



Handbuch und Konfiguration

Zeitgeber und Mapper Applikation für Enertex KNX IP Systemgeräte



Hinweis

Der Inhalt dieses Dokuments darf ohne vorherige schriftliche Genehmigung durch die Enertex® Bayern GmbH in keiner Form, weder ganz noch teilweise, vervielfältigt, weitergegeben, verbreitet werden.

Enertex® ist eine eingetragene Marke der Enertex® Bayern GmbH. Andere in diesem Handbuch erwähnte Produkt- und Firmennamen können Marken- oder Handelsnamen ihrer jeweiligen Eigentümer sein.

Dieses Handbuch kann ohne Benachrichtigung oder Ankündigung geändert werden und erhebt keinen Anspruch auf Vollständigkeit oder Korrektheit.

Inhalt

Sicherheitshinweise.....	3
Montage und Anschluss.....	3
Inbetriebnahme.....	3
<i>Applikation.....</i>	<i>3</i>
Getrennte Ausführung.....	3
Eigenschaften.....	3
Zeitgeber.....	3
Mapper.....	4
<i>Update von Geräten mit FW < 1.050.....</i>	<i>4</i>
KNX IP Secure.....	4
Physikalische Adressvergabe.....	4
FDSK.....	4
<i>Anzeigen.....</i>	<i>4</i>
Funktionsübersicht.....	5
ETS Parameter.....	5
<i>Begriffe.....</i>	<i>5</i>
<i>ETS</i>	<i>6</i>
Version.....	6
<i>Gerätespezifische Parameter.....</i>	<i>7</i>
Zeitgeber.....	7
Mapper.....	8
Funktionsweise.....	8
Kommunikationsrichtung.....	9
Anwendungsfall 1: Außenlinie	10
Anwendungsfall 2: Richtungsabhängiges Mapping	11
<i>Kommunikationsobjekte.....</i>	<i>11</i>

Sicherheitshinweise

- Einbau und Montage elektrischer Geräte darf nur durch Elektrofachkräfte erfolgen.
- Beim Anschluss von KNX IP Secure Schnittstellen werden Fachkenntnisse durch KNX™-Schulungen vorausgesetzt.
- Bei Nichtbeachtung der Anleitung können Schäden am Gerät, sowie ein Brand oder andere Gefahren entstehen.
- Diese Anleitung ist Bestandteil des Produkts und muss beim Endanwender verbleiben.
- Der Hersteller haftet nicht für Kosten oder Schäden, die dem Benutzer oder Dritten durch den Einsatz dieses Gerätes, Missbrauch oder Störungen des Anschlusses, Störungen des Gerätes oder der Teilnehmergeräte entstehen.
- Das Öffnen des Gehäuses, andere eigenmächtige Veränderungen und / oder Umbauten am Gerät führen zum Erlöschen der Gewährleistung!
- Für eine nicht bestimmungsgemäße Verwendung haftet der Hersteller nicht.

Montage und Anschluss

Für den Betrieb der Zeitgeber und Mapper Applikation wird benötigt:

- Ein Enertex KNX IP Secure Interface oder Enertex KNX IP Secure Router

Inbetriebnahme

Applikation

Getrennte Ausführung

Zeitgeber und Mapper ist eine getrennte KNX TP (Secure) Applikation für das Enertex KNX IP Secure Interface bzw. Enertex KNX IP Secure Router. Diese Applikation läuft komplett getrennt von der KNX IP Secure Applikation, deren ETS Konfiguration von der KNX TP Applikation nicht abhängig ist. Die KNX TP Applikation benötigt eine eigene physikalische Adresse, sowie einen eigenen FDSK.

Eigenschaften

Die TP Applikation besteht aus den Funktionsblöcken Zeitgeber und Mapper. Sie kann unabhängig von der IP Applikation verschlüsselt (Secure) oder unverschlüsselt in Betrieb genommen werden.

Zeitgeber

Der Zeitgeber synchronisiert die Uhrzeit der eingebauten Echtzeituhr über das Internet mit pool.ntp.org oder mit einer anderen lokalen Quelle. Diese Uhrzeit kann als Zeit- bzw. Datumstrogramm auf den KNX Bus ausgegeben werden. Bei Spannungsunterbrechung puffert das Gerät ca. 36 Stunden die Uhrzeit. Die Uhrzeit wird automatisch mit der externen Quelle (interner oder externer NTP) alle 48 Stunden und beim Neustart synchronisiert. Der Anwender kann über ein KO die Synchronisierung manuell triggern.

Die „Gültigkeit“ der Uhrzeit wird über ein separates KO ausgegeben. Solange die eingebaute Echtzeituhr versorgt wird, so ist die Uhrzeit gültig. Wenn im Normalbetrieb beispielsweise die Synchronisation nicht möglich ist, weil die Internetverbindung unterbrochen ist, so bleibt die interne Uhrzeit dennoch gültig. Die Nacherreichbarkeit des letzten Synchronisationsversuchs ist über ein getrenntes KO per Leseanforderung abzufragen. Wenn sich der Zustand ändert, wird dieser per KO auf den Bus ausgegeben.

Mapper

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekten. Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Die Datenlänge der entsprechenden Kommunikationsobjekte kann parametrieren werden (max. 14 Byte).

Eine Erläuterung zur Anwendung dieser Funktionalität findet sich im Abschnitt Funktionsübersicht.

Update von Geräten mit FW < 1.050

KNX IP Secure

Die IP Secure Applikation und deren Parametrierung ist durch die neue TP-Applikation nicht verändert. Insbesondere ist bei bestehenden Geräten keine neue KNX IP Secure Applikation zu konfigurieren, die bestehende ist nach wie vor gültig.

