Produktdokumentation

KNX IP-Router

Art.-Nr.: IPR 300 SREG

KNX IP-Schnittstelle

Art.-Nr.: IPS 300 SREG

ALBRECHT JUNG GMBH & CO. KG
Volmestraße 1
58579 Schalksmühle
GERMANY
Tel. +49 2355 806-0
Fax +49 2355 806-204
kundencenter@jung.de
www.jung.de

06/2020

Inhaltsverzeichnis

1 Sicherheitshinweise und Geräteaufbau

1.1 Sicherheitshinweise

Montage und Anschluss elektrischer Geräte dürfen nur durch Elektrofachkräfte erfolgen.

Schwere Verletzungen, Brand oder Sachschäden möglich. Anleitung vollständig lesen und beachten.
Diese Anleitung ist Bestandteil des Produktes und muss beim Endkunden verbleiben.
Dieses Produkt ist nur zur Verwendung in trockenen Räumen bestimmt.

1.2 Geräteaufbau

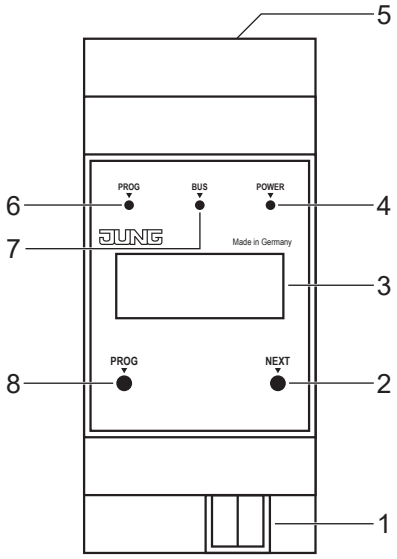

Abb. 1: Geräteaufbau

1	Anschluss KNX	5	Anschluss LAN
2	Taste NEXT	6	LED PROG
3	Display	7	LED BUS
4	LED POWER	8	Taste PROG

2 Funktion

2.1 Systeminformation

Das Gerät ist updatefähig. Firmware-Updates können komfortabel durchgeführt werden.

Das Gerät ist KNX Data Secure fähig. KNX Data Secure bietet Schutz vor Manipulation in der Gebäudeautomation und kann im ETS-Projekt konfiguriert werden. Detaillierte Fachkenntnisse werden vorausgesetzt. Zur sicheren Inbetriebnahme ist ein Gerätezertifikat erforderlich, das auf dem Gerät angebracht ist. Im Zuge der Montage ist das Gerätezertifikat vom Gerät zu entfernen und sicher aufzubewahren.

Planung, Installation und Inbetriebnahme des Gerätes erfolgen mit Hilfe der ETS ab Version 5.7.

2.2 Bestimmungsgemäßer Gebrauch

2.2.1 KNX IP-Router und KNX IP-Schnittstelle

- Verbindung von KNX-Geräten mit PC oder anderen Datenverarbeitungsgeräten via IP
- Montage auf Hutschiene gemäß DIN EN 60715 in Unterverteiler

2.2.2 KNX IP-Schnittstelle

- Betrieb als Datenschnittstelle

2.2.3 KNX IP-Router

- Betrieb als KNX Bereichs-/Linienkoppler oder Datenschnittstelle

2.3 Produkteigenschaften

2.3.1 KNX IP-Router und KNX IP-Schnittstelle

- Unterstützung von KNX Data Secure ab ETS Version 5.7
- Unterstützung von KNX IP Secure ab ETS Version 5.7
- Max. 48 Telegramme pro Sekunde im Modus IP Secure
- LED-Anzeige für KNX-Kommunikation, Ethernet-Kommunikation und Programmiermodus
- Konfiguration über ETS, Telnet oder separatem Softwaretool
- SNTP-Server, gepuffert
- Inbetriebnahme mit Display-Unterstützung
- Max. 8 Verbindungen zu IP-Endgeräten, z.B. zum gleichzeitigen Visualisieren und Konfigurieren
- Ausfallmeldung des KNX-Systems an IP-System
- Galvanische Trennung zwischen KNX und IP-Netzwerk
- Leistungsaufnahme max. 1 W

2.3.2 KNX IP-Router

- KNXnet/IP Routing zur Kommunikation zwischen KNX-Linien, Bereichen und Systemen über das IP-Netzwerk
- Telegrammweiterleitung und Filterung nach physikalischer Adresse oder Gruppenadresse

3 Montage und elektrischer Anschluss

3.1 Information für Elektrofachkräfte

GEFAHR
Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung.
Elektrischer Schlag kann zum Tod führen.
Vor Arbeiten am Gerät freischalten und spannungsführende Teile in der Umgebung abdecken!

3.2 Montage

Gerät auf Hutschiene gemäß DIN EN 60715 in Unterverteiler montieren.

3.3 Anschluss

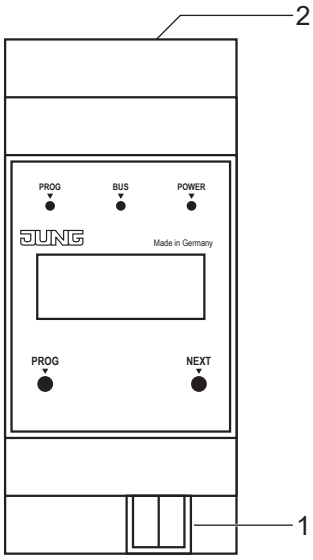

Abb. 2: Anschluss

1 Anschluss KNX 2 Anschluss LAN

Voraussetzungen:

- eine Ethernetverbindung mit 10/100 Mbit
- eine KNX/EIB-Busverbindung

Position der Anschlüsse siehe Geräteaufbau.

• LAN und KNX anschließen.

4 Inbetriebnahme

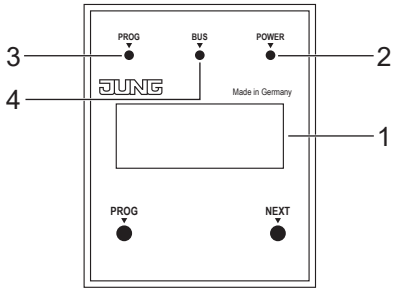

Abb. 3: Inbetriebnahme

1	Display	3	LED PROG
2	LED POWER	4	LED BUS

4.1 Einschalten

Nach dem Anschließen wird das Gerät automatisch eingeschaltet. Beim Einschalten werden auf dem Display der Produktname und die zugewiesene IP-Adresse angezeigt.

4.2 Bootvorgang

Nach dem Einschalten startet der automatische Bootvorgang. Während des Bootvorgangs blinken die drei LEDs auf der Frontseite des Geräts als Lauflicht.

LED PROG – rot

LED BUS – gelb

LED POWER – grün

Die Dauer des Bootvorgangs verlängert sich, wenn dem IP-Router die IP-Adresse per DHCP zugewiesen wird. DHCP wird durch die Werkseinstellungen vorgegeben. Während der Zuweisung der IP-Adresse blinkt die grüne LED POWER.

Am Ende des Bootvorgangs wird die IP-Adresse des Geräts im Display angezeigt.

5 Bedienung

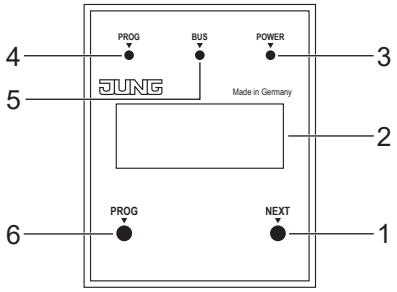

Abb. 4: Bedienung

1	Taste NEXT	4	LED PROG
2	Display	5	LED BUS
3	LED POWER	6	Taste PROG

5.1 Display

Das Display schaltet sich nach einer Minute automatisch aus.

Display einschalten:

• Taste NEXT betätigen.

Menü durchblättern:

• Taste NEXT bei eingeschaltetem Display mehrfach betätigen.

Menüstruktur:

- Seite 1:
  Anzeige der Firmware-Version, IP-Adresse, physikalischen Adresse, Seriennummer und der genutzten Tunnelverbindungen
- Seite 2:
  Anzeige sämtlicher IP-Einstellungen
  Anzeige der Bootzeit
- Seite 3:
  Informationen zur Telegrammlast
- Seite 4:
  Anzeige des IP Secure FDSK (Factory Default Setup Key)
  Wird nur angezeigt, wenn sich das Gerät noch im Auslieferungszustand befindet.
- Seite 5:
  Anzeige des Data Secure FDSK (Factory Default Setup Key)
  Wird nur angezeigt, wenn das Gerät noch nicht in den Secure-Zustand gesetzt wurde.
- Seite 6:
  Anzeige der Geräteuhrzeit
  Wird nur angezeigt, wenn das Gerät die Zusatzapplikation geladen hat.

5.2 LED-Anzeigen

Auf der Frontseite des Geräts befinden sich drei LEDs. Die LEDs signalisieren während des Betriebs folgende Gerätezustände:

- LED PROG leuchtet rot:
  Gerät ist im Programmiermodus.
- LED BUS blinkt gelb:
  Gerätebus ist aktiv.
- LED POWER leuchtet grün:
  Gerät ist betriebsbereit.

Neben dem Anschluss LAN befinden sich zwei weitere LEDs. Die LEDs signalisieren während des Betriebs folgende Gerätezustände:

- grüne LED:
  Verbindung zu einem anderen IP Gerät oder Switch ist hergestellt.
- gelbe LED:
  IP-Datentransfer ist aktiv.

5.3 Programmiermodus

Gerät programmieren:

• Taste PROG betätigen.
  LED PROG leuchtet rot.

Produktapplikation programmieren:

• Taste PROG erneut betätigen.
  LED PROG blinkt rot.

Programmiermodus beenden:

• Taste PROG erneut betätigen.

5.4 Master-Reset

• Sicherstellen, dass das Gerät ausgeschaltet ist (Bus- und Versorgungsspannung trennen).
• Taste PROG drücken, gedrückt halten und Gerät anschließen.
  Das Gerät wird eingeschaltet.
• Taste PROG gedrückt halten bis die LED PROG langsam blinkt (ca. 1 Hz).
• Taste PROG loslassen.
• Taste PROG erneut drücken und gedrückt halten bis die LED PROG schnell blinkt (ca. 4 Hz).
  Der Master-Reset wird durchgeführt.
• Taste PROG kann nun losgelassen werden.

6 Konfiguration

Die Geräte bestehen aus einer Kombination von folgenden Geräten:

- KNX IP-Schnittstelle
- KNX IP-Schnittstelle - Zusatzfunktionen

bzw.

- KNX IP-Router
- KNX IP-Router - Zusatzfunktionen

Die Zusatzfunktionen können beispielsweise für den Zeitgeber genutzt werden.
Die Konfiguration der beiden Geräte erfolgt über die ETS 5.
Um die volle Funktionalität nutzen zu können, sind für beide Geräte Produktapplikationen notwendig.
Beide Geräte benötigen eine eindeutige physikalische Adresse in der ETS.

6.1 Topologie

6.1.1 KNX IP-Schnittstelle

Um die IP-Schnittstelle in ein ETS-Projekt einzufügen, muss dieses eine TP-Line besitzen, in welchen die IP-Schnittstelle als Gerät eingefügt wird.

