enertexbayern gmbh
simulation entwicklung consulting

Handbuch und Konfiguration

Zeitgeber und Mapper Applikation für Enertex KNX IP Systemgeräte

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

Hinweis

Inhalt

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. Datumstelegramm 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 Nichterreichbarkeit 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 parametriert 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 Werkszustand (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

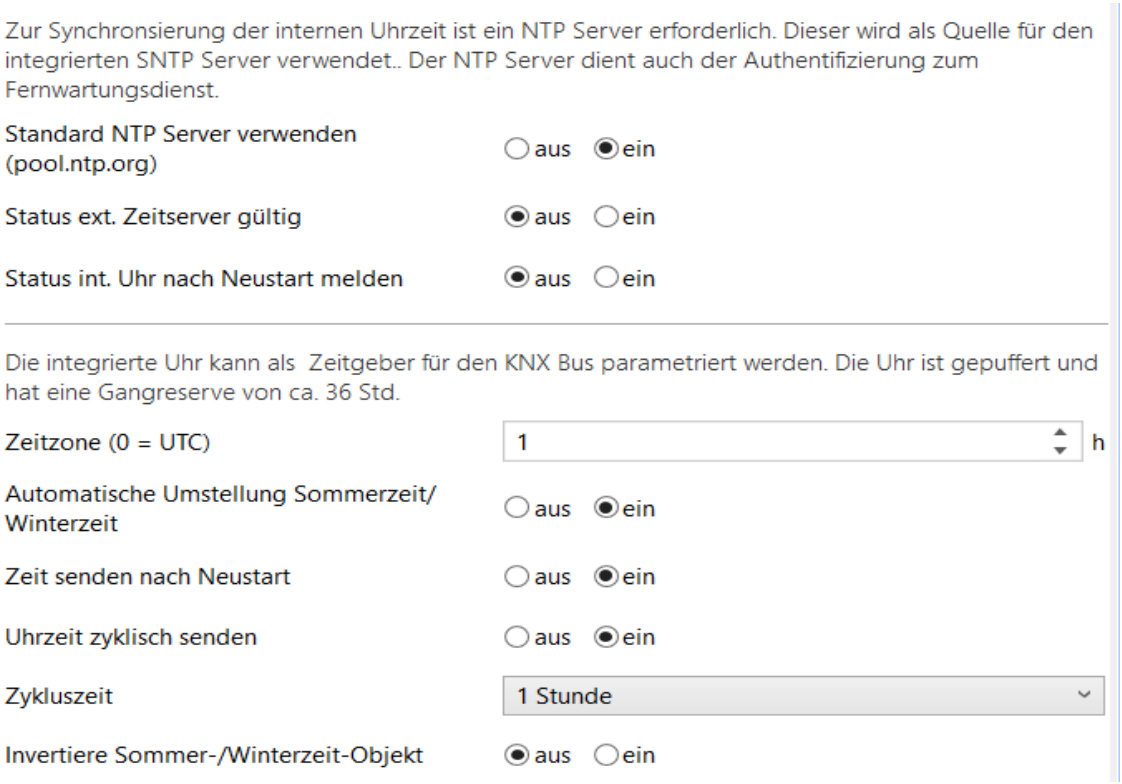

Abbildung 1: Zeitgeber

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, 1 Stunde, 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).