Nach einem Update ist allerdings die bestehende Applikation und Parametrierung in jedem Fall neu zu laden, da ein Werksreset ausgeführt wird.

Physikalische Adressvergabe

Die KNX TP Applikation benötigt eine eigene physikalische Adresse (PA), sowie einen eigenen FDSK. Der Programmiermodus für die physikalische Adresse ist mit dem PROG-Taster wie folgt zu aktivieren:

- 1x Drücken
PROG LED (rot) leuchtet dauerhaft, entspricht Programmiermodus der PA der IP Applikation
- 2x Drücken
PROG LED (rot) blinkt, entspricht Programmiermodus der PA der TP Applikation

FDSK

Die Applikation benötigt einen eigenen FDSK, falls diese über Data Secure verschlüsselt kommunizieren soll. Bei Geräten im Auslieferungszustand der Firmware kleiner 1.050 ist der FDSK der TP Applikation nicht auf dem Beipackzettel aufgedruckt. Dieser muss, wie in Abschnitt „Anzeigen“ vorgestellt, auf Seite 5 der Displayanzeige abgelesen werden.

Anzeigen

Nach einer Minute schaltet sich das Display automatisch aus. Um dieses wieder einzuschalten, muss die DISPLAY Taste auf der Gerätefront kurz betätigt werden.

Bei eingeschaltetem Display wird durch Betätigen der DISPLAY Taste ein Durchblättern von sechs verschiedenen Informationsseiten ausgelöst.

Die Informationen auf den Display-Seiten 1 bis 4 entnehmen Sie der Beschreibung des Applikation der Beschreibung des IP Systemgerätes (Enertex® KNX IP Secure Router oder Enertex® KNX IP Secure Interface).

Seite 5 zeigt den FDSK der in diesem Dokument beschriebenen Applikation „ZeitserverMapper“, solange das Gerät nicht in den Secure – Zustand gesetzt wurde.

Seite 6 zeigt an, ob die interne Uhr während eines Stromausfalls noch innerhalb der Gangreserve aktiv war: „Clock has hibernated“. Falls der Stromausfall zu lange dauert (>36 Std), zeigt das Display „Clock was down“. Falls die Applikation geladen wurde, wird die aktuelle Uhrzeit (inkl. Sommerzeit und Zeitzone) angezeigt, sowie der Zeitpunkt der letzten Synchronisierung (UTC) und die IP Adresse der externen Quelle der Zeitsynchronisierung.

Auf der Vorderseite befinden sich drei LEDs. Die grüne LED blinkt im Sekundentakt mit einem Tastverhältnis 1:30 und zeigt Betriebsbereitschaft an. Die rote LED dient zur Anzeige des Programmiermodus, die gelbe LED zeigt Busaktivität.

In der LAN Buchse sind zwei weitere LEDs verbaut. Die grüne zeigt eine Verbindung zu einem anderen IP Gerät oder Switch an („Link“), die gelbe LED zeigt den IP Datentransfer.

Funktionsübersicht

Das Gerät weist folgende Funktionalitäten auf:

- Zeitgeber
 - Externer Zeitserver (NTP) als Quelle der Zeitsynchronisierung bei Inbetriebnahme
 - Externer Zeitserver einstellbar auf feste IP Adresse oder über pool.ntp.org
 - Status für die Erreichbarkeit des externen Zeitservers
 - Status für die Gültigkeit der internen Uhr (z.B. nach Spannungsausfall)
 - KO für benutzergesteuerte Synchronisierung mit externem Zeitserver (automatisch nach 2 Tagen)
- Mapper
 - Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekten
 - Mapping von bis zu 20 Kommunikationsobjekten
 - Größe jedes Kommunikationsobjekts parametrierbar: 1 Bit, 2 Bit, 4 Bit, 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes oder 14 Bytes

ETS Parameter

Begriffe

Verschlüsselung, Verschlüsselt Wenn Geräte Dateninformationen in Form von Telegrammen über den TP-Bus oder IP-Netzwerk schicken, so sind diese grundsätzlich von Dritten lesbar. Diese benötigen hierzu lediglich Zugang zum TP-Bus oder IP-Netzwerk. Verschlüsselung der Daten soll in diesem Zusammenhang bedeuten, dass die Inhalte der Telegramme nicht mehr zu deuten sind, wenn die Verschlüsselungsparameter (z.B. Kennwörter) nicht bekannt sind.

Schlüssel, Verschlüsselungsparameter Eine Folge von Zahlen, die nur dem ETS Projekt bekannt sind. Diese Zahlen dienen zur Umformung der Daten in beide Richtungen: Ver- und Entschlüsseln.

FDSK (Factory Default Setup Key) Der initiale Fabrikschlüssel. Dieser Schlüssel dient bei der Inbetriebnahme der initialen Programmierung. Dabei wird ein neuer Schlüssel in das Gerät geladen, wobei dieser Vorgang mit dem FDSK verschlüsselt wird. Der FDSK Schlüssel ist danach nicht mehr gültig. Erst beim Zurücksetzen auf den Werkzustand (Factory Reset) wird er wieder aktiviert.

Tunnelling Eine KNX Punkt-zu-Punkt Verbindung auf dem TCP/IP Netzwerk, die entweder per UDP oder TCP Protokoll aufgebaut wird. Tunnelling hat immer eine Sicherungsschicht eingebaut, d.h. unabhängig von der Ethernetverbindung, z.B. Kabel oder WLAN, und unabhängig vom TCP/IP Protokoll (UDP oder TCP) gehen keine Daten verloren. Bei UDP gilt allerdings die Einschränkung, dass die Sicherungsschicht mit einem 1-Sekunden-Timeout arbeitet. Bei Enertex Geräten kann dieser Timeout im erweiterten Setup angepasst werden.