6.1.2 KNX IP-Router

Um den Router in ein ETS-Projekt einzufügen, muss dieses ein IP-Backbone besitzen.
Beispiel:

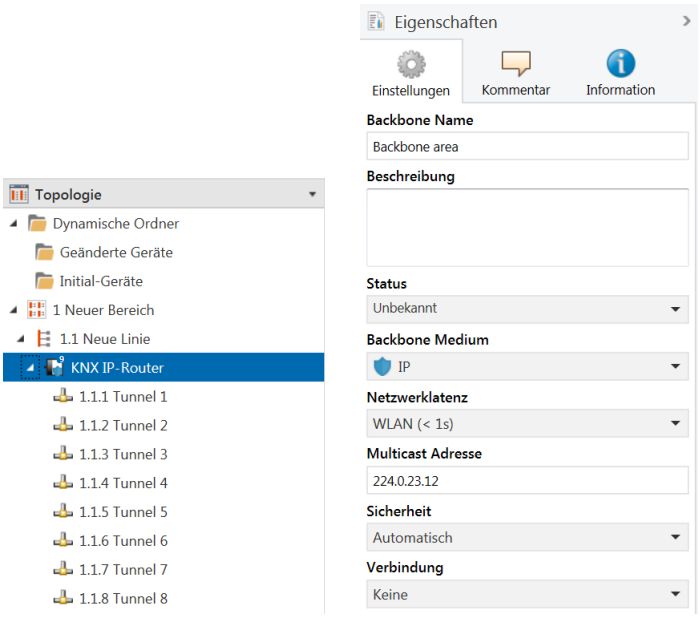

Abb. 5: Topologie (links) und Eigenschaften des Backbone

Linie 1: Backbone Medium IP
Linie 1.1: Linie Medium TP
Im Eigenschaftendialog des Backbones (HINWEIS: Hierzu auf Topologie, direkt oberhalb von „Dynamische Ordner“, vgl. Abbildung 5, klicken), finden sich die Einstellungen zum Multicast des Backbones. Die Netzwerklatenz (vgl. Abbildung 5) kann verändert werden, wenn das Routing über ein großes verteiltes System läuft. In diesem Fall ist die Zeitkonstante zu erhöhen.
Der KNX IP-Router unterstützt bis zu acht KNX-(Secure)-IP-Tunnelverbindungen und kann als Linien- oder Bereichskoppler eingesetzt werden.

6.2 Geräteeigenschaften

6.2.1 Allgemein

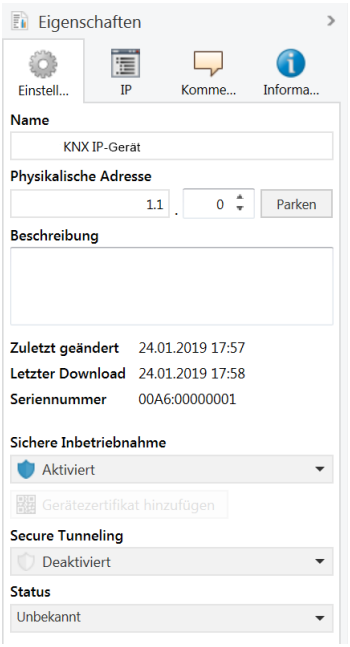

Abb. 6: Eigenschaften des Geräts

Funktion	Beschreibung
Name	Es kann ein beliebiger Name vergeben werden, max. 30 Zeichen.
Sichere Inbetriebnahme	Wenn aktiviert, ist die Verschlüsselung für die Inbetriebnahme aktiv: Es werden dann alle Parameter bereits verschlüsselt übertragen, wenngleich z. B. Tunnelverbindungen noch unverschlüsselt genutzt werden.
Secure Tunneling	Wenn aktiviert, können die Tunnelverbindungen nur über KNX Secure Tunneling aufgebaut werden.

6.2.2 IP-Einstellungen

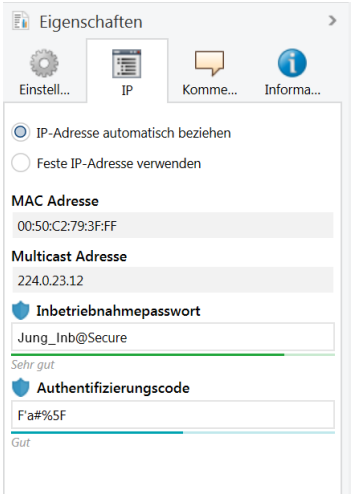

Abb. 7: IP-Einstellungen des Geräts

Funktion	Beschreibung
IP-Adresse automatisch beziehen	Das Gerät benötigt einen DHCP-Server für die IP-Adressvergabe.
Feste IP-Adresse verwenden	Der Anwender gibt die IP-Einstellungen selbst vor.
Inbetriebnahmepasswort	Ein Passwort, aus welchem die ETS einen Schlüssel generiert. Dieser ist der Schlüssel für die Sichere Inbetriebnahme (s. o.).
Authentifizierungscode	Mit dem Authentifizierungspasswort beweist der Anwender, dass er Zugriff auf das Projekt hat.
MAC-Adresse	Wird vom Gerät vorgegeben.
Multicast-Adresse	Wird vom Backbone (vgl. Abbildung 5) vorgegeben.

6.2.3 KNX IP Secure

Für einen fehlerfreien Betrieb der Geräte im abgesicherten Modus (Secure Mode) benötigt man die ETS 5.7.0 oder höher.

Voraussetzungen:

- Sichere Inbetriebnahme aktiviert
- FDSK eingegeben/eingescannt bzw. Gerätezertifikat hinzugefügt

Konfiguration von KNX IP Secure:

- Secure Tunneling aktivieren.
- Passwort für jeden Tunnel (max. 8 Tunnel) festlegen.
- Passwort für Inbetriebnahme und Authentifizierungscode festlegen.

ⓘ Alle Passwörter dokumentieren und sicher aufbewahren.

6.2.4 KNX Data Secure

KNX Data Secure signiert und verschlüsselt die Kommunikation im KNX-Netzwerk und gewährleistet eine gesicherte Datenübertragung von Telegrammen.

Die Kommunikation bei Inbetriebnahmevorgängen mit der ETS und die Laufzeitkommunikation zwischen Geräten sowie zu Visualisierungen ist hierdurch gesichert. Somit wird gewährleistet, dass unabhängig vom Medium alle oder nur ausgewählte KNX-Telegramme authentifiziert und verschlüsselt werden. Die Kommunikation zwischen Sender und Empfänger ist weder interpretierbar noch manipulierbar.

Voraussetzungen:

- ETS 5.7.4 oder höher
- FDSK eingegeben/eingescannt bzw. Gerätezertifikat hinzugefügt

Zur KNX Secure-Inbetriebnahme ist ein Gerätezertikat erforderlich, das seitlich auf dem Gerät angebracht ist.

Bestandsgeräte an denen kein Gerätezertifkat (IP Secure/Data Secure) angebracht ist, können das Gerätezertifikat im Display anzeigen. Weitere Informationen sind im Kapitel zum Display enthalten.

6.2.5 Zusatzfunktionen

Abb. 8: Zusatzfunktionen Eigenschaften des Geräts

Funktion	Beschreibung
Name	Es kann ein beliebiger Name vergeben werden, max. 50 Zeichen.
Sichere Inbetriebnahme	Wenn aktiviert, ist die Verschlüsselung für die Inbetriebnahme aktiv: Es werden dann alle Parameter bereits verschlüsselt übertragen, wenngleich z. B. Tunnelverbindungen noch unverschlüsselt genutzt werden.

Die Zusatzapplikation stellt folgende weitere Funktionalitäten zur Verfügung:

- Zeitgeber
- Fernwartung – Nur IP-Schnittstelle
- Mapper

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)
- Benutzergesteuerte Synchronisierung mit externem Zeitserver

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 alle 48 Stunden und beim Neustart mit dem NTP-Server synchronisiert. Der Anwender kann über ein Kommunikationsobjekt (nachfolgend KO genannt) die Synchronisierung manuell anfordern.

Die „Gültigkeit“ der Uhrzeit wird über ein separates KO ausgegeben. Solange die eingebaute Echtzeituhr versorgt wird, 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.

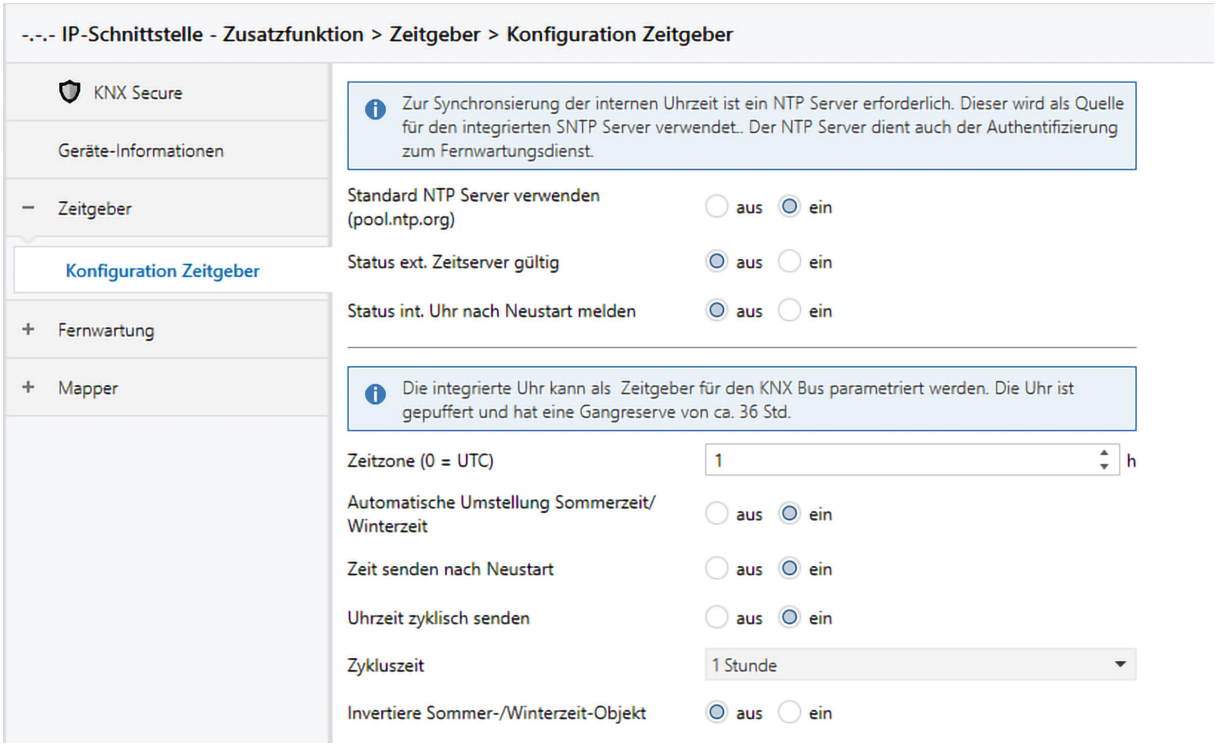

Abb. 9: Zusatzfunktionen Zeitgeber

Funktion	Auswahl	Beschreibung
Standard NTP-Server verwenden (pool.ntp.org)	aus/<u>ein</u>	Vgl. Parameterdialog Falls hier „aus“ gewählt wird, erscheint ein Eingabefeld für die IP-Adresse des eigenen externen Zeitservers
Status ext. Zeitserver gültig	<u>aus</u>/ein	Meldung über KO1
Status int. Uhr nach Neustart melden	<u>aus</u>/ein	Meldung über KO2
Zeitzone (0 = UTC)	-12 ... <u>1</u> ... +14	Stundenversatz der internen Uhr zu UTC
Automatische Umstellung Sommerzeit/Winterzeit	aus/<u>ein</u>	
Zeit senden nach Neustart	aus/<u>ein</u>	Ausgabe von Zeit und Datum auf KO3, KO4, KO5

Funktion	Auswahl	Beschreibung
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

Bei Auslieferung des Geräts ist die interne Uhr ungültig, das Kommunikationsobjekt KO2 ist daher false [0].
Die interne Uhr wird gültig (Wert = wahr [1]), wenn das Gerät einen externen Zeitserver (NTP-Server) erreichen kann.
Dies erfolgt nach jedem Neustart bzw. jede Woche einmal automatisch. Hierzu muss der angegebene NTP-Server erreichbar sein.
Nach einem Neustart bzw. einer ETS-Programmierung des Geräts bleibt die Uhrzeit weiterhin gültig.
Nur im Fall, dass die Gangreserve der internen Uhr aufgrund eines mehr als 36-stündigen Stromausfalls zu stark entladen wurde, wird die Uhr wieder ungültig.
Die interne Uhr kann pro 2 Tage um ca. 1 Sekunde von der realen Zeit abweichen.

