enertexbayern gmbh
simulation entwicklung consulting

Manual and Configuration

Timeserver and Mapper Application for Enertex KNX IP system devices

Enertex® Bayern GmbH – Ebermannstädter Straße 8 - 91301 Forchheim - Germany - mail@enertex.de

Note

Content

Security Notes

- Installation and assembly of electrical equipment may only be carried out by qualified electricians.
- When connecting KNX / EIB interfaces, KNX ™ training is required.
- Failure to observe this instruction may result in damage to the unit, fire or other hazards.
- This guide is part of the product and must remain with the end user.
- The manufacturer is not liable for costs or damages caused to the user or third parties by the use of this device, misuse or interference of the connection, malfunctions of the device or of the subscriber devices.
- The opening of the housing, other unauthorized modifications and / or conversions to the device will void the guarantee!
- The manufacturer shall not be liable for any inappropriate use.

Assembly and connection

To operate the Timeserver and Mapper Application, you need:

- An Enertex KNX IP Secure Router or Enertex KNX IP Secure Interface

Commissioning

Application

Separate execution

Timeserver and Mapper is a separate KNX TP (Secure) application for the Enertex KNX IP Secure Interface or Enertex KNX IP Secure Router. This application runs completely separate from the KNX IP Secure application, whose ETS configuration is not dependent on the KNX TP application. The KNX TP Application needs its own physical address and FDSK.

Features

The TP application consists of the function blocks timer and mapper. It can be operated encrypted (secure) or unencrypted independently of the IP application.

Timeserver

The timeserver synchronizes the time of the built-in real time clock over the Internet with pool.ntp.org or with any local NTP server. The time can be output to the KNX bus as time or date telegram. In case of power failure, the device buffers the time for approx. 36 hours. The timeserver is automatically synchronized with the external source (internal or external NTP) every 48 hours and on restart. The user can trigger the synchronization manually via a KO.

The validity of the time of the timeserver is output via a separate CO. As long as the built-in real time clock is powered, the time is valid. If, for example, synchronization is not possible in normal operation because the Internet connection is interrupted, the internal clock still remains valid. The inaccessibility of the last synchronization attempt must be queried via a separate CO by read request. If the status changes, it is output to the bus via CO.

Mapper

The mapper is used to translate from encrypted (secure) to unencrypted (plain) communication objects. For this purpose, the mapper provides 20 channels that establish bidirectional communication. The data length of the corresponding communication objects can be parameterized (max. 14 bytes).

An explanation of how to use this functionality can be found in the section Function Overview

Update of devices with Firmware < 1.050

KNX IP Secure

The IP Secure application and its parametrization is not changed by the new TP application. In particular, no new KNX IP Secure application has to be configured for existing devices, the existing one is still valid.

After an update, however, the existing application and parametrization must be reloaded, as with updating the device a factory reset is performed.

Individual address download

The KNX TP application requires its own physical address (PA) and its own FDSK. The programming mode for the physical address can be activated with the PROG push-button as follows

- Press once

  PROG LED (red) lights up continuously, corresponds to the individual address programming mode of the IP application

- Press twice

  PROG LED (red) flashes, corresponds to programming mode of the individual address of the TP application

FDSK

The application requires its own FDSK for secure communication encrypted. On devices with firmware less than 1.050, this (second) FDSK of the TP application is not printed on the package insert. It must be read from the device display as described in section Display on the device display page 5 .

Display

After one minute the display switches off automatically. To switch it on again, press the DISPLAY button on the front panel.

When the display is switched on, pressing the DISPLAY key causes the user to scroll through six different information pages.

The information on the display pages 1 to 4 can be found in the application description of the IP system device (Enertex® KNX IP Secure Router or Enertex® KNX IP Secure Interface).

Page 5 shows the FDSK of the "Time Server Mapper" application described in this document as long as the device has not been set to the Secure state.