Secure Tunnelling oder Sicheres Tunnelling bedeutet, dass die Tunnelverbindung verschlüsselt übertragen wird.

Abgesicherter Modus, Secure Mode Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur verschlüsselt erfolgt, spricht man vom abgesicherten Modus oder engl. Secure Mode.

Nicht abgesicherter Modus, Plain Mode Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur unverschlüsselt erfolgt, spricht man vom nicht abgesicherten Modus oder engl. Plain Mode.

ETS

Version

Für einen fehlerfreien Betrieb der Geräte im abgesicherten Modus (Secure Mode) benötigt man die ETS 5.7.4 oder höher.

Gerätespezifische Parameter

Zeitgeber

Zur Synchronisierung der internen Uhrzeit ist ein NTP Server erforderlich. Dieser wird als Quelle für den integrierten SNTP Server verwendet.. Der NTP Server dient auch der Authentifizierung zum Fernwartungsdienst.

Standard NTP Server verwenden
(pool.ntp.org) aus ein

Status ext. Zeitserver gültig aus ein

Status int. Uhr nach Neustart melden aus ein

Die integrierte Uhr kann als Zeitgeber für den KNX Bus parametert werden. Die Uhr ist gepuffert und hat eine Gangreserve von ca. 36 Std.

Zeitzone (0 = UTC)	<input type="text" value="1"/> h
Automatische Umstellung Sommerzeit/ Winterzeit	<input type="radio"/> aus <input checked="" type="radio"/> ein
Zeit senden nach Neustart	<input type="radio"/> aus <input checked="" type="radio"/> ein
Uhrzeit zyklisch senden	<input type="radio"/> aus <input checked="" type="radio"/> ein
Zykluszeit	<input type="text" value="1 Stunde"/> ▼
Invertiere Sommer-/Winterzeit-Objekt	<input checked="" type="radio"/> aus <input type="radio"/> ein

Abbildung 1: Zeitgeber

Name	Auswahlmöglichkeiten	Beschreibung
Standard NTP Server verwenden (pool.ntp.org)	aus/ein	Vgl. Parameterdialog Falls hier „aus“ gewählt wird, erscheint ein Eingabefeld für die IP Adresse des eigenen lokalen Zeitservers
Status ext. Zeitservers gültig	aus/ein	Meldung über KO 1
Status int. Uhr nach Neustart melden	aus/ein	Meldung über KO 2
Zeitzone (0=UTC)	-12 .. 0, +1 .. +14	Stundenversatz der internen Uhr zu UTC
Automatische Umstellung Sommerzeit/Winterzeit	aus/ein	
Zeit senden nach Neustart	aus/ein	Ausgabe von Zeit und Datum auf KO3, KO4, KO5
Uhrzeit zyklisch senden	aus/ein	
Zykluszeit	24 Stunden, 12 Stunden, 3 Stunden, <u>1 Stunde</u> , 30 Minuten, 15 Minuten	Zyklische Ausgabe von Zeit und Datum auf KO3, KO4, KO5
Invertiere Sommer/Winterzeit Objekt	aus/ein	KO9: Für Parameter „aus“: Winter = 1, Sommer = 0 Für Parameter „ein“: Winter = 0, Sommer = 1

Bei Auslieferung des Geräts ist die interne Uhr nicht gültig, das Kommunikationsobjekt KO2 ist

daher gleich falsch [0]. Die Uhr wird dann gültig (Wert = wahr [1]), wenn das Gerät sich über einen Zeitserver (NTP Server) auf dessen Uhrzeit synchronisieren kann. Dies erfolgt nach jedem Neustart bzw. alle 2 Tage einmal automatisch. Dazu muss eine Internetverbindung bestehen bzw. eine IP Adresse eines eigenen Zeitserver im Parameterdialog eingetragen werden (z.B. IP der Fritzbox). Nach einem Neustart bzw. einer ETS-Programmierung des Geräts bleibt die Uhrzeit weiterhin gültig. Nur in dem Fall, dass der interne Pufferkondensator aufgrund eines mehr 36 stündigen Stromausfalls zu weit entladen wurde, wird die Uhr wieder ungültig.

Die interne Uhr kann pro 2 Tage um ca. 1 Sekunde von der realen Zeit abweichen. Sie synchronisiert sich automatisch alle 2 Tage mit den externen NTP Server bzw. falls dies durch Schreiben (Wert beliebig) mit KO 7 initiiert wird.

Hinweis

Wenn das Kommunikationsobjekt KO2 falsch [0] ist, so ist die Uhr nicht synchronisiert. Sollte keine Internetverbindung bestehen, kann die Zeit des Zeitservers über das telnet-Interface per „date“ Befehl (siehe Handbuch des Systemgerätes) gesetzt werden. Das Synchronisieren der Uhr über telnet wirkt dann wie eine Synchronisation über NTP und setzt das Kommunikationsobjekt KO2 auf gültig (Wert = wahr [1]).

Mapper

Funktionsweise

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekten und umgekehrt.

Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Die Datenlänge der entsprechenden Kommunikationsobjekte kann parametriert werden: 1 Bit, 2 Bit, 4 Bit, 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes oder 14 Bytes (vgl. Abbildung 2).