Mapper

- Übersetzung von verschlüsselte (secure) auf unverschlüsselte (plain) Kommunikationsobjekte
- Mapping von bis zu 20 Kommunikationsobjekten
- Größe jedes Kommunikationsobjekts parametrierbar zwischen 1 Bit, 2 Bit, 4 Bit , 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes und 14 Bytes

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekte. Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Der Anwender kann die Kommunikationsobjekte so konfigurieren, dass die Gruppenadressen unterschiedliche Längen (max. 14 Byte) aufweisen.

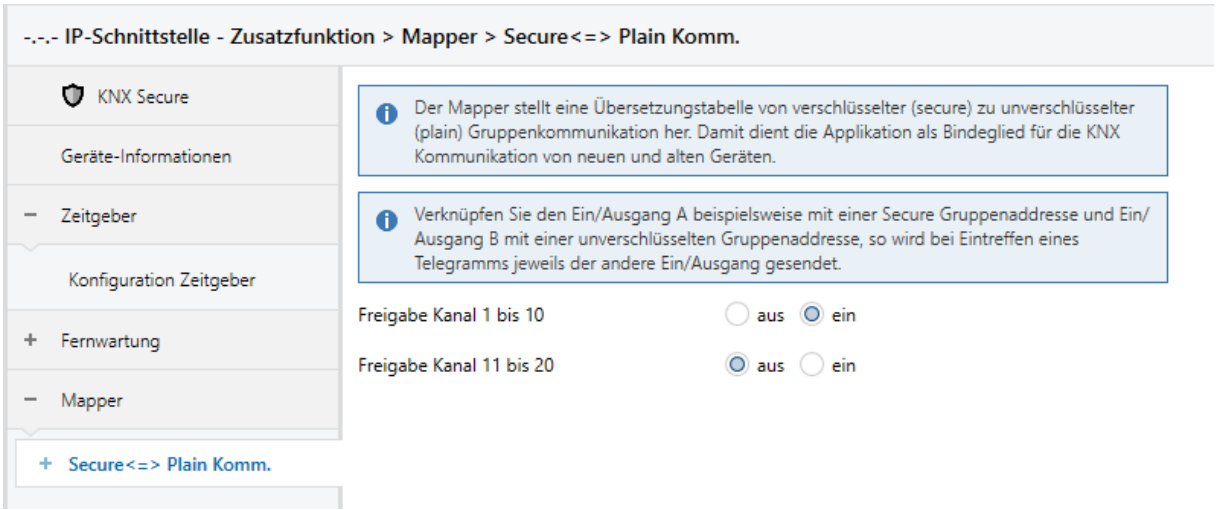

Abb. 10: Zusatzfunktionen Mapper

Funktion	Auswahl	Beschreibung
Freigabe Kanal 1 bis 10	aus/ein	s. u.
Freigabe Kanal 11 bis 20	aus/ein	s. u.

Der Mapper dient der Übersetzung von verschlüsselten (secure) auf unverschlüsselte (plain) Kommunikationsobjekte. Dazu stellt der Mapper 20 Kanäle zur Verfügung, die bidirektional die Kommunikation herstellen. Der Anwender kann die Kommunikationsobjekte so konfigurieren, dass die Gruppenadressen unterschiedliche Längen (max. 14 Byte) aufweisen. Die Länge kann parametriert werden zwischen 1 Bit, 2 Bit, 4 Bit , 8 Bit, 16 Bit, 24 Bit, 32 Bit, 6 Bytes, 8 Bytes und 14 Bytes.

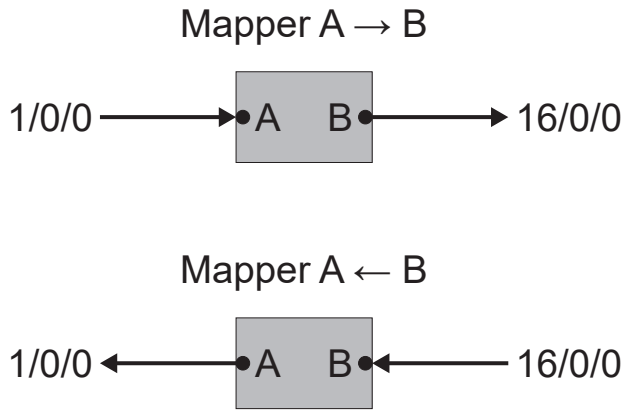

Abb. 11: Mapper Schreiben auf Gruppenadressen

Abbildung 11 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 16/0/0 eine unverschlüsselte. Auf diese Weise werden daher eine (oder mehrere) verschlüsselte Gruppenadressen 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.

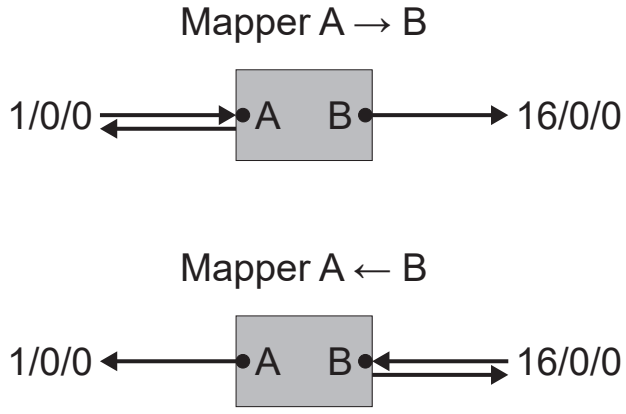

Abb. 12: Mapper Lesen auf Gruppenadressen

Abbildung 12 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. Wenn danach die beteiligten Kommunikationspartner ein Antworttelegramm senden, so wird dieses behandelt wie in Abbildung 11. 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.

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

ⓘ Der Mapper arbeitet nur mit Gruppenadressen, die mit einem anderen Gerät verbunden sind. Gruppenadressen, die mit den eigenen Kommunikationsobjekten, z. B. KO1 bis KO13 verknüpft sind, werden vom Mapper nicht in der beschriebenen Art und Weise behandelt.

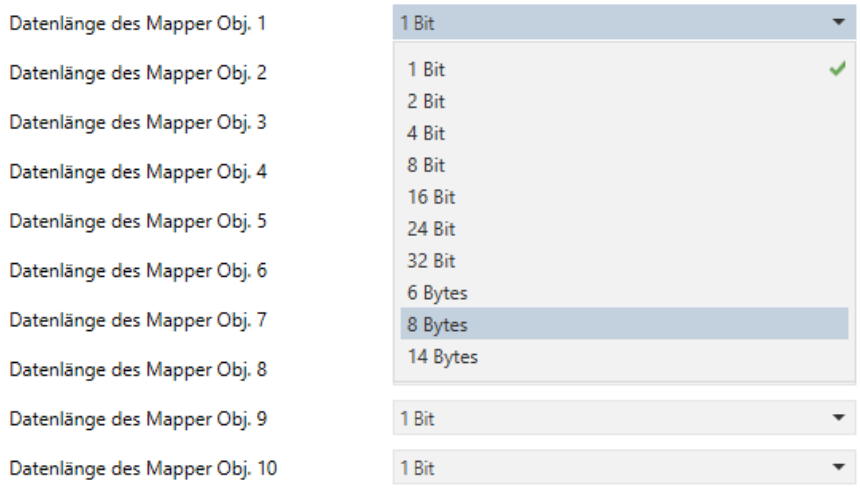

Abb. 13: Mapper Datenlänge

Kommunikationsrichtungen:

Mit Hilfe der Flags der Gruppenadressen kann das „Durchleiten“ von Gruppenadressen durch den Mapper richtungsabhängig und abhängig von der Art der Kommunikation (Lesen oder Schreiben) eingestellt werden. Dazu müssen die Kommunikationsflags wie in der Tabelle gesetzt werden.

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 der Tabelle angegeben möglich, von B nach A erfolgt kein Mapping der Gruppenadresse.

Die Kommunikationsflags findet man in der ETS wie in Abbildung 14 angedeutet.

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

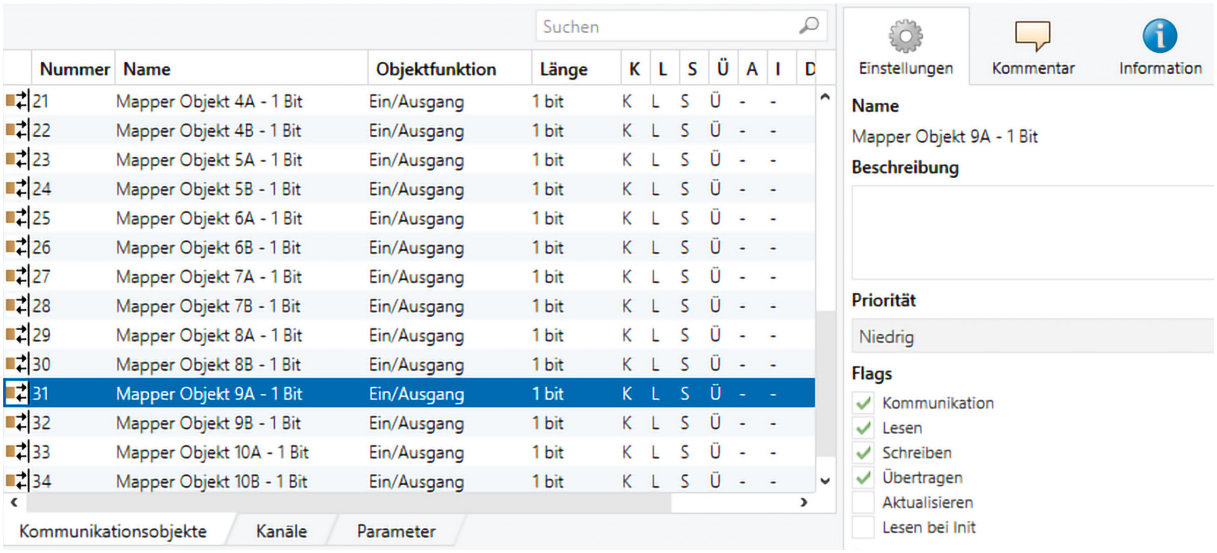

Abb. 14: Mapper Flags

Richtungen	Lesen	Schreiben	Flags A	Flags B
A ↔ B	ja	ja	KLSÜ--	KLSÜ--
A ↔ B	ja	–	KL-Ü--	KL-Ü--
A ↔ B	–	ja	K-SÜ--	K-SÜ--
A → B	ja	ja	KLS---	K-SÜ--
A → B	ja	–	KL----	K-SÜ--
A → B	–	ja	K-S---	K-SÜ--
A ← B	ja	ja	K-SÜ--	KLS---
A ← B	ja	–	K-SÜ--	KL----
A ← B	–	ja	K-SÜ--	K-S---