Page 6 shows whether the internal clock was still active within the power reserve during a power failure: "Clock has hibernated". If the power failure lasts too long (>36 hours), the display shows "Clock was down". If the application has been loaded, the current time (including daylight saving time and time zone) is displayed, as well as the time of the last synchronization (UTC) and the IP address of the external source of the time synchronization.

There are three LEDs on the front panel. The green LED flashes every second with a 1:30 duty cycle and indicates readiness for operation. The red LED indicates programming mode, the yellow LED indicates bus activity.

Two further LEDs are installed in the LAN socket. The green LED indicates a connection to another IP device or switch ("Link"), the yellow LED indicates IP data transfer.

Function Overview

The device has the following functional features

- Timeserver
  - External time server (NTP) as a source of time synchronization during commissioning
  - External time server adjustable to a fixed IP address or via pool.ntp.org
  - Status for the availability of the external time server
  - Status for the validity of the internal clock (e.g. after power failure)
  - CO for user-controlled synchronization with external time server (automatically after 2 days)
- Mapper
  - Translation from encrypted (secure) to unencrypted (plain) communication objects
  - Mapping of up to 20 communication objects
  - Size of each communication object parameterisable: 1 bit, 2 bit, 4 bit, 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes or 14 bytes

ETS Parameter

Terms

Encryption, encrypted If devices send data information via the TP bus or IP network, they are generally readable by third parties. These only require access to the TP bus or IP network for reading. Encryption of the data in this context means that the contents of the telegrams are no longer to be interpreted if the encryption parameters (for example passwords) are unknown.

Key, Key Parameter A series of numbers known only to the ETS project. These numbers are used to transform the data in both directions: encryption and decryption.

FDSK (Factory Default Setup Key) The initial factory key. This key is used when commissioning the initial programming. A new key is loaded into the device, whereby this process is encrypted with the FDSK. The FDSK key is then no longer valid. It is reactivated only when resetting to factory settings.

Telnet A simple TCP server on port 23 that enables direct text-based communication with the IP device. Telnet is a de facto standard used at the window level, e.g. with "Putty" is addressed.

Secure Mode If the device is parameterized via the ETS so that the communication is only encrypted, this is referred to as secure mode.

Plain Mode If the device is parameterized via the ETS so that the communication is only unencrypted, this is called unsecured mode.

ETS

Version requirements

ETS 5.7.4 or higher is required for error-free operation of the devices in secure mode.