Datenlänge des Mapper Obj. 1	1 Bit
Datenlänge des Mapper Obj. 2	1 Bit
Datenlänge des Mapper Obj. 3	2 Bit
Datenlänge des Mapper Obj. 4	4 Bit
Datenlänge des Mapper Obj. 5	8 Bit
Datenlänge des Mapper Obj. 6	16 Bit
Datenlänge des Mapper Obj. 7	24 Bit
Datenlänge des Mapper Obj. 8	32 Bit
Datenlänge des Mapper Obj. 9	6 Bytes
Datenlänge des Mapper Obj. 10	8 Bytes
	14 Bytes
	18 Bytes
	22 Bytes
	26 Bytes
	30 Bytes
	34 Bytes
	38 Bytes
	42 Bytes
	46 Bytes
	50 Bytes
	54 Bytes
	58 Bytes
	62 Bytes
	66 Bytes
	70 Bytes
	74 Bytes
	78 Bytes
	82 Bytes
	86 Bytes
	90 Bytes
	94 Bytes
	98 Bytes
	102 Bytes
	106 Bytes
	110 Bytes
	114 Bytes
	118 Bytes
	122 Bytes
	126 Bytes
	130 Bytes
	134 Bytes
	138 Bytes
	142 Bytes
	146 Bytes
	150 Bytes
	154 Bytes
	158 Bytes
	162 Bytes
	166 Bytes
	170 Bytes
	174 Bytes
	178 Bytes
	182 Bytes
	186 Bytes
	190 Bytes
	194 Bytes
	198 Bytes
	202 Bytes
	206 Bytes
	210 Bytes
	214 Bytes
	218 Bytes
	222 Bytes
	226 Bytes
	230 Bytes
	234 Bytes
	238 Bytes
	242 Bytes
	246 Bytes
	250 Bytes
	254 Bytes
	258 Bytes
	262 Bytes
	266 Bytes
	270 Bytes
	274 Bytes
	278 Bytes
	282 Bytes
	286 Bytes
	290 Bytes
	294 Bytes
	298 Bytes
	302 Bytes
	306 Bytes
	310 Bytes
	314 Bytes
	318 Bytes
	322 Bytes
	326 Bytes
	330 Bytes
	334 Bytes
	338 Bytes
	342 Bytes
	346 Bytes
	350 Bytes
	354 Bytes
	358 Bytes
	362 Bytes
	366 Bytes
	370 Bytes
	374 Bytes
	378 Bytes
	382 Bytes
	386 Bytes
	390 Bytes
	394 Bytes
	398 Bytes
	402 Bytes
	406 Bytes
	410 Bytes
	414 Bytes
	418 Bytes
	422 Bytes
	426 Bytes
	430 Bytes
	434 Bytes
	438 Bytes
	442 Bytes
	446 Bytes
	450 Bytes
	454 Bytes
	458 Bytes
	462 Bytes
	466 Bytes
	470 Bytes
	474 Bytes
	478 Bytes
	482 Bytes
	486 Bytes
	490 Bytes
	494 Bytes
	498 Bytes
	502 Bytes
	506 Bytes
	510 Bytes
	514 Bytes
	518 Bytes
	522 Bytes
	526 Bytes
	530 Bytes
	534 Bytes
	538 Bytes
	542 Bytes
	546 Bytes
	550 Bytes
	554 Bytes
	558 Bytes
	562 Bytes
	566 Bytes
	570 Bytes
	574 Bytes
	578 Bytes
	582 Bytes
	586 Bytes
	590 Bytes
	594 Bytes
	598 Bytes
	602 Bytes
	606 Bytes
	610 Bytes
	614 Bytes
	618 Bytes
	622 Bytes
	626 Bytes
	630 Bytes
	634 Bytes
	638 Bytes
	642 Bytes
	646 Bytes
	650 Bytes
	654 Bytes
	658 Bytes
	662 Bytes
	666 Bytes
	670 Bytes
	674 Bytes
	678 Bytes
	682 Bytes
	686 Bytes
	690 Bytes
	694 Bytes
	698 Bytes
	702 Bytes
	706 Bytes
	710 Bytes
	714 Bytes
	718 Bytes
	722 Bytes
	726 Bytes
	730 Bytes
	734 Bytes
	738 Bytes
	742 Bytes
	746 Bytes
	750 Bytes
	754 Bytes
	758 Bytes
	762 Bytes
	766 Bytes
	770 Bytes
	774 Bytes
	778 Bytes
	782 Bytes
	786 Bytes
	790 Bytes
	794 Bytes
	798 Bytes
	802 Bytes
	806 Bytes
	810 Bytes
	814 Bytes
	818 Bytes
	822 Bytes
	826 Bytes
	830 Bytes
	834 Bytes
	838 Bytes
	842 Bytes
	846 Bytes
	850 Bytes
	854 Bytes
	858 Bytes
	862 Bytes
	866 Bytes
	870 Bytes
	874 Bytes
	878 Bytes
	882 Bytes
	886 Bytes
	890 Bytes
	894 Bytes
	898 Bytes
	902 Bytes
	906 Bytes
	910 Bytes
	914 Bytes
	918 Bytes
	922 Bytes
	926 Bytes
	930 Bytes
	934 Bytes
	938 Bytes
	942 Bytes
	946 Bytes
	950 Bytes
	954 Bytes
	958 Bytes
	962 Bytes
	966 Bytes
	970 Bytes
	974 Bytes
	978 Bytes
	982 Bytes
	986 Bytes
	990 Bytes
	994 Bytes
	998 Bytes
	1002 Bytes
	1006 Bytes
	1010 Bytes
	1014 Bytes
	1018 Bytes
	1022 Bytes
	1026 Bytes
	1030 Bytes
	1034 Bytes
	1038 Bytes
	1042 Bytes
	1046 Bytes
	1050 Bytes
	1054 Bytes
	1058 Bytes
	1062 Bytes
	1066 Bytes
	1070 Bytes
	1074 Bytes
	1078 Bytes
	1082 Bytes
	1086 Bytes
	1090 Bytes
	1094 Bytes
	1098 Bytes
	1102 Bytes
	1106 Bytes
	1110 Bytes
	1114 Bytes
	1118 Bytes
	1122 Bytes
	1126 Bytes
	1130 Bytes
	1134 Bytes
	1138 Bytes
	1142 Bytes
	1146 Bytes
	1150 Bytes
	1154 Bytes
	1158 Bytes
	1162 Bytes
	1166 Bytes
	1170 Bytes
	1174 Bytes
	1178 Bytes
	1182 Bytes
	1186 Bytes
	1190 Bytes
	1194 Bytes
	1198 Bytes
	1202 Bytes