6.3 Gerätespezifische Parameter

6.3.1 KNX IP-Schnittstelle

Allgemeine Einstellungen

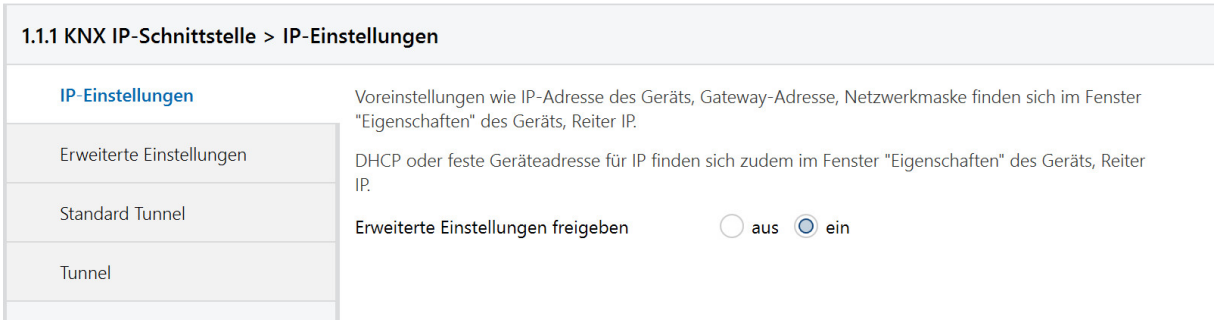

Abb. 15: Allgemeine Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
(Erläuternder Text)		Die ETS hat herstellerunabhängig einheitliche Parameterbeschreibungen für verschiedene Einstellungen. Um die Anwendung zu vereinfachen, wird hier ein Hinweistext eingeblendet.
Erweiterte Einstellungen freigeben	aus/ein	Erweiterte Funktionen, um den Anwendern die max. Flexibilität zu gewährleisten.

Erweiterte Einstellungen

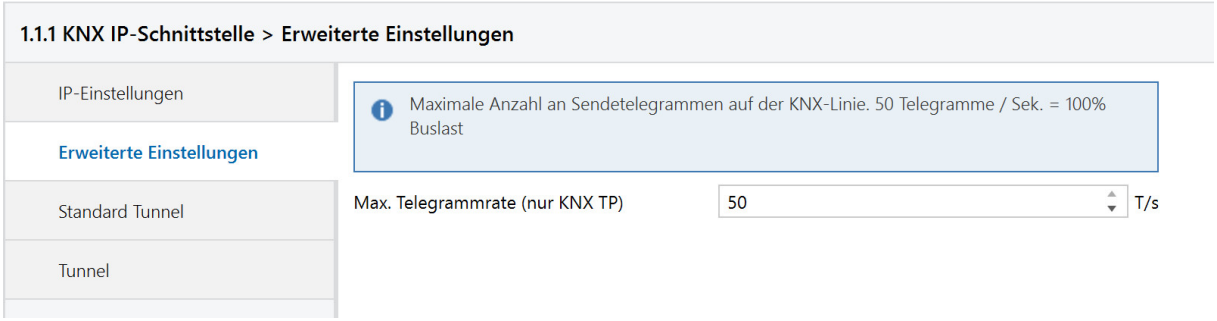

Abb. 16: Erweiterte Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
Max. Telegrammrate	5 .. 50	Vgl. Parameterbeschreibung

Erweiterte Einstellungen Standard Tunnel bevorzugte IP

Die KNX IP-Schnittstellen bieten für Standard-Tunnelverbindungen (vor 2019) die Möglichkeit, jede dieser Tunnelverbindungen jeweils einer IP-Adresse zuzuordnen. Dies ermöglicht bei der Analyse von Gruppentelegrammen eine leichtere Zuordnung der Telegramme zum Sender, der hinter dem Tunnel „sitzt“, wie z. B. Visualisierungen oder Smartphone-Apps.

ⓘ Diese Zuordnung kann allerdings jederzeit durch die ETS oder eine neue sog. erweiterte Tunnelverbindung (Stand 2019) aufgelöst werden.

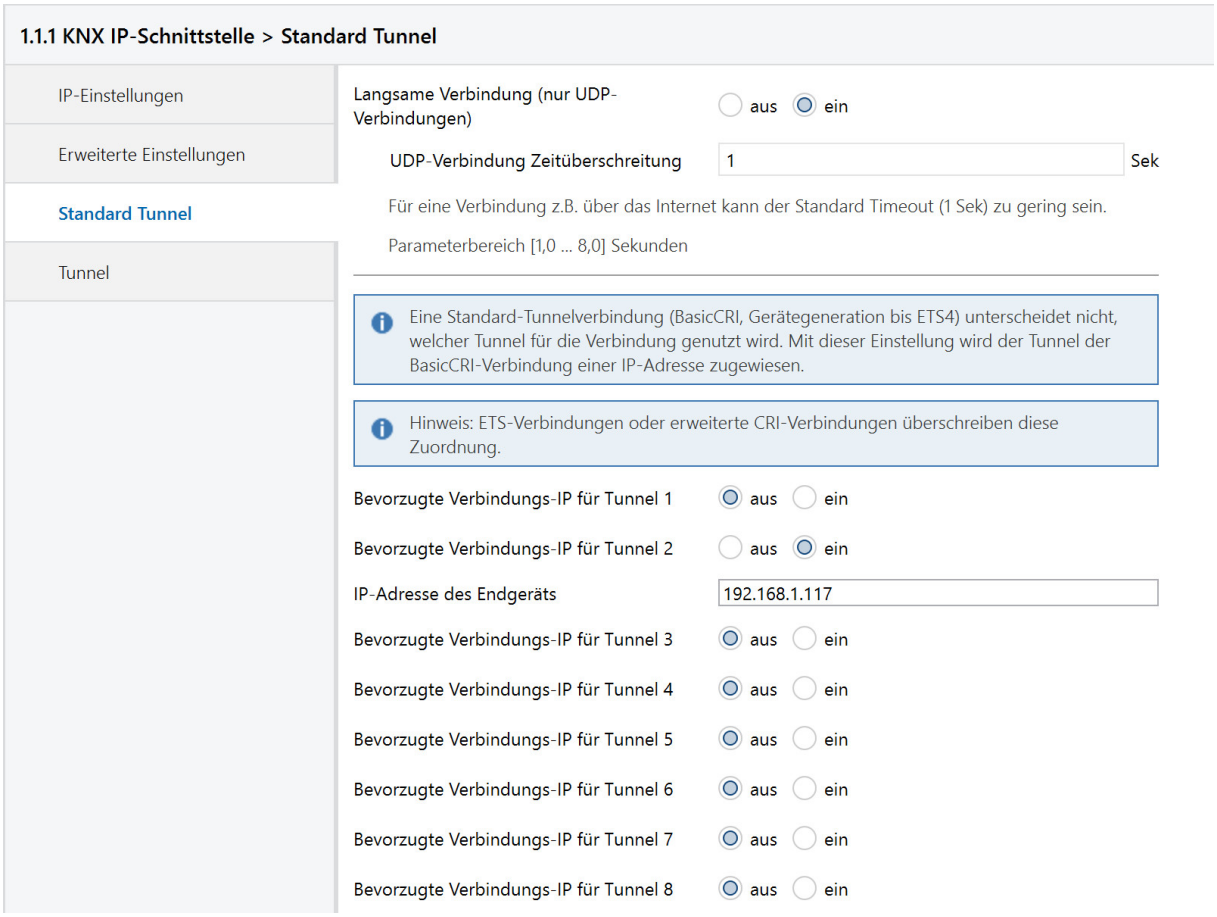

Abb. 18: Bevorzugte Verbindungs-IP für Tunneling

Funktion	Auswahl	Beschreibung
Langsame Verbindung	aus/ein	Die Tunnelverbindungen über UDP werden standardmäßig mit einem Verbindungstimeout von 1 Sekunde betrieben. Dies kann bei Verbindungen über das Internet zu kurz sein.
UDP-Verbindung Zeitüberschreitung	1,0 ... 8,0 sec	Einstellung des Timeouts für UDP-Tunnelverbindungen
Bevorzugte Verbindungs-IP für Tunnel X	aus/ein	Tunnel X soll bevorzugt für eine IP-Adresse verwendet werden.
IP-Adresse des Endgeräts	(IP-V4-Adresse)	IP-Adresse des Endgeräts.

Zusatzfunktion Fernwartung

Die Fernwartung ermöglicht einen Fernzugriff über den KNX-Bus bzw. dort angeschlossenen KNX-Geräten über eine Internetverbindung nach Freigabe durch den Kunden.

Vor der Nutzung ist eine kostenpflichtige Freischaltung durch die Fernzugriffslizenz „IPS-L“ notwendig.

Die Verbindung wird durch die IP-Schnittstelle hergestellt. Die Daten sind voll verschlüsselt und können weder interpretiert noch verändert werden. Die Fernwartung funktioniert unabhängig von der Art des Internetanschlusses (IPv4,IPv6) und benötigt keine Konfiguration der lokalen Netzwerkumgebung.

Nach Freigabe über ein Kommunikationsobjekt stellt die IP-Schnittstelle eine Verbindung zum Remote Access Server (RAS) her.

Die ETS-App JUNG IPS-Remote verbindet sich ebenfalls zu diesem Server und stellt die zugehörige Verbindung her. Um eine verschlüsselte Verbindung zwischen der ETS und der entfernten IP-Schnittstelle herzustellen, ist die neue Datenschnittstelle „IPS-Remote“ zu nutzen.

Weitere Informationen zur Einrichtung können Sie dem Quick Start Guide auf unserer Webseite entnehmen.

- Secure Tunnelling (verschlüsselt) nach KNX-Standard für die Fernwartungsverbindung
- Umschalten zwischen verschlüsselten und unverschlüsselten Tunnelling ohne Neustart
- Erhaltung von Verbindungen beim Umschalten
- Statusobjekte für die Inbetriebnahme

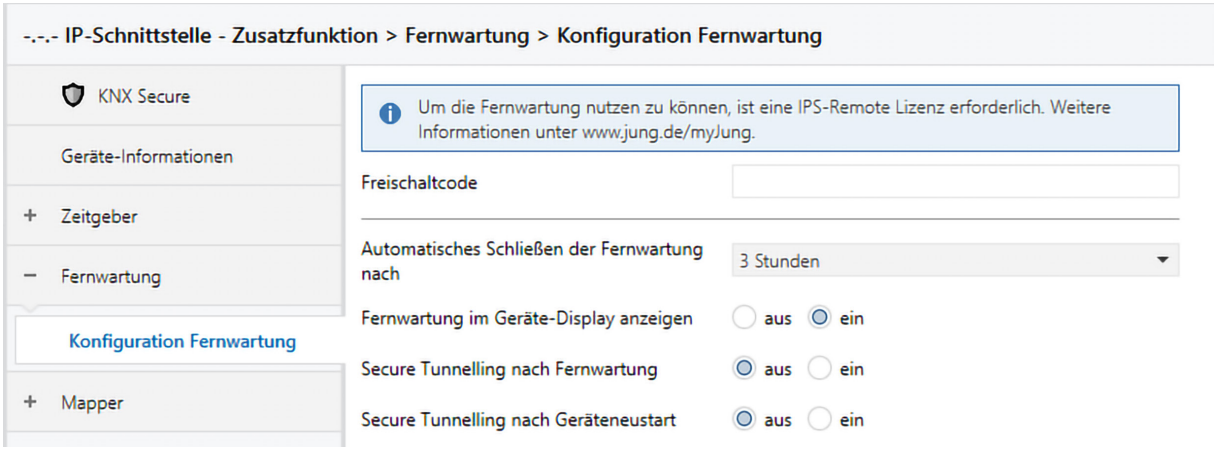

Abb. 19: Zusatzfunktion Fernwartung

Funktion	Auswahl	Beschreibung
Freischaltcode	64 Zeichen	erhältlich über MyJUNG
Automatisches Schließen der Fernwartung	24 Stunden, 12 Stunden, 3 Stunden, 1 Stunde, 30 Minuten, 15 Minuten	
Fernwartung im Gerätedisplay anzeigen	aus/ein	Meldung über KO1
Secure Tunnellling nach Fernwartung	aus/ein	s. u.
Secure Tunnellling nach Geräteneustart	aus/ein	s. u.

