more details on this.

Q: Where do I find the changes from one to another firmware?
A: Each firmware image provides release notes. These are available for download on our website mobatime.com. Or read them in markdown format which is provided within the firmware zip or after updating accessible via TUI under help.

Q: Why does network redundancy (HSR/PRP) not work properly using 10/100/1000Mbps SFP modules?
A: This is a known limitation; HSR/PRP redundancy only works using native Ethernet (copper, RJ45) or native fiber optical connections. Use fiber optical GBIC modules instead of copper RJ45.

Q: Why does my device reboot after enabling a PTP instance on LAN 1 or 2.
A: This is a known and resolved issue; please update your device to the latest firmware.

Q: Why does update.log not contain the entire update process?
A: This is known and by design the case. Firmware version 2.0.0 changes the update procedure, which allows you to see the entire update process in the update.log.

Q: Why is update.log not visible or empty?
A: A known bug may lead to wrong file permissions. Reboot the device and the permissions will be set correctly.

Q: Why did the device not reboot after an update?
A: Device update may have failed; check update.log for details.

Q: Why does device status show “reboot canceled”?
A: This is a known and resolved issue; please manually reboot the device via the reset button or power cut and update your device to the latest firmware.

Q: How can I check the state of synchronization or any other status?
A: Open TUI, navigate to Status and select time or any other file.

Q: Why do I see different directories and files when logged in as dts.admin over serial compared to SSH connection?
A: This is a known and resolved issue. Execute `cd /jail/home/` to reach the correct home directory and please update your device to the latest firmware.

Q: Why can probing measurements not be deleted?
A: This is a known and resolved issue; please update your device to the latest firmware.

Q: Executing `trace` or `route` prints error “command not found”, why?
A: This is a known and resolved issue; please update your device to the latest firmware.

Q: Executing `reboot` or `shutdown` prints an error message and does not reboot, why?
A: This is a known issue and can be resolved with an update. However, you can reboot using TUI or the reset button.

Q: My SSH connection does not behave properly or not the same on all LAN ports, what reasons could there be?
A: None of the LAN ports support PoE (power over Ethernet). PoE capable switches (depending on their port configuration), may interfere with the Ethernet link and cause connection break-downs or cause auto-negotiation of link-speed to fail. Make sure the device is connected to only non-PoE ports.

Q: Why does my SSH connection get timeouts from time to time?
A: This might be a routing issue. Make sure to have only a single IP subnet match a single port. Also, add static routes where needed. Configure correct gateway addresses and if available add multiple DNS servers.

24 Revision History

Revision	Date	Remarks
00	29.09.2023	Initial version with quick start guide, user interface and PTP probing
01	16.10.2023	Add chapters for firmware update, security and hardware interfaces
02	24.01.2024	Add chapter FAQ and fixed tipos
03	01.05.2024	Add hardware interface specifications, extend security and update chapters
04	30.05.2024	Add network configuration chapter
05	30.07.2024	Add SNMP configuration section
06	09.01.2025	Restructure all chapters, add terms and definitions, extend network configuration, add chapters time handling, PTP, notifications, maintenance, device types, mounting instructions, electrical and technical specifications and compliance statements
07	07.03.2025	Add PICS table, minor term changes, add user password change
08	22.04.2025	Add event switch and time stamper description. Add safety remarks to mounting instructions. Fix power ratings.
09	04.07.2025	Add installation instruction for GNSS 4500. Several adaptations for firmware 2.2.0.
10	24.07.2025	Add time core section with holdover setup. Adopt firmware update process.
11	02.10.2025	Reorganize some chapters to match menu. Add general and hostname sections. Add and adopt Manual and Oscillator time source. Add unique password to login section. Add security audit section. Adopt extension parts to revision 02.
12	21.11.2025	Spelling correction. Add safety certificate. Remove shutdown. Improve mounting description.

Headquarters/Production
Sales Worldwide

MOSER-BAER AG | Spitalstrasse 7 | CH-3454 Sumiswald
Tel. +41 34 432 46 46 | Fax +41 34 432 46 99
moserbaer@mobatime.com | www.mobatime.com

Sales Switzerland

MOBATIME AG | Stettbachstrasse 5 | CH-8600 Dübendorf
Tel. +41 44 802 75 75 | Fax +41 44 802 75 65
info-d@mobatime.ch | www.mobatime.ch

MOBATIME SA | En Budron H 20 | CH-1052 Le Mont-sur-Lausanne
Tél. +41 21 654 33 50 | Fax +41 21 654 33 69
info-f@mobatime.ch | www.mobatime.ch

Sales Germany/Austria

BÜRK MOBATIME GmbH
Postfach 3760 | D-78026 VS-Schwenningen
Steinkirchring 46 | D-78056 VS-Schwenningen
Tel. +49 7720 8535 0 | Fax +49 7720 8535 11
buerk@buerk-mobatime.de | www.buerk-mobatime.de