	1206 Bytes
	1210 Bytes
	1214 Bytes
	1218 Bytes
	1222 Bytes
	1226 Bytes
	1230 Bytes
	1234 Bytes
	1238 Bytes
	1242 Bytes
	1246 Bytes
	1250 Bytes
	1254 Bytes
	1258 Bytes
	1262 Bytes
	1266 Bytes
	1270 Bytes
	1274 Bytes
	1278 Bytes
	1282 Bytes
	1286 Bytes
	1290 Bytes
	1294 Bytes
	1298 Bytes
	1302 Bytes
	1306 Bytes
	1310 Bytes
	1314 Bytes
	1318 Bytes
	1322 Bytes
	1326 Bytes
	1330 Bytes
	1334 Bytes
	1338 Bytes
	1342 Bytes
	1346 Bytes
	1350 Bytes
	1354 Bytes
	1358 Bytes
	1362 Bytes
	1366 Bytes
	1370 Bytes
	1374 Bytes
	1378 Bytes
	1382 Bytes
	1386 Bytes
	1390 Bytes
	1394 Bytes
	1398 Bytes
	1402 Bytes
	1406 Bytes
	1410 Bytes
	1414 Bytes
	1418 Bytes
	1422 Bytes
	1426 Bytes
	1430 Bytes
	1434 Bytes
	1438 Bytes
	1442 Bytes
	1446 Bytes
	1450 Bytes
	1454 Bytes
	1458 Bytes
	1462 Bytes
	1466 Bytes
	1470 Bytes
	1474 Bytes
	1478 Bytes
	1482 Bytes
	1486 Bytes
	1490 Bytes
	1494 Bytes
	1498 Bytes
	1502 Bytes
	1506 Bytes
	1510 Bytes
	1514 Bytes
	1518 Bytes
	1522 Bytes
	1526 Bytes
	1530 Bytes
	1534 Bytes
	1538 Bytes
	1542 Bytes
	1546 Bytes
	1550 Bytes
	1554 Bytes
	1558 Bytes
	1562 Bytes
	1566 Bytes
	1570 Bytes
	1574 Bytes
	1578 Bytes
	1582 Bytes
	1586 Bytes
	1590 Bytes
	1594 Bytes
	1598 Bytes
	1602 Bytes
	1606 Bytes
	1610 Bytes
	1614 Bytes
	1618 Bytes
	1622 Bytes
	1626 Bytes
	1630 Bytes
	1634 Bytes
	1638 Bytes
	1642 Bytes
	1646 Bytes
	1650 Bytes
	1654 Bytes
	1658 Bytes
	1662 Bytes
	1666 Bytes
	1670 Bytes
	1674 Bytes
	1678 Bytes
	1682 Bytes
	1686 Bytes
	1690 Bytes
	1694 Bytes
	1698 Bytes
	1702 Bytes
	1706 Bytes
	1710 Bytes
	1714 Bytes
	1718 Bytes
	1722 Bytes
	1726 Bytes
	1730 Bytes
	1734 Bytes
	1738 Bytes
	1742 Bytes
	1746 Bytes
	1750 Bytes
	1754 Bytes
	1758 Bytes
	1762 Bytes
	1766 Bytes
	1770 Bytes
	1774 Bytes
	1778 Bytes
	1782 Bytes
	1786 Bytes
	1790 Bytes
	1794 Bytes
	1798 Bytes
	1802 Bytes
	1806 Bytes
	1810 Bytes
	1814 Bytes
	1818 Bytes
	1822 Bytes
	1826 Bytes
	1830 Bytes
	1834 Bytes
	1838 Bytes
	1842 Bytes
	1846 Bytes
	1850 Bytes
	1854 Bytes
	1858 Bytes
	1862 Bytes
	1866 Bytes
	1870 Bytes
	1874 Bytes
	1878 Bytes
	1882 Bytes
	1886 Bytes
	1890 Bytes
	1894 Bytes
	1898 Bytes
	1902 Bytes
	1906 Bytes
	1910 Bytes
	1914 Bytes
	1918 Bytes
	1922 Bytes
	1926 Bytes
	1930 Bytes
	1934 Bytes
	1938 Bytes
	1942 Bytes
	1946 Bytes
	1950 Bytes
	1954 Bytes
	1958 Bytes
	1962 Bytes
	1966 Bytes
	1970 Bytes
	1974 Bytes
	1978 Bytes
	1982 Bytes
	1986 Bytes
	1990 Bytes
	1994 Bytes
	1998 Bytes
	2002 Bytes
	2006 Bytes
	2010 Bytes
	2014 Bytes
	2018 Bytes
	2022 Bytes
	2026 Bytes
	2030 Bytes
	2034 Bytes
	2038 Bytes
	2042 Bytes
	2046 Bytes
	2050 Bytes
	2054 Bytes
	2058 Bytes
	2062 Bytes
	2066 Bytes
	2070 Bytes
	2074 Bytes
	2078 Bytes
	2082 Bytes
	2086 Bytes
	2090 Bytes
	2094 Bytes
	2098 Bytes
	2102 Bytes
	2106 Bytes
	2110 Bytes
	2114 Bytes
	2118 Bytes
	2122 Bytes
	2126 Bytes
	2130 Bytes
	2134 Bytes
	2138 Bytes
	2142 Bytes
	2146 Bytes
	2150 Bytes
	2154 Bytes
	2158 Bytes
	2162 Bytes
	2166 Bytes
	2170 Bytes
	2174 Bytes
	2178 Bytes
	2182 Bytes
	2186 Bytes
	2190 Bytes
	2194 Bytes
	2198 Bytes
	2202 Bytes
	2206 Bytes
	2210 Bytes
	2214 Bytes
	2218 Bytes
	2222 Bytes
	2226 Bytes
	2230 Bytes
	2234 Bytes
	2238 Bytes
	2242 Bytes
	2246 Bytes
	2250 Bytes
	2254 Bytes
	2258 Bytes
	2262 Bytes
	2266 Bytes
	2270 Bytes
	2274 Bytes
	2278 Bytes
	2282 Bytes
	2286 Bytes
	2290 Bytes
	2294 Bytes
	2298 Bytes
	2302 Bytes
	2306 Bytes
	2310 Bytes
	2314 Bytes
	2318 Bytes
	2322 Bytes
	2326 Bytes
	2330 Bytes
	2334 Bytes
	2338 Bytes
	2342 Bytes
	2346 Bytes
	2350 Bytes
	2354 Bytes
	2358 Bytes
	2362 Bytes
	2366 Bytes
	2370 Bytes
	2374 Bytes
	2378 Bytes
	2382 Bytes
	2386 Bytes
	2390 Bytes
	2394 Bytes
	2398 Bytes
	2402 Bytes
	2406 Bytes
	2410 Bytes
	2414 Bytes
	2418 Bytes
	2422 Bytes
	2426