Um die Fernwartung nutzen zu können, muss die die Hauptapplikation der IP-Schnittstelle mit der sicheren Inbetriebnahme eingerichtet werden. Zudem ist das Secure Tunneling zu aktivieren.

ⓘ Das Secure Tunneling wird nur für die Fernwartung benötigt.
Ein Verbindungsaufbau mit sämtlichen Visualisierungslösungen ist weiterhin wie gewohnt möglich.

- Aktivieren Sie unter Eigenschaften die Sichere Inbetriebnahme und fügen Sie das Gerätezertifikat hinzu.
- Im Anschluss aktivieren Sie das Secure Tunneling.

Weitere Voraussetzungen für die Fernwartung:

- permanente Internetverbindung am Inbetriebnahme-PC und in der Anlage, in der die IP-Schnittstelle verbaut wurde
- Firmwareupdate der IP-Schnittstelle auf Version 1.0.55 oder höher durchgeführt
- Lizenz für IPS-Remote (IPS-L) erworben
- sichere Inbetriebnahme (IP Secure) der IP-Schnittstelle durchgeführt
  - Secure Tunnelling aktiviert
- Zusatzapplikation geladen, physikalische Adresse und Applikationsprogramm übertragen
  - Freischaltcode für IPS-Remote eingetragen
  - Kommunikationsobjekt 9: Fernwartung freigegeben und Objekt verknüpft
  - Kommunikationsobjekt 2: Interne Uhr gültig
- ETS-Applikation für IPS-Remote geladen
  - erstmalig lokal mit der IP Schnittstelle synchonisiert
  - nach der Freischaltung per Kommunikationsobjekt mit der IP-Schnittstelle verbunden

Expertenwissen:
Bei Spannungsunterbrechung wird die Fernwartungsverbindung abgemeldet bzw. deaktiviert.
Falls aktiviert, wird nach dem Neustart die Verbindung automatisch wiederhergestellt.
Der Zustand der Fernwartung kann am Gerätedisplay (vgl. Abbildung 15) abgelesen werden.
Wenn keine Fernwartung aktiv ist, werden die Standardseiten des Geräts angezeigt (vgl. Abschnitt Anzeigen). Während der Fernwartung ist das Display permanent aktiv, um jederzeit detaillierte Informationen anzeigen zu können.
Beim Starten der Fernwartung erscheint im Display:

```
Remote Access active
====================
```

Ggf. wird (automatisch) Sicheres Tunnelling eingeschaltet und dann die Verbindung zum Relaisserver aufgebaut. Falls nicht, wird jeweils für 30 Sekunden das Gerät von sich versuchen, die Verbindung herzustellen, bis die parametrierte Zeit „Automatisches Schließen der Fernwartung“, Abbildung 15, abgelaufen ist. Während dieser Zeit, erscheint im Display:

```
Remote Access active
====================
→ RAS wait for reconnect
```

Wenn die Verbindung zum Relaisserver erfolgreich war, erscheint im Display:

```
Remote Access active
====================
→ Device secured
→ RAS opened
```

Wenn sich nun die ETS-App JUNG IPS-Remote der Fernwartung am Gerät anmeldet, wird die Anzeige um eine Zeile ergänzt:

```
Remote Access active
====================
→ Device secured
→ RAS opened
→ Remote ETS opened
```

Falls sich die ETS-App JUNG IPS-Remote wieder abmeldet (Aktualisierung-Zeitversatz wie bei KO13, s. dort), erscheint im Display:

```
Remote Access active
====================
→ Device secured
→ RAS opened
→ Remote ETS closed
```

In diesem Fall besteht noch die Verbindung zum Server.

Alsbald die Fernwartung über KO9 ausgeschaltet wird, ist wieder die Standardanzeige des Geräts (vgl. Abschnitt Anzeigen) sichtbar.

6.3.2 KNX IP-Router

Allgemeine Einstellungen

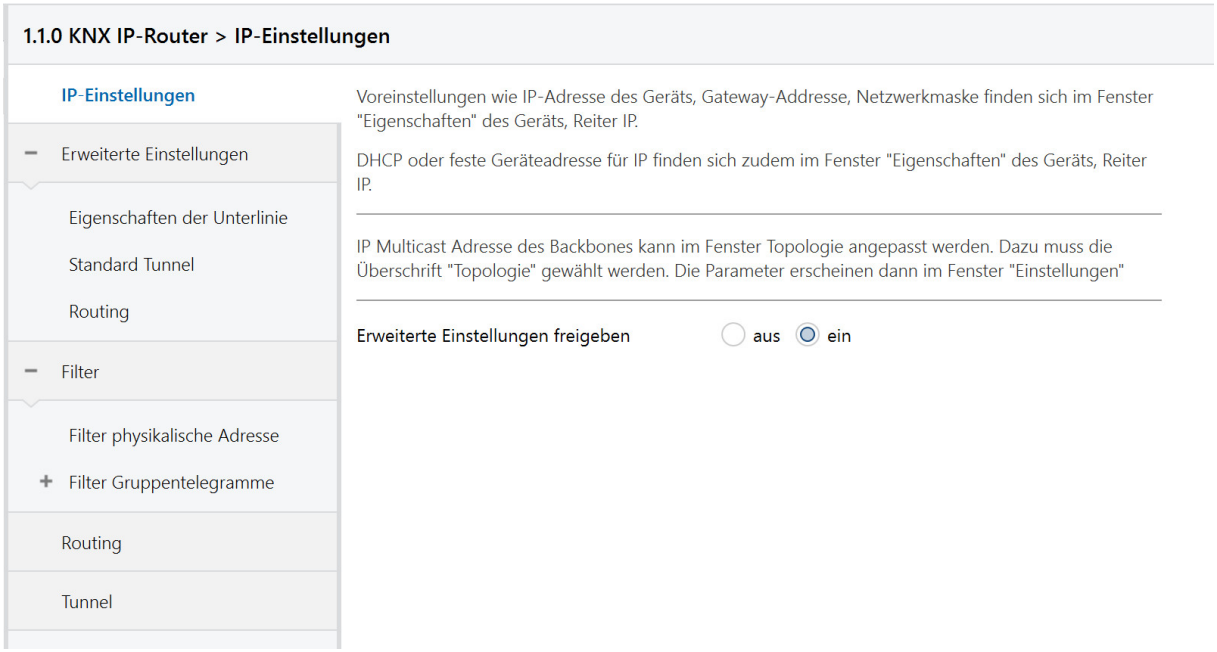

Abb. 20: Allgemeine Einstellungen des Geräts

Funktion	Auswahl	Beschreibung
(Erläuternder Text)		Die ETS hat herstellerunabhängig einheitliche Parameterbeschreibungen für verschiedene Einstellungen. Um die Anwendung zu vereinfachen, wird hier ein Hinweistext eingeblendet.
Erweiterte Einstellungen freigeben	aus/ein	Erweiterte Funktionen, um den Anwendern die max. Flexibilität zu gewährleisten.

Erweiterte Einstellungen Eigenschaften der Unterlinie

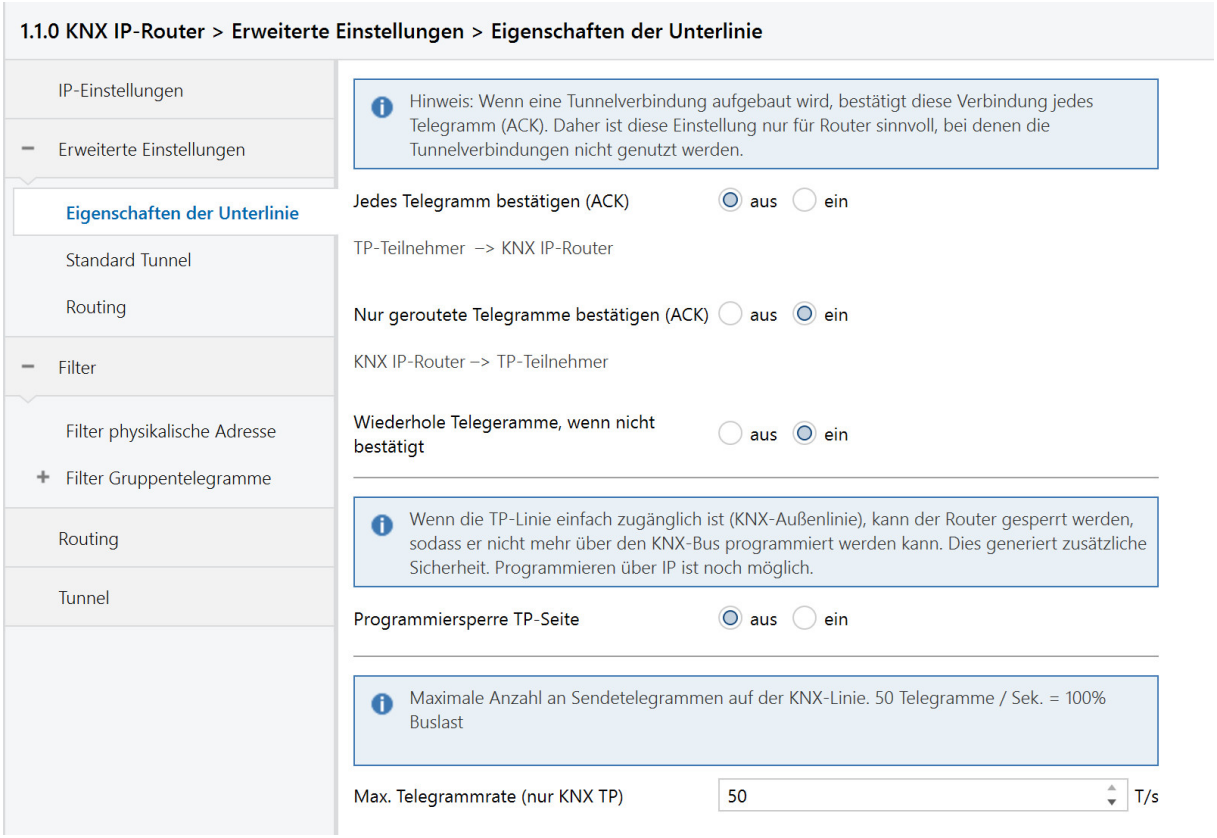

Abb. 21: Eigenschaften der Unterlinie

Funktion	Auswahl	Beschreibung
Jedes Telegramm bestätigen (ACK)	aus/ein	Der Router bestätigt jedes Telegramm, auch wenn er dieses nicht weiterleitet (nur TP)
Nur geroutete Telegramme bestätigen (ACK)	aus/ein	Der Router bestätigt nur die Telegramme, die er weiterleitet (nur TP)
Wiederhole Telegramme, wenn nicht betätigt	aus/ein	Der Router wiederholt nicht bestätigte phy. adressierte Telegramme (nur TP)
Programmiersperre TP-Seite	aus/ein	Vgl. Parameterbeschreibung
Max. Telegrammrate	5 .. 50	Vgl. Parameterbeschreibung

Erweiterte Einstellungen Standard Tunnel bevorzugte IP

Für Standard-Tunnelverbindungen (vor 2019) besteht die Möglichkeit, jede dieser Tunnelverbindungen jeweils einer IP-Adresse zuzuordnen. Dies ermöglicht bei der Analyse von Gruppentelegrammen eine leichtere Zuordnung der Telegramme zum Sender, der hinter dem Tunnel „sitzt“, wie z. B. Visualisierungen oder Smartphone-Apps.