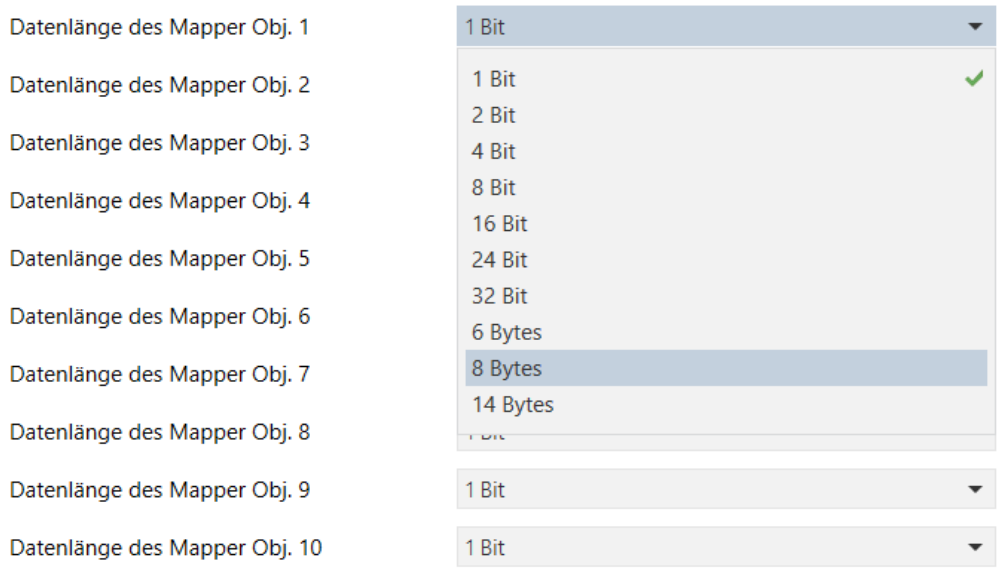

Abbildung 2: Mapper Datentypen

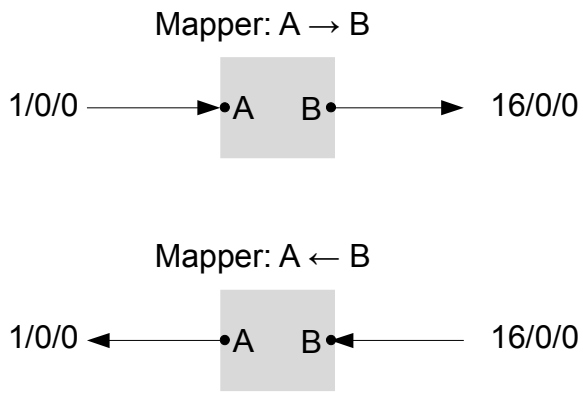

Abbildung 3: Mapper: Schreiben auf Gruppenadressen

Abbildung 3 zeigt die beschriebene Funktionsweise: Ein Schreiben (oder Antworten) auf 1/0/0 (Ein-/Ausgang A) löst ein Schreiben auf 16/0/0 (Ein-/Ausgang B) aus. 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 Gruppenadresse darstellen und und 16/0/0 eine unverschlüsselte. Auf diese Weise wird daher eine (oder mehrere) verschlüsselte Gruppenadresse auf eine unverschlüsselte gesendet. Das gleiche gilt sinngemäß in umgekehrter Richtung. Dabei ist im Falle von mehreren Verknüpfungen gemäß KNX Vorgaben zu beachten, dass maximal nur eine Gruppenadresse sendend ist.

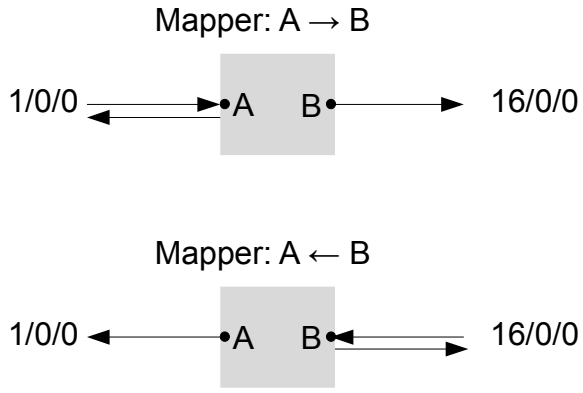

Abbildung 4: Mapper: Lesen auf Gruppenadressen

Abbildung 4 zeigt die beschriebene Funktionsweise für Leseanfragen: Ein Lesen auf 1/0/0

(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.