(Ein-/Ausgang A) löst ein Lesen auf 16/0/0 (Ein-/Ausgang B) aus. Wenn das Leseflag für Ein-/Ausgang A gesetzt ist, wird die Anfrage vom Ein-/Ausgang A mit einem Antworttelegramm beantwortet. Dabei spielt es keine Rolle, ob 1/0/0 oder 16/0/0 jeweils verschlüsselt sind oder nicht. Es kann z.B. 1/0/0 eine verschlüsselte GA sein und 16/0/0 unverschlüsselt. Auf diese Weise kann daher eine Leseanfrage einer verschlüsselten Gruppenadresse auf eine unverschlüsselte erfolgen. Das gleiche gilt sinngemäß in umgekehrter Richtung.

Zur Einstellung der Kommunikationsrichtung siehe nächster Abschnitt bzw. Tabelle 1.

Die Applikation paart der Übersichtlichkeit halber die Mapper in die Kanäle 1..10 und 11 bis 20. Jeder Kanal, bestehend aus den beiden Ein-/Ausgängen A und B, ist auf die gewünschte Länge einstellbar.

Hinweis:

Der Mapper arbeitet beim Lesen nur mit Gruppenadressen, die mit einem anderen Gerät verbunden sind. Gruppenadressen, die mit den eigenen Kommunikationsobjekten, z.B. KO1 bis KO7 verknüpft sind, werden bei Leseanfragen vom Mapper nicht in der beschriebenen Art und Weise behandelt. Diese werden nicht verarbeitet und gemappt.

Kommunikationsrichtung

Mit Hilfe der Flags der Gruppenadressen kann das „Durchleiten“ von Gruppenadressen durch den Mapper richtungsabhängig und von der Art der Kommunikation (Lesen oder Schreiben) eingestellt werden. Die richtungsabhängige Einstellung für Kommunikationsflags ist in Tabelle 1 angegeben. Dort sind die Kommunikationsflags für Kanal A in der Spalte „Flags A“ und für B in Spalte „Flags B“ eingetragen. Jeweils nicht aufgeführte Flags sind nicht einzustellen.

Die Pfeilrichtung gibt an, in welche Richtung die Kommunikation Lesen oder Schreiben möglich ist. A → B bedeutet, von A nach B ist die Mapper-Richtung wie in Tabelle 1 angegeben möglich, von B nach A erfolgt kein Mapping der Gruppenadresse.

Die Kommunikationsflags findet man in der ETS wie in Abbildung 5 angedeutet.

In der Tabelle 1 bezeichnen die Buchstaben die gleichen Flags wie in der ETS, also z.B. K für Kommunikation, L für Lesen usw.