ⓘ Diese Zuordnung kann allerdings jederzeit durch die ETS oder eine neue sog. erweiterte Tunnelverbindung (Stand 2019) aufgelöst werden.

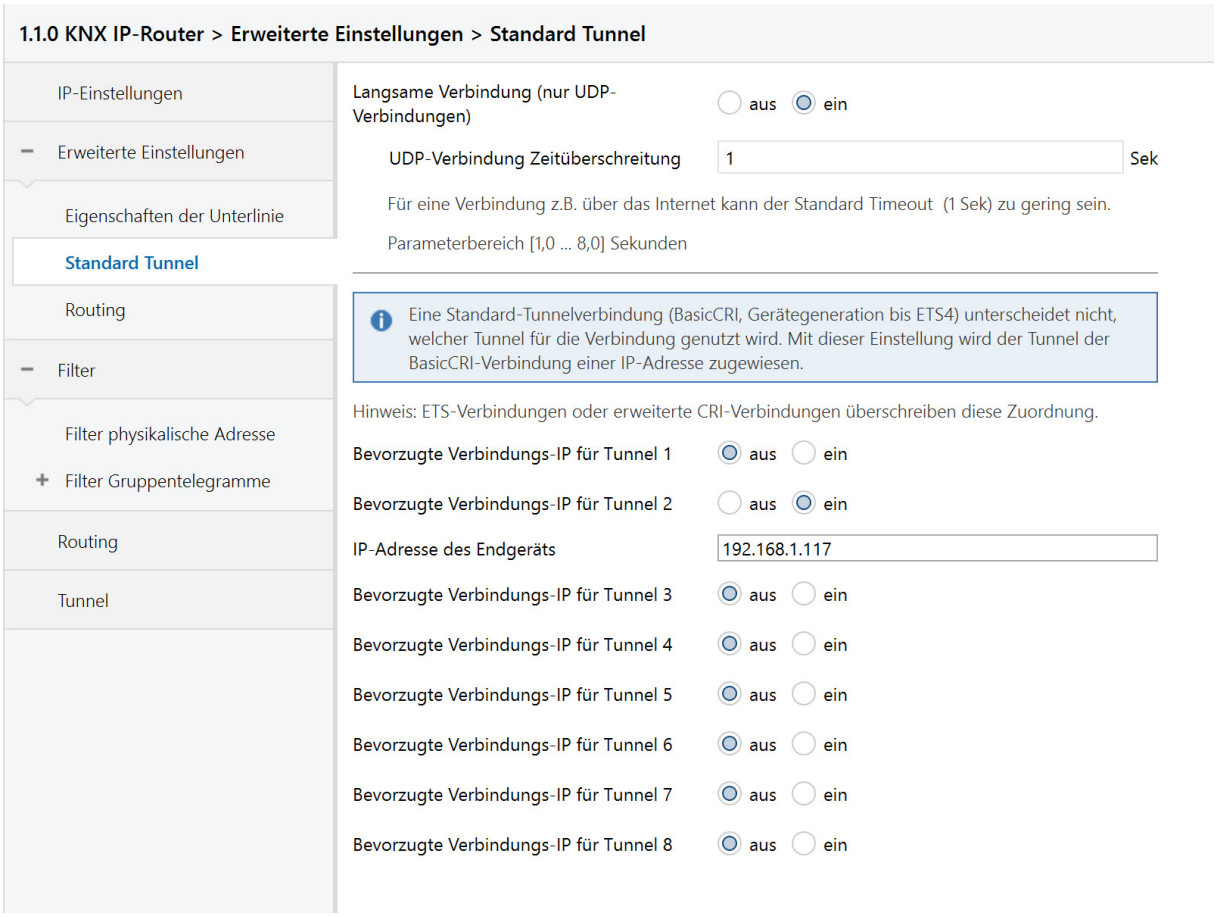

Abb. 22: Standard Tunnel

Funktion	Auswahl	Beschreibung
Langsame Verbindung	aus/ein	Die Tunnelverbindungen über UDP werden standardmäßig mit einem Verbindungstimeout von 1 Sekunde betrieben. Dies kann bei Verbindungen über das Internet zu kurz sein.
UDP-Verbindung Zeitüberschreitung	1,0 ... 8,0 sec	Einstellung des Timeouts für UDP-Tunnelverbindungen
Bevorzugte Verbindungs-IP für Tunnel X	aus/ein	Tunnel X soll bevorzugt für eine IP-Adresse verwendet werden.
IP-Adresse des Endgeräts	(IP-V4-Adresse)	IP-Adresse des Endgeräts

Erweiterte Einstellungen Routing

Abb. 23: Routing

Funktion	Auswahl	Beschreibung
Überprüfung der Topologie	aus/ein	Vgl. Parameterbeschreibung
Aktivierung Routing Algorithmus (<2018)	aus/ein	Vgl. Parameterbeschreibung

Filter physikalisch adressierte Telegramme

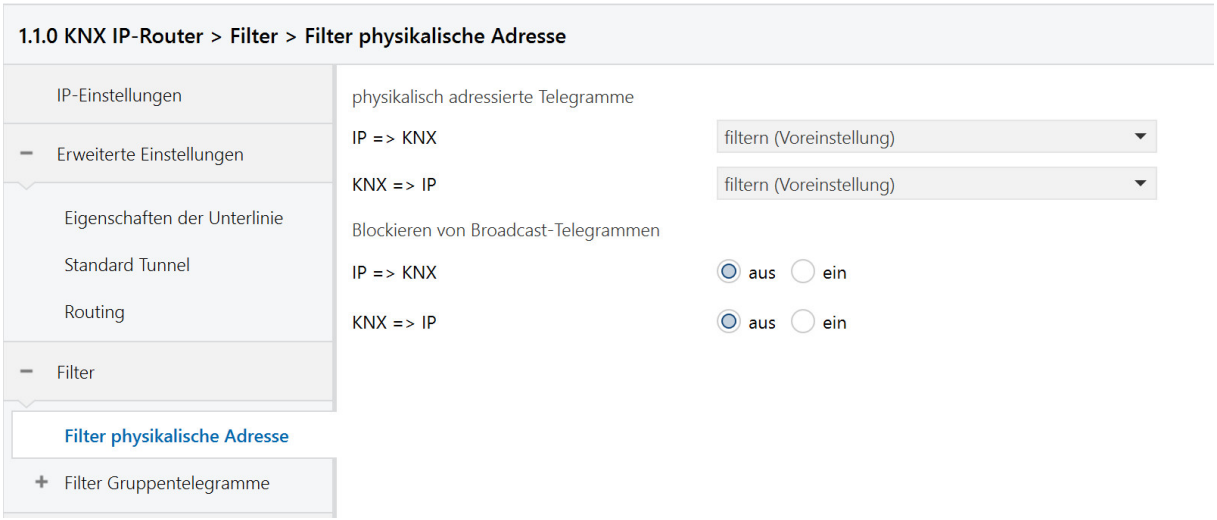

Abb. 24: Filter für physikalisch adressierte Telegramme

Funktion	Auswahl	Beschreibung
Physikalisch adressierte Telegramme	filtern, blockieren, weiterleiten	Die physikalisch adressierten Telegramme (z. B. Programmierung von Aktoren) können über das Routing weitergeleitet, blockiert oder gefiltert werden. Dies betrifft damit sämtliche Kommunikation, die sich auf die Geräteadresse bezieht.
Blockieren von Broadcast-Telegrammen	aus/ein	Broadcast-Telegramme (z. B. Suchen nach Aktoren im Programmierzustand) können über den Router weitergeleitet oder blockiert werden.

Filter Gruppentelegramme

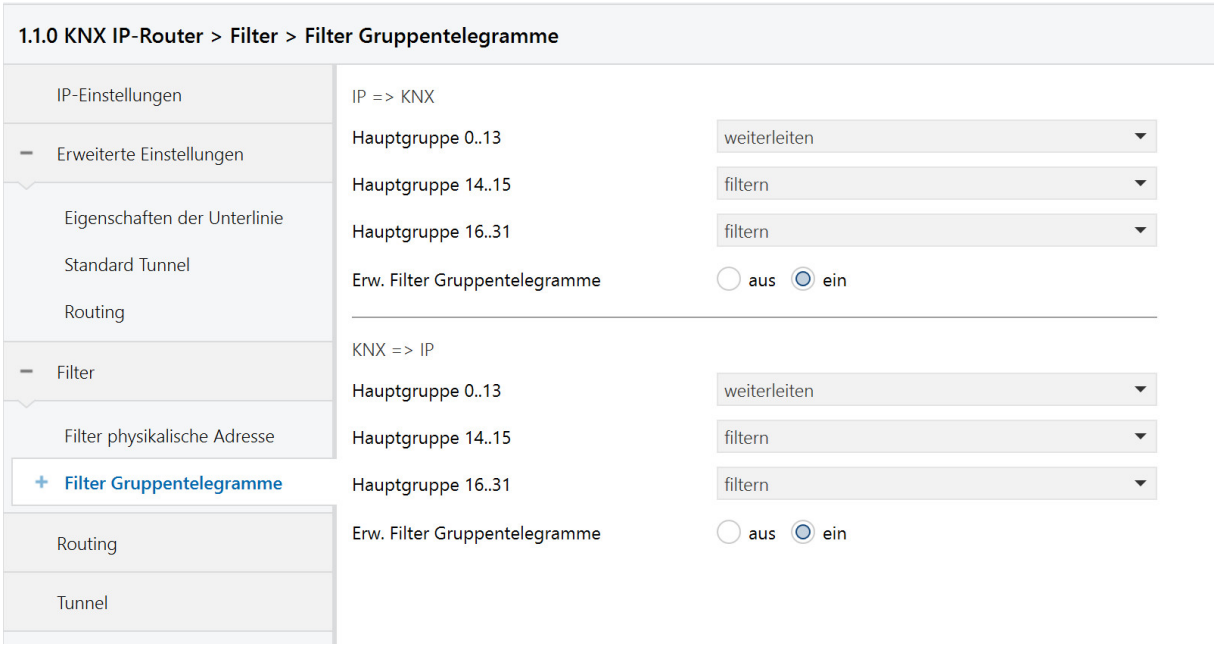

Abb. 25: Filter für Gruppentelegramme

Funktion	Auswahl	Beschreibung
IP => KNX		Richtung: Telegramme von der IP-Seite auf die KNX-Seite
Hauptgruppe 0 bis 13	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 0 bis 13 werden hier zu einem Block zusammengefasst.
Hauptgruppe 14 bis 15	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 14 und 15 werden hier zu einem Block zusammengefasst.
Hauptgruppe 16 bis 31	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 16 und 31 werden hier zu einem Block zusammengefasst.
Erweiterter Gruppenadressfilter	aus/ein	Neben der blockorientierten Filterung von Gruppenadresstelegrammen kann jede Gruppe auch einzeln für sich über das Routing weitergeleitet, blockiert oder gefiltert werden. Mit dieser Funktion kann die Parameterbeschreibung hierzu geöffnet werden.
KNX => IP		Richtung: Telegramme von der KNX-Seite auf die IP-Seite
Hauptgruppe 0 bis 13	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 0 bis 13 werden hier zu einem Block zusammengefasst.
Hauptgruppe 14 bis 15	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 14 und 15 werden hier zu einem Block zusammengefasst.