Device Properties

Timeserver

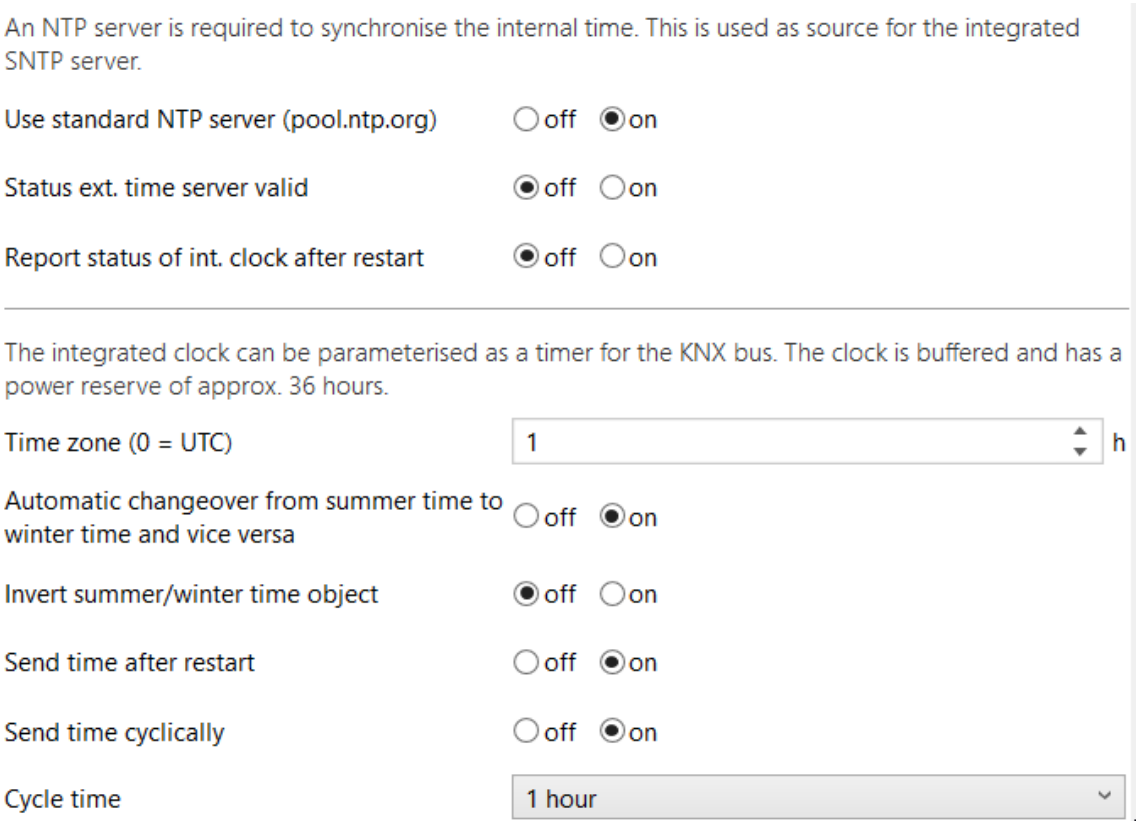

Figure 1: Timerserver

Name	Options	Description
Use standard NTP server (pool.ntp.org)	off,on	See parameter dialog . If "off" is selected here, an input field for the IP address of the local time server appears
Status ext. time server valid	off,on	Notification with CO 2
Report status of int. clock after restart	off,on	Notification with CO 3
Time zone (0=UTC)	-12 .. 0, +1 .. +14	Offset of the internal clock to UTC
Automatic changeover from summer to wintertime and vice a versa	off,on	
Invert summer/winter time object	off,on	CO9: For parameter "off": winter = 1, summer = 0 For parameter "on": winter = 0, summer = 1
Send time after restart	off,on	Sending time and date with CO3, CO4, CO5
Send time cylically	off,on	Sending time and date with CO3, CO4, CO5 cyclically
Cycle Time	24 hours, 12 hours, 3 hours, 1 hour, 30 minutes, 15 minutes	

Invertiere Sommer/Winterzeit Objekt	aus/ein	KO9: Für Parameter „aus“: Winter = 1, Sommer = 0 Für Parameter „ein“: Winter = 0, Sommer = 1

When the unit is initially powered, the internal clock is not valid, therefore the communication object CO2 is false [0]. The clock becomes valid (value = true [1]) if the device can synchronize to the time of a time server (NTP server). This is performed automatically after each restart or once every 2 days. For this purpose, an Internet connection must exist or an IP address of a separate time server must be entered in the parameter dialog (e.g. IP of the Fritzbox). After a restart or an ETS programming of the device, the time remains valid. In the case that the internal buffer capacitor has been discharged too far due to a power failure lasting more than 36 hours, the clock becomes invalid again.

The internal clock can deviate from the real time by approx. 1 second per 2 days. It automatically synchronizes itself every 2 days with the external NTP server or if this is initiated by writing (any value) with CO 7.

Note

If the communication object CO2 is false [0], the clock is not synchronized. If there is no Internet connection, the time of the time server can be set via the telnet interface using the "`date`" command (see manual of the system device). Synchronizing the clock via telnet then acts like synchronization via NTP and sets the communication object CO2 to valid (value = true [1]).

Mapper

Functionality

The mapper is used to translate from encrypted (secure) to unencrypted (plain) communication objects and vice versa.

For this purpose, the mapper provides 20 channels that establish bidirectional communication. The data length of the corresponding communication objects can be parametrized: 1 bit, 2 bit, 4 bit, 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes or 14 bytes (see Figure 2).