Abbildung 5: Flags

Richtungen	Lesen	Schreiben	Flags A	Flags B
A ↔ B	ja	ja	K L S Ü -	K L S Ü
A ↔ B	ja	--	K L - Ü	K L - Ü
A ↔ B	--	ja	K - S Ü	K - S Ü
A → B	ja	ja	K L S -	K - S Ü
A → B	ja	--	K L - -	K - S Ü
A → B	--	ja	K - S -	K - S Ü
A ← B	ja	ja	K - S Ü	K L S -
A ← B	ja	--	K - S Ü	K L - -
A ← B	--	ja	K - S Ü	K - S -

Tabelle 1 Kommunikationsrichtung

Anwendungsfall 1: Außenlinie

Der praktische Nutzen des Mappers ist im folgenden Szenario nach Abbildung 6 zu erläutern:

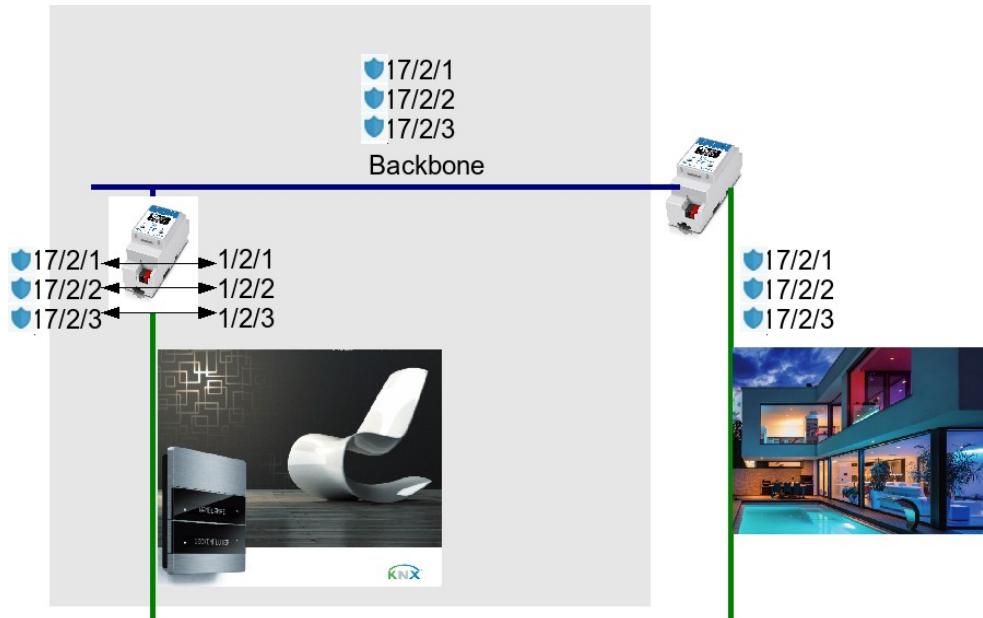


Abbildung 6: Anwendung Mapper

Eine Anlage besteht aus einer Innen- und Außenlinie. Um die Sicherheit der Anlage zu erhöhen, wird beschlossen, die Außenlinie Secure umzurüsten. Z.B. die Öffnung des Garagentors bzw. die Schließung erfolgt über KNX und Secure Kommunikation. Im Beispiel seien das die Gruppenadressen 17/2/1, 17/2/2 und 17/2/3. Diese werden über zwei Router in die Innenlinie geführt. Die Geräte dort realisieren diese Funktionen in der Gruppenkommunikation 1/2/1, 1/2/2 und 1/2/3. Die Innenlinie verfügt aber nur über unverschlüsselte Aktorik und Sensorik. Über den Mapper werden nun die GAs 17/2/1 auf 1/2/1, 17/2/2 auf 1/2/2, 17/2/3 auf 1/2/3 gemappt. Daher können nun die Geräte auf der Innenlinie mit der Außenlinie kommunizieren. Über das Routing von Enertex® IP Secure Router oder gleichermaßen von Enertex TP Secure Coupler kann nun festgelegt werden, dass die Hauptgruppe 17 geroutet wird, aber die Hauptgruppe 2 blockiert wird. Damit kann nun Sicherheit auf der Außenlinie problemlos mit der Innenlinie kombiniert werden.

Anwendungsfall 2: Richtungsabhängiges Mapping

Ein weiteres Anwendungsbeispiel ist das richtungsabhängige Mapping in einer Anlage, bei der (unterschiedliche) Gruppenadressen sowohl unverschlüsselt als auch verschlüsselt kommunizieren. Beispielsweise wird eine Zentralfunktion „Nachtmodus“ auf eine GA 1/2/3 unverschlüsselt gesendet. Diese Zentralfunktion soll sowohl alle Lichter ausschalten als auch das Türschloss schließen, welches auf eine verschlüsselte (secure) Gruppenadresse 17/1/1 kommuniziert (vgl. Abbildung 7).

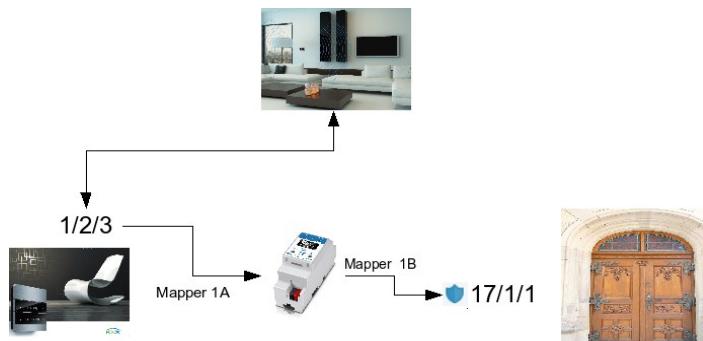


Abbildung 7: Anwendung richtungsabhängiges Mapping

Wenn nun der Mapper mit Hilfe von Tabelle 1 so eingestellt wird, dass Schreiben A → B möglich

ist, und die Verknüpfungen entsprechend der Zeichnung Abbildung 7 erfolgt, so ist die Kommunikation auf der Gruppenadresse 17/1/1 völlig unabhängig vom Zentralbefehl „Nachtmodus“. Gleichzeitig bleibt die Sicherheit des Türschlosses bzw. der Kommunikation über 17/1/1 unabhängig vom Zentralbefehl. Wird nur das Türschloss bedient, so wird auch kein Zentralbefehl an die unverschlüsselte Aktorik geleitet.