Funktion	Auswahl	Beschreibung
Hauptgruppe 16 bis 31	filtern, blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 16 und 31 werden hier zu einem Block zusammengefasst.
Erweiterter Gruppenadressfilter	aus/ein	Neben der blockorientierten Filterung von Gruppenadresstelegrammen kann jede Gruppe auch einzeln für sich über das Routing weitergeleitet, blockiert oder gefiltert werden. Mit dieser Funktion kann die Parameterbeschreibung hierzu geöffnet werden.

Erweiterter Filter Gruppentelegramme

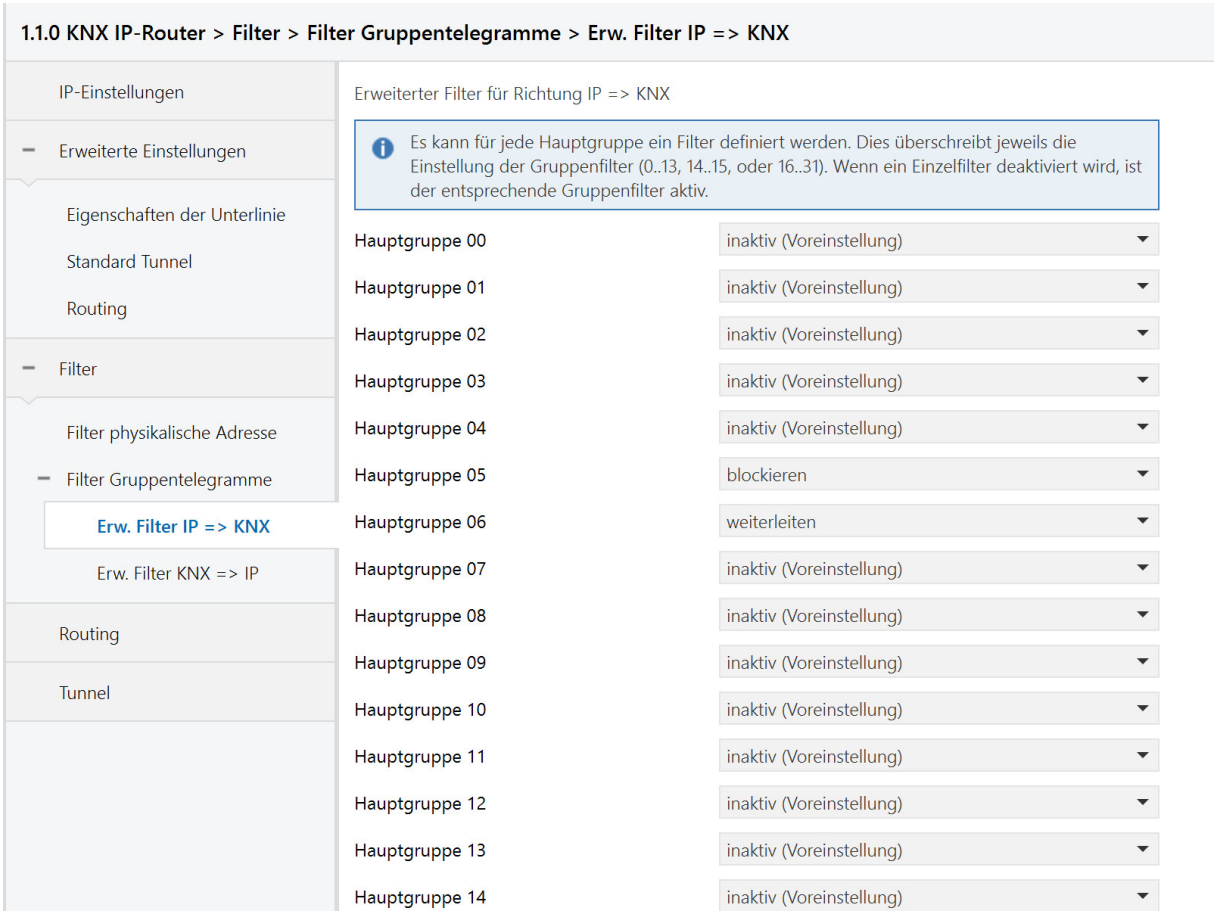

Abb. 26: Erweiterter Filter für Gruppentelegramme

Funktion	Auswahl	Beschreibung
Hauptgruppe 00	inaktiv, filtern, blockieren, weiterleiten	Gruppentelegramme dieser Hauptgruppe können über das Routing weitergeleitet, blockiert oder gefiltert werden. Wenn der Filter nicht aktiv ist, so gilt das Verhalten der Parameter von Abbildung 16 bzw. Abbildung 17.
Hauptgruppe NN **NN = 1 ... 31**	s. o.	s. o.

6.4 Kommunikationsobjekte

ⓘ Abhängig von der Parametrierung können einige Objekte nicht verfügbar sein.

ID	Name	Objektfunktion	Länge	Typ	Flags
1	Externer Zeitserver gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
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 dem externen NTP-Server bzw. falls dies mit KO7 initiiert wird. Wenn der Zeitserver bei der zuletzt ausgeführten Synchronisation nicht erreichbar war, wird der Zustand über dieses KO auf den Bus ausgegeben.					

2	Interne Uhr gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Gibt an, ob die interne Uhr gültig ist. Wert wahr [1] steht für gültig, Wert falsch [0] für ungültig. Über die Parametrierung kann das 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 sich über einen NTP-Server auf dessen Uhrzeit eichen 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 stark entladen wurde, wird die Uhr wieder ungültig (Wert = falsch [0]).					

3	Uhrzeit - Ausgang	**Zeitausgabe**	3 Byte	[10.001] DPT_TimeOf Day	KL-Ü--
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.					

4	Datum - Ausgang	**Datumsausgabe**	3 Byte	[11.001] DPT_Date	KL-Ü--
Kommunikationsobjekt zur Ausgabe des Kalenders der internen Uhr.					

5	Uhrzeit und Datum - Ausgang	**Zeit- und Datumsausgabe**	8 Byte	[19.001] DPT_DateTime	KL-Ü--
Uhrzeit und Datum zur Ausgabe der aktuellen Uhrzeit und Datums auf den Bus.					

6	Datum/Uhrzeit - Eingang	**Anfordern**	1 Bit	[1.017] DPT_Trigger	K-SÜ--
Trigger zum Schreiben von KO3, KO4 und KO5. Es triggert sowohl ein Schreiben mit 0 als auch 1.					

7	NTP Server Synch. - Eingang	**Anfordern**	1 Bit	[1.017] DPT_Trigger	K-SÜ--
Die interne Uhr synchronisiert sich automatisch alle 2 Tage neu mit den externen NTP-Server bzw. falls dieses KO geschrieben wird. Es triggert sowohl ein Schreiben mit 0 als auch 1.					

ID	Name	Objektfunktion	Länge	Typ	Flags
8	Sommer- / Winterzeit - Ausgang	**Status**	1 Bit	[1.xxx]	KL-Ü--
Wenn Sommerzeit aktiv ist, wird dieses KO 0, während der Winterzeit 1. Dieses KO ist daher für die Winterumschaltung von Heizungen direkt nutzbar.					

9	Fernwartung aktivieren - Eingang	**Schalten**	1 Bit	[1.002] DPT_Switch	KLSÜ--
Einschalten der Fernwartung (1) bzw. stoppen der Fernwartung (0): Wenn der Anwender über dieses KO den Fernwartungszugang öffnet, wird sicheres Tunnelling während dieser Zeit aktiviert. Die Schnittstelle verbindet sich dann zum Relaisserver. Eine Entschlüsselung in der Cloud erfolgt nicht. Der kundenseitige Anschluss kann dabei vom Typ IPv4 oder IPv6 sein.					

10	Freischaltcode gültig - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Zeigt wahr [1], wenn das Gerät mindestens einmal mit einem gültigen Freischaltcode geladen wurde und die Fernwartung grundsätzlich möglich ist. Ansonsten ist der Wert falsch [0].					

11	Abgesicherter Modus aktiv - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Zeigt wahr [1], wenn die IPS 300 SREG sicher in Betrieb genommen und das sichere (=verschlüsselte) Tunnelling in der Schnittstellenapplikation aktiviert wurde. Ansonsten ist der Wert falsch [0].					

12	Serververbindung - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	KL-Ü--
Wenn die Verbindung zum Relaisserver steht, so wird dieses KO wahr [1], sonst falsch [0].					

13	Secure Tunnelling aktiv - Ausgang	**Status**	1 Byte	[5.1] DPT_Scaling	KL-Ü--
Status des Secure Tunnellings: falsch [0] = inaktiv, wahr [1] = aktiv. Inaktiv bedeutet, dass unverschlüsselte Tunnelverbindungen aufgebaut werden können.					

14	Programmierung der Fernwartung aktiv - Ausgang	**Status**	1 Bit	[1.2] DPT_Bool	K--Ü--
Wenn eine Fernwartung vom Rechner des Installateurs (ETS) zum IPS 300 SREG aufgebaut wird, ist dies wahr [1], sonst falsch [0]. Da generell eine Verbindung zum Gerät erst nach ca. 10 Sekunden komplett geschlossen wird, wird in der Regel ein zeitlicher Versatz zwischen der Ausgabe des KOs und beispielsweise der Anzeige im Gruppenmonitor beobachtbar.					

ID	Name	Objektfunktion	Länge	Typ	Flags
15	MapperObjekt Kanal A - Feldlänge	**Ein/Ausgang**	1 Bit bis 14 Byte	n.a.	KLSÜ--
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.					

16	MapperObjekt Kanal B - Feldlänge	**Ein/Ausgang**	1 Bit bis 14 Byte	n.a.	KLSÜ--
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 B ausgegeben.					

7 Erweiterte Konfiguration

7.1 Konfigurationstool

Die Software vereinfacht die Konfiguration des Geräts und stellt detaillierte Informationen zur Fehleranalyse zur Verfügung.
Wenn das Gerät im Secure-Modus betrieben wird, kann das Konfigurationstool keine Verbindung zum Gerät herstellen.

7.1.1 KNX IP-Router und KNX IP-Schnittstelle

Geräteverbindung

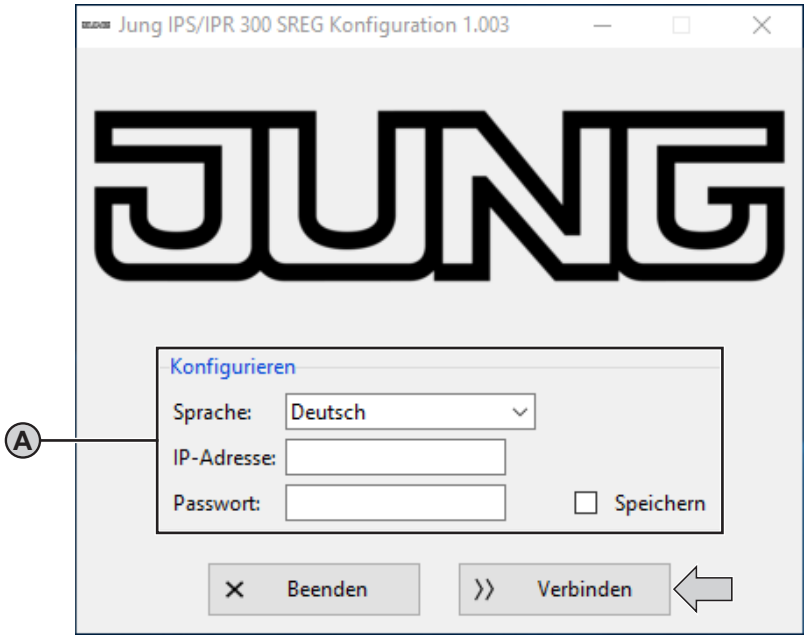

Abb. 27: Geräteverbindung

Voraussetzungen:

- Gerät angeschlossen und gebootet
- Konfigurationstool gestartet

Konfigurieren (A)

Sprache ändern:

- Sprache auswählen.
  Konfigurationstool wird in der ausgewählten Sprache angezeigt.