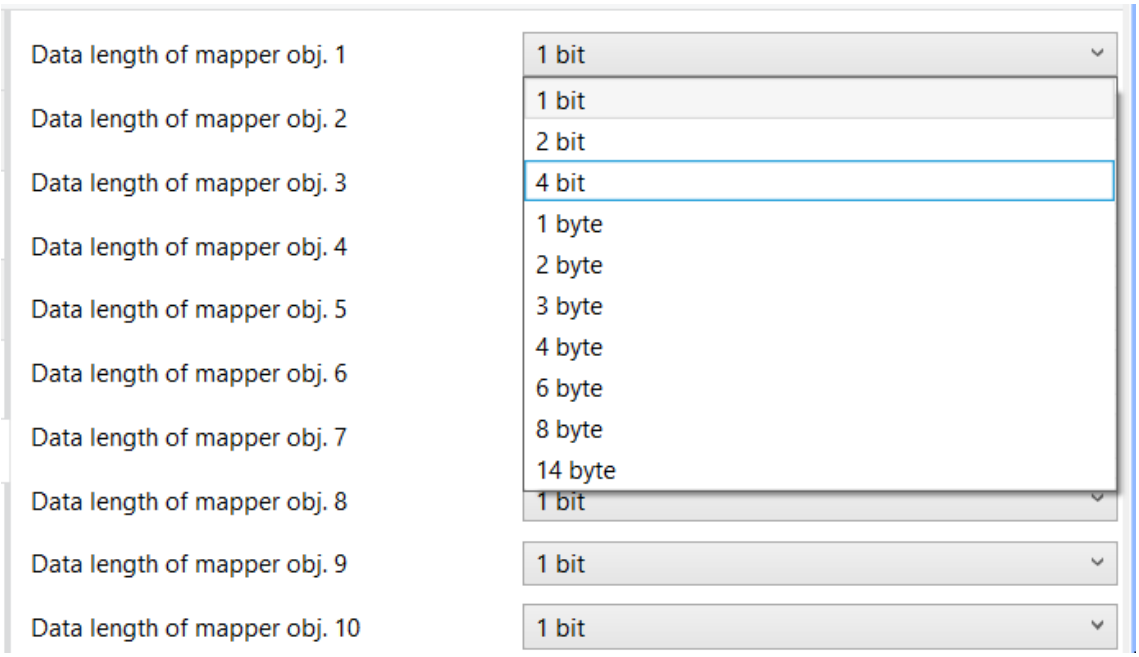

Figure 2: Mapper Datatypes

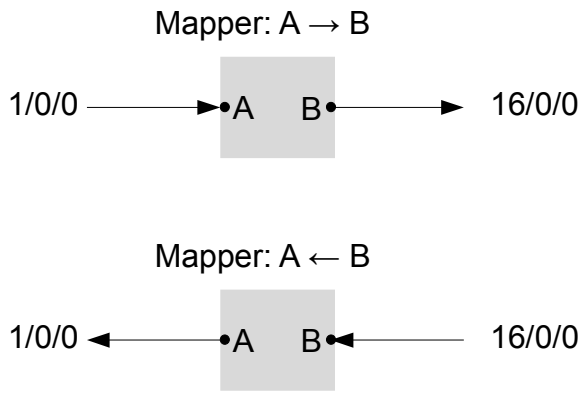

Figure 3: Mapper: writing to group addresses

Figure 3 shows the functionality: A write (or reply) to 1/0/0 (input/output A) triggers a write to 16/0/0 (input/output B). It does not matter whether 1/0/0 or 16/0/0 are encrypted or not. For example, 1/0/0 can represent an encrypted group address and 16/0/0 an unencrypted one. In this way, therefore, one (or more) encrypted group address is sent to an unencrypted one. The same applies analogously in the opposite direction. Please note that only one group address will be sent, in the case of several links according to KNX specifications.