Kommunikationsobjekte

Hinweis:

Abhängig von der Parametrierung können einige Objekte nicht verfügbar sein.

ID	Name	Objekt-funktion	Beschreibung	Länge	Typ
1	Externer Zeitserver gültig - Ausgang	Status	<p>Gibt an, ob der externe Zeitserver pool.ntp.org vom Gerät erreichbar ist. Die Namensauflösung erfolgt über den DNS Server 9.9.9.9. Infos hierzu unter www.quad9.net.</p> <p>Wenn ein eigener NTP Zeitserver eingestellt werden soll, muss dessen IP Adresse bekannt sein. In diesem Fall sendet das KO nichts.</p> <p>Die Uhrzeit synchronisiert sich automatisch alle 2 Tage neu mit den externen NTP Server bzw. falls dies mit KO 7 initiiert wird.</p>	1 Bit	[1.2] DPT_Bool
2	Interne Uhr gültig - Ausgang	Status	<p>Gibt an, ob die interne Uhr gültig ist. Wert wahr [1] steht für gültig, Wert falsch [0] für ungültig. Über die Parametrierung kann dass Kommunikationsobjekt nach jedem Neustart automatisch gesendet werden. Bei Auslieferung des Geräts ist das Kommunikationsobjekt gleich falsch [0]. Die Uhr wird dann gültig (Wert = wahr [1]), wenn das Gerät die Uhrzeit über einen NTP Server abfragen und die interne Uhrzeit entsprechend einstellen kann. Nach einem Neustart bzw. einer ETS-Programmierung des Geräts bleibt der Wert weiterhin wahr [1]. Nur in dem Fall, falls der interne Pufferkondensator aufgrund eines mehrtägigen Stromausfalls zu weit entladen wurde, wird die Uhr wieder ungültig (Wert = falsch [0]).</p> <p>Hinweis</p> <p>Wenn das Kommunikationsobjekt KO2 falsch [0] ist, so ist die Uhr nicht synchronisiert. Sollte keine Internetverbindung bestehen, kann die Zeit des Zeitervers über das telnet-Interface per „date“ Befehl (siehe Handbuch des Systemgerätes) gesetzt werden. Das Synchronisieren der Uhr über telnet wirkt dann wie eine Synchronisation über NTP und setzt das Kommunikationsobjekt KO2 auf gültig (Wert = wahr [1]).</p>	1 Bit	[1.2] DPT_Bool
3	Uhrzeit - Ausgang	Zeitausgabe	Kommunikationsobjekt zur Ausgabe der aktuellen Uhrzeit auf den Bus. Die interne Uhr ist für ca. 1,5 Tage intern (per Supercap-Kondensator) gepuffert. Die interne Uhr kann pro 2 Tage um ca. 1 Sekunde von der realen Zeit abweichen. Ein Lesetelegramm liefert stets die aktuelle Zeit.	3 Byte	[10.001] DPT_TimeOfDay
4	Datum - Ausgang	Datums-ausgabe	Kommunikationsobjekt zur Ausgabe des Kalenders der internen Uhr.	3 Byte	[11.001] DPT_Date
5	Uhrzeit und Datum - Ausgang	Zeit- und Datumsausgabe	Uhrzeit und Datum zur Ausgabe der aktuellen Uhrzeit und Datums auf den Bus.	8 Byte	[19.001] DPT_DateTime
6	Datum/Uhrzeit - Eingang	Anfordern	Trigger zum Schreiben von KO 3, KO 4 und KO 5. Es triggert gleichermaßen ein Schreiben von 0 und 1.	1 Bit	[1.017] DPT_Trigger
7	NTP Server Sync: - Eingang	Anfordern	Die interne Uhr synchronisiert sich automatisch alle 2 Tage neu mit dem NTP Server bzw. falls dieses KO geschrieben wird. Es triggert gleichermaßen ein Schreiben von 0 und 1.	1 Bit	[1.017] DPT_Trigger

ID	Name	Objekt-funktion	Beschreibung	Länge	Typ
8	Sommer / Winterzeit - Ausgang	Status	Wenn Sommerzeit aktiv ist, wird dieses KO 0, während der Winterzeit 1. Dieses KO ist daher für die Winterumschaltung von Heizungen direkt nutzbar. Über den Parameter „Invertiere Sommer/Winterzeit Objekt“ kann die Polarität dieses KOs invertiert werden (vgl. Abbildung 1)	1 Bit	[1.xxx]
9	MapperObjekt Kanal A - Feldlänge	Ein/Ausgang	Bei Schreiben oder Antworten auf dieses KO wird der Wert auf das KO des Kanal B auf den Bus geschrieben. Dabei wird die Verschlüsselung der einzelnen Kanäle berücksichtigt. Bei einer Leseanforderung wird diese beantwortet und gleichzeitig eine Leseanforderung auf Kanal B ausgegeben.	1 Bit bis 14 Byte	n.a.
10	MapperObjekt Kanal B - Feldlänge	Ein/Ausgang	Bei Schreiben oder Antworten auf dieses KO wird der Wert auf das KO des Kanal A auf den Bus geschrieben. Dabei wird die Verschlüsselung der einzelnen Kanäle berücksichtigt. Bei einer Leseanforderung wird diese beantwortet und gleichzeitig eine Leseanforderung auf Kanal A ausgegeben.	1 Bit bis 14 Byte	n.a.
Weitere 19 Mapper Kanalpaare					

Aktuelle Daten

Unter <http://www.enertex.de/d-produkt.html> finden Sie die aktuelle ETS Datenbankdatei sowie die aktuelle Produktbeschreibung.