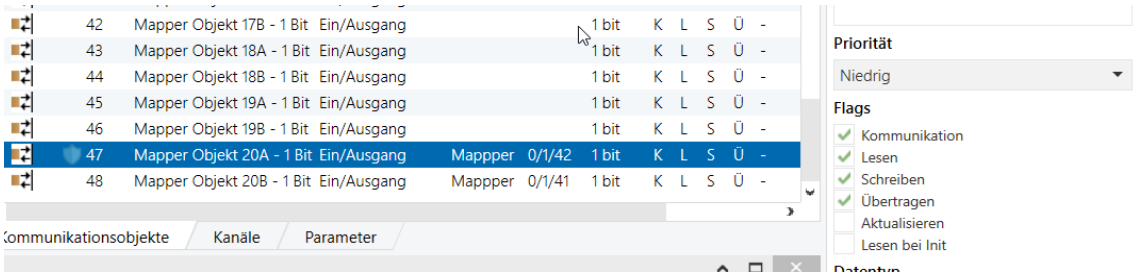

Abbildung 5: Flags

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:

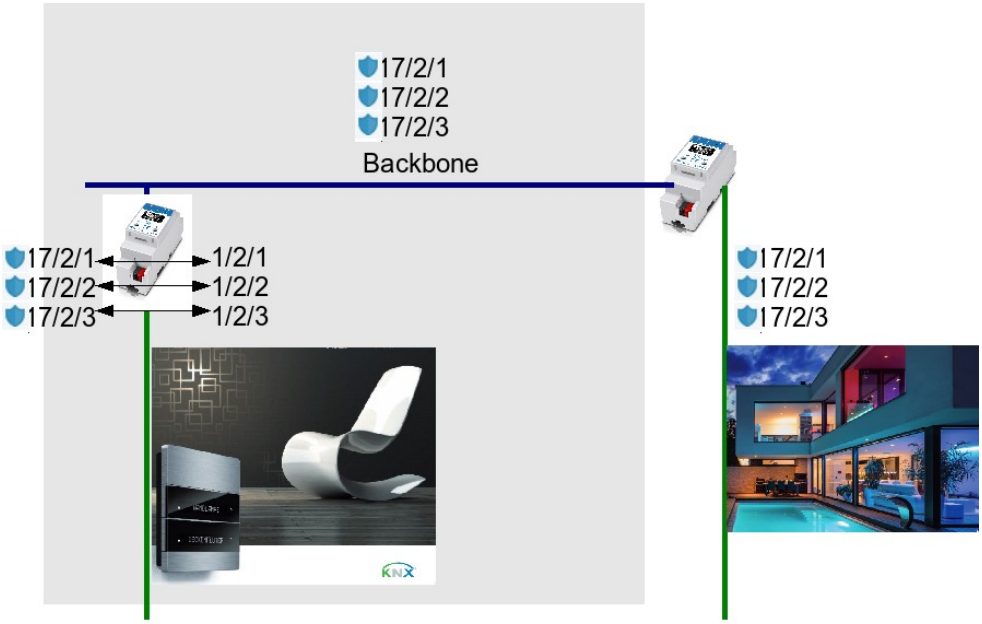

Abbildung 6: Anwendung Mapper

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).

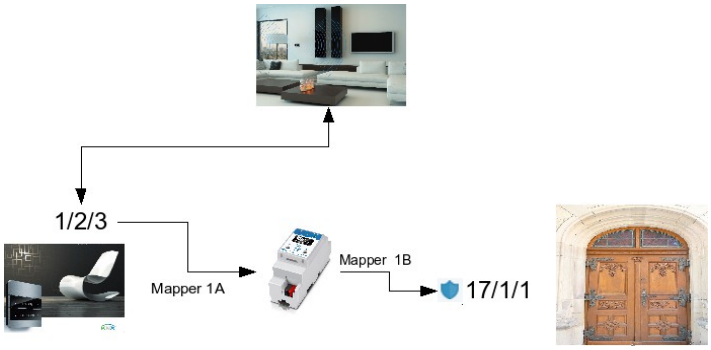

Abbildung 7: Anwendung richtungsabhängiges Mapping

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	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. Wenn ein eigener NTP Zeitserver eingestellt werden soll, muss dessen IP Adresse bekannt sein. In diesem Fall sendet das KO nichts. Die Uhrzeit synchronisiert sich automatisch alle 2 Tage neu mit den externen NTP Server bzw. falls dies mit KO 7 initiiert wird.	1 Bit	[1.2] DPT_Bool
2	Interne Uhr gültig - Ausgang	Status	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]). **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]).	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 - F*eldlänge*	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 - F*eldlänge*	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.