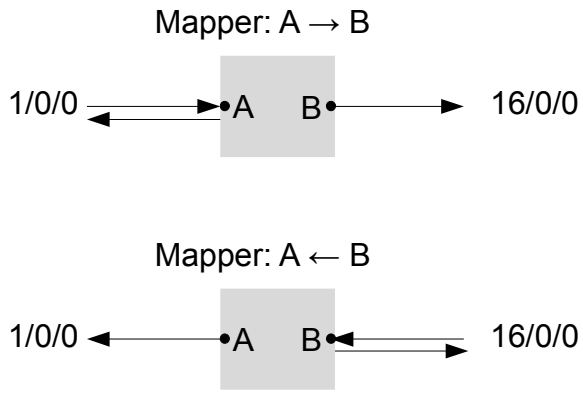

Figure 4: Mapper: Reading group addresses

Figure 4 shows read requests: A read on 1/0/0 (input/output A) triggers a read on 16/0/0 (input/output B). If the read flag for input/output A is set, the request is answered by input/output

A with a response telegram. It does not matter whether 1/0/0 or 16/0/0 are encrypted or not. For example, 1/0/0 can be an encrypted GA and 16/0/0 unencrypted. In this way, a read request from an encrypted group address to an unencrypted one can be made. The same applies analogously in the opposite direction.

To set the communication direction, see the Table 1.

For the sake of clarity, the application pairs the mappers into channels 1..10 and 11 to 20. Each channel, consisting of the two inputs/outputs A and B, can be set to the desired length.

Note

When reading, the mapper only works with group addresses that are connected to another device. Group addresses which are linked with the own communication objects, e.g. CO1 to CO7, are not handled by the mapper in the described way during read requests. These are not processed and mapped.

Direction of Communication

The flags of the group addresses can be used to set the "passing through" of group addresses by the mapper depending on the direction and the type of communication (read or write). The direction dependent setting for communication flags is given in table 1. There the communication flags for channel A are entered in column "Flags A" and for channel B in column "Flags B". Flags which are not listed in each case are not to be set.

The direction of the arrow indicates in which direction the communication read or write is possible. A → B means, from A to B the mapper direction as shown in table 1 is possible, from B to A there is no mapping of the group address.

The communication flags can be found in the ETS as shown in figure 5.

In table 1 the letters denote the same flags as in the ETS, e.g. C for communication, R for reading etc.

Figure 5 Flags

Direction	Read	Write	Flags A	Flags B
A ↔ B	ja	ja	C R W U	C R W U
A ↔ B	ja	--	C R - U	C R - U
A ↔ B	--	ja	C - W U	C - W U
A → B	ja	ja	C R W -	C - W U
A → B	ja	--	C R - -	C - W U
A → B	--	ja	C - R -	C - W U
A ← B	ja	ja	C - W U	C R W -
A ← B	ja	--	C – W U	C R - -
A ← B	--	ja	C - W U	C - W -

Table 1 direction of communication

Application case 1: Second TP Line in Outdoor area

The practical use of the mapper is explained in the following scenario according to Figure 6:

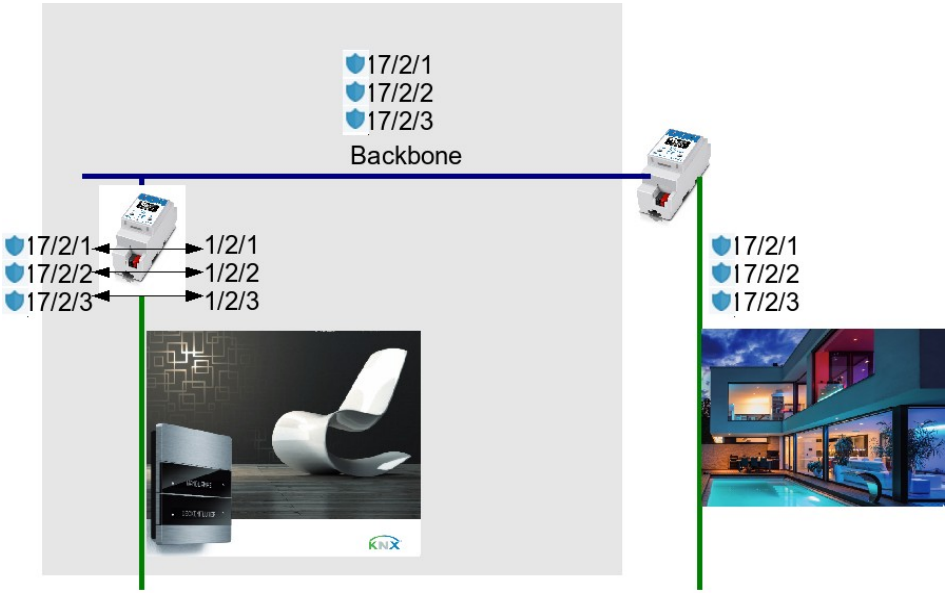

Figure 6: Application Mapper - Second TP Line in Outdoor area

A system consists of an inner TP and outer TP line. E.g. the second TP Line represents an Outdoor area.

In order to increase the security of the installation, it was decided to use the outer line with KNX Data Secure. Therefor for example the opening of the garage door or the closing is done via KNX Secure communication. In the example, the group addresses 17/2/1, 17/2/2 and 17/2/3 are used for that purpose. The group addresses are routed to the inner line via two IP routers. On the inner line the opening functions are communicating with group addresses 1/2/1, 1/2/2 and 1/2/3. However, the inner line only has unencrypted actuators and sensors. Via the mapper the GAs 17/2/1 are now mapped to 1/2/1, 17/2/2 to 1/2/2, 17/2/3 to 1/2/3. Therefore the devices on the inner line can now communicate with the outer line. Via the routing of the Enertex® IP Secure Router or equally of the Enertex TP Secure Coupler, there is a very detailed routing possible. These devices can be parametrized that the main group 17 is routed, but the main group 2 is blocked. Thus, security on the outer line can now be combined with the inner line without problems.

Application case 2: Directional Mapping

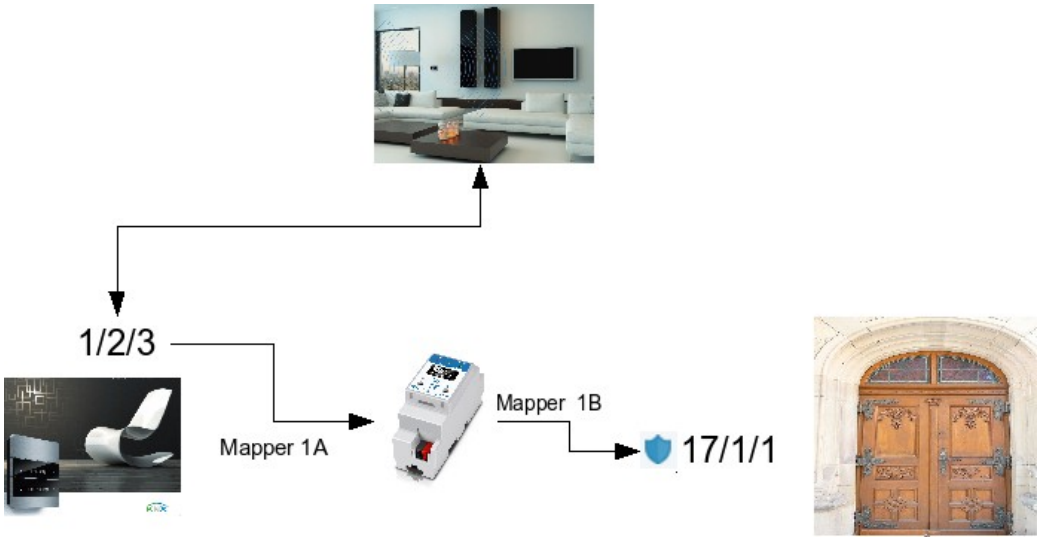

Figure 7: Directional Mapping

Another relevant application example is the direction-dependent mapping in a KNX installation where (different) group addresses communicate both unencrypted and encrypted. For example, a central function "night mode" is sent unencrypted to a GA 1/2/3. This central function should both switch off all lights and close the door lock, which communicates on a secure group ad-

dress 17/1/1 (see Figure 7).

If the mapper is set according to table 1 that write A → B is possible and the group addresses are set up according to figure 7, the communication at group address 17/1/1 is completely independent of the central command "night mode".

At the same time, the security of the door lock or communication via 17/1/1 remains independent of the central command. If only the door lock is operated, no central command is sent to the unencrypted actuators.

Communication Objects

Note

Depending on the parameters some of the group objects might be not visable in the ETS.

ID	Name	Object function	Description	Length	Type
1	External timeserver valid – output	Status	Specifies whether the external time server pool.ntp.org is accessible from the device. The name resolution is done via the DNS server 9.9.9.9. For more information, see www.quad9.net. If an own NTP time server is to be set, its IP address must be known. In this case the CO will not send anything. The time is automatically synchronized with the external NTP server every two days or if this is initiated with CO 7.	1 Bit	[1.2] DPT_Bool
2	Internal clock valid - output	Status	Indicates whether the internal clock is valid. Value true [1] stands for valid, value false [0] for invalid. The communication object can be sent automatically after each restart via the parametrization. When the device is initially powered, the communication object is false [0]. The clock becomes valid (value = true [1]) if the device can query the time via an NTP server and set the internal clock accordingly. After a restart or ETS programming of the device, the value remains true [1]. Only if the internal buffer capacitor has been discharged too far due to a power failure lasting several days, the clock becomes invalid again (value = false [0]). **Note** If the communication object CO2 is false [0], the clock is not synchronized. If there is no Internet connection, the time of the time server can be set via the telnet interface using the "`date`" command (see manual of the system device). Synchronizing the clock via telnet then acts like synchronization via NTP and sets the communication object CO2 to valid (value = true [1]).	1 Bit	[1.2] DPT_Bool
3	Time – output	time output	Communication object for outputting the current time to the bus. The internal clock is buffered internally (via supercap capacitor) for approx. 1.5 days. The internal clock can deviate from the real time by approx. 1 second per 2 days. A read telegram always provides the current time.	3 Byte	[10.001] DPT_TimeOfDay
4	Date – output	date output	Communication object for displaying the calendar of the internal clock.	3 Byte	[11.001] DPT_Date
5	Time and Date – output	time and date output	Time and date to output the current time and date to the bus.	8 Byte	[19.001] DPT_DateTime
6	Date/time – input	requesting	Trigger for writing CO 3, CO 4 and CO 5. It triggers both writing 0 and 1.	1 Bit	[1.017] DPT_Trigger
7	NTP server sync. - input	requesting	The internal clock synchronizes automatically every 2 days with the NTP server or if this KO is written. It triggers both writing 0 and 1.	1 Bit	[1.017] DPT_Trigger

ID	Name	Object function	Description	Length	Type
8	Sommer /wintertime – output	status	If summer time is active, this CO becomes 0, during winter time it becomes 1, so this CO can be used directly for the winter changeover of heating systems. The polarity of this CO can be inverted via the parameter "Invert summer/winter time object" (see Figure 1)	1 Bit	[1.xxx]
9	MapperObjekt Chanel A – *field lentgh*	in-/output	When writing or replying to this CO, the value is written to the CO of channel B on the bus. The encryption of the individual channels is taken into account. If a read request is received, it is answered and a read request is simultaneously issued on channel B.	1 Bit bis 14 Byte	n.a.
10	MapperObjekt Chanel B - *field lentgh*	in-/output	When writing or replying to this CO, the value is written to the CO of channel A on the bus. The encryption of the individual channels is taken into account. If a read request is received, it is answered and a read request is simultaneously issued on channel A.	1 Bit bis 14 Byte	n.a.
Additional 19 mapper channel pairs					

Latest documentation and Software

Under http://www.enertex.de/d-produkt.html you will find the current ETS database file as well as the current product description.