Gerät verbinden zur Gerätekonfiguration:

- IP-Adresse des Geräts eingeben.
  Die IP-Adresse wird auf dem Display des Geräts angezeigt oder kann wie folgt ermittelt werden:
  Feste IP-Adresse: siehe ETS
  Dynamische IP-Adresse: siehe DHCP-Server
- Passwort eingeben.
  Das voreingestellte Passwort ist „knxsecure“.
  Das eingegebene Passwort kann gespeichert werden, damit es nach dem nächsten Start des Konfigurationstools nicht erneut eingegeben werden muss.
- „Verbinden“ auswählen.
  Gerät wird verbunden.
  Gerätekonfiguration wird angezeigt.

Gerätekonfiguration

Der KNX IP-Router bietet mehr Konfigurationsmöglichkeiten als die KNX IP-Schnittstelle.
Die folgende Abbildung zeigt daher exemplarisch nur die Konfiguration des KNX IP-Routers.

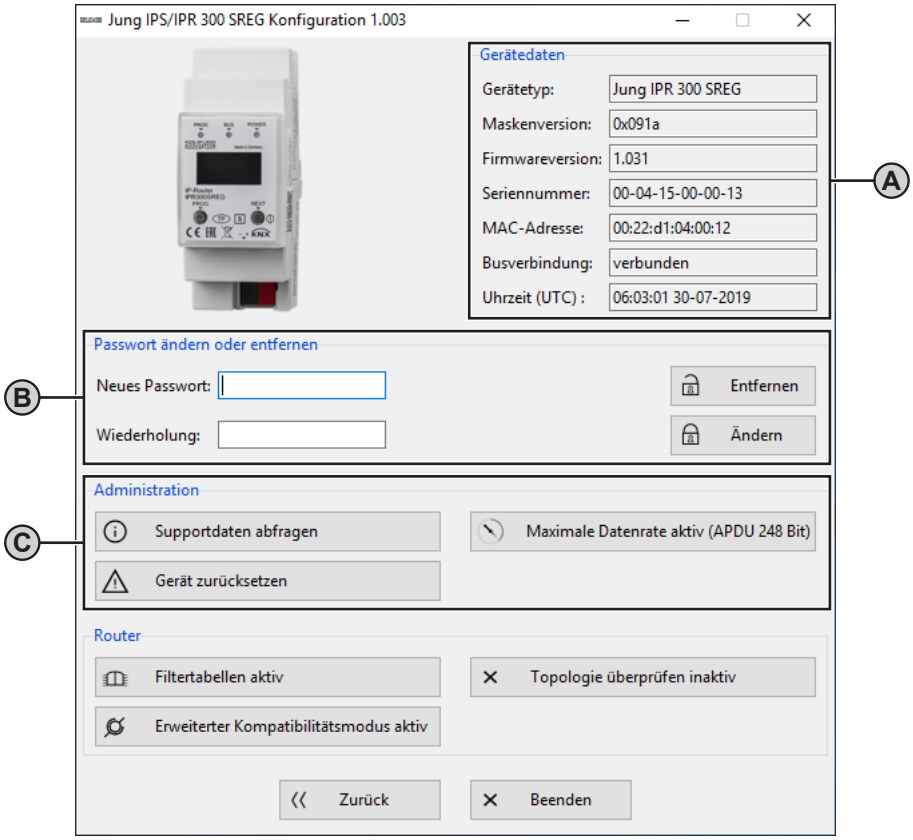

Abb. 28: Gerätekonfiguration – KNX IP-Router und KNX IP-Schnittstelle

Voraussetzung:

- Geräteverbindung hergestellt

Gerätedaten (A)

Zeigt aktuelle Eigenschaften des Geräts an.

Passwort ändern oder entfernen (B)

Passwort ändern:

- Neues Passwort eingeben und Eingabe wiederholen.
- Neues Passwort mit „Ändern“ bestätigen.
  Passwort ist geändert.

Passwort entfernen:

- „Entfernen“ auswählen.
  Passwort wird entfernt.

Administration (C)

Geräteinformationen abspeichern zur Fehlerbehebung:

- „Supportdaten abfragen“ auswählen.
  Eine Textdatei mit Geräteinformationen wird im Hauptverzeichnis der Software abgespeichert.
  Beispielpfad: C:\Programme\KonfigTool\

Master-Reset durchführen zur Wiederherstellung von Werkseinstellungen:

- „Gerät zurücksetzen“ auswählen.
  Master-Reset wird durchgeführt.
  Konfigurationstool wird neugestartet.

Min. / max. Länge der Telegramme auswählen zur Fehlerbehebung durch Drittanbieterprodukte:

- „Maximale Datenrate aktiv (APDU 248 Bit)“ bzw. „Minimale Datenrate aktiv (APDU 55 Bit)“ auswählen.
  Telegrammlänge wird angepasst.

7.1.2 KNX IP-Router

Gerätekonfiguration

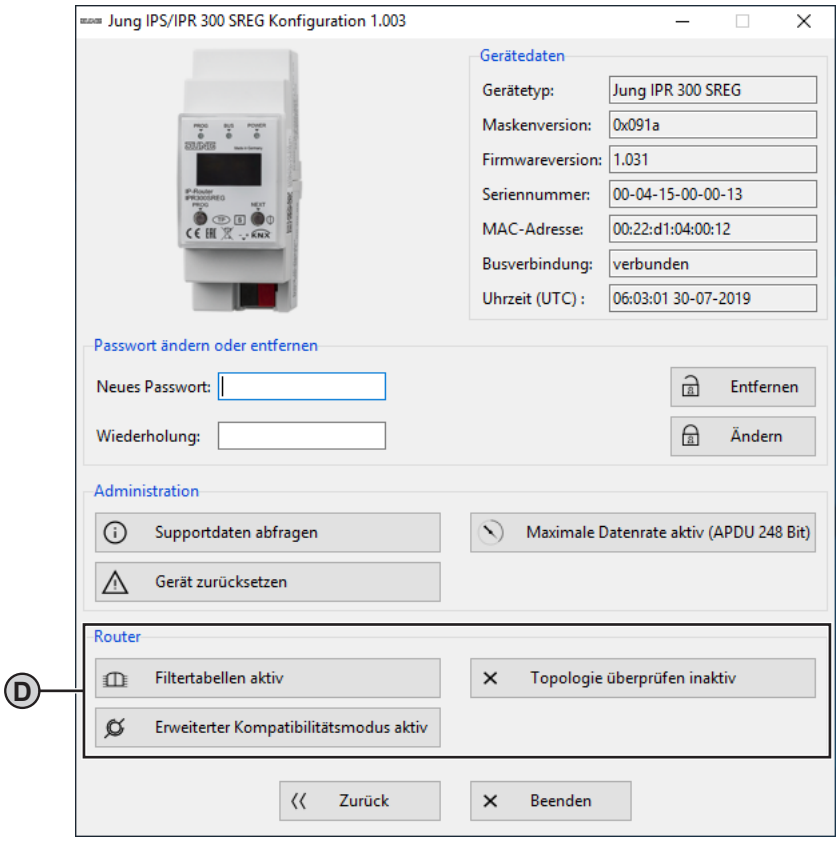

Abb. 29: Gerätekonfiguration – KNX IP-Router

Router (D)

ⓘ Dieser Bereich wird nur angezeigt, wenn das Konfigurationstool mit einem KNX IP-Router verbunden ist.

Filtertabellen kurzzeitig deaktivieren zur Fehlerbehebung:

- „Filtertabellen aktiv“ auswählen.
  Filtertabellen werden deaktiviert.
- Fehlerursache beheben.
- „Filtertabellen inaktiv“ auswählen.
  Filtertabellen werden wieder aktiviert.

Physikalische Adressen aller Geräte in der Linie überprüfen:

- „Topologie überprüfen inaktiv“ auswählen.
  Alle Geräte in der Linie werden überprüft.
  Fehlerhafte physikalische Adresse wird im Telnet-Interface und auf dem Display des Geräts angezeigt sowie in der Textdatei mit Geräteinformationen abgespeichert.
  Telegramm wird unabhängig von Filtertabellen nicht weitergeleitet.

Kompatibilität zu Drittanbieterprodukten verbessern:

- „Erweiterter Kompatibilitätsmodus aktiv“ auswählen.
  Kompatibilität zu Drittanbieterprodukten wird verbessert.

7.2 Anwendungsfälle

7.2.1 KNX IP-Router und KNX IP-Schnittstelle

Mapper

Der praktische Nutzen des Mappers wird im folgenden Szenario erläutert:

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 kann nun festgelegt werden, dass die Hauptgruppe 17 geroutet wird, aber die Hauptgruppe 2 blockiert wird. Damit kann nun die Sicherheit auf der Außenlinie problemlos mit der Innenlinie kombiniert werden.

7.2.2 KNX IP-Schnittstelle

Fernwartung

Über die einstellbaren Parameter „Secure Tunnelling nach Geräteneustart“ bzw. „Secure Tunnelling nach Fernwartung“ kann ein verschlüsselter oder ein herkömmlicher Zugriff über die Tunnelverbindungen gewährleistet werden. Die zugreifende Visualisierung muss alle Eigenschaften der verschlüsselten Tunnelverbindung unterstützen und bewusst aktiviert werden.

Für den herkömmlichen Zugriff (z. B. Smart Visu Server) sind beide Parameter auf „Aus“ einzustellen.

Für den verschlüsselten Zugriff (z. B. JUNG Visu Pro) sind beide Parameter auf „An“ einzustellen.

7.3 Telnet-Interface

Telnet ist ein weit verbreitetes Netzwerkprotokoll auf Basis einer TCP-Verbindung zwischen einem Telnet-Server und einem Client.

Voraussetzung für die Kommunikation ist, dass das Gerät im Netzwerk administriert ist und vom Inbetriebnahme-PC über IP erreicht wird. Über Telnet können dann Einstellungen vorgenommen, sowie Statusinformationen eingesehen werden, ohne dass eine Verbindung zur ETS besteht.

Telnet kann entweder als Funktion des Betriebssystems Windows aktiviert werden oder über ein Drittprogramm, wie z. B. PuTTY, genutzt werden.

Der Telnet-Zugang ist ab Werk mit dem Passwort „knxsecure“ geschützt.

Sobald das Gerät im Secure-Modus betrieben wird, ist das Telnet-Interface deaktiviert.

7.3.1 KNX IP-Router und KNX IP-Schnittstelle

Telnet-Eingabe	Beschreibung
`help`	Zeigt alle verfügbaren Kommandos an

`ifconfig`	Zeigt Netzwerkparameter an
	
	`IP mode.....: DHCP`
	`IP.....: 192.168.33.142`
	`Subnet mask...: 255.255.0.0`
	`Gateway.....: 192.168.33.1`
	`NTP server....: 192.53.103.108`
	`Sys multicast.: 224.0.23.12`
	`RT multicast..: 224.0.23.12`
	`Hardware addr.: 00:50:c2:79:3f:ff`
	Sys multicast: Multicastadresse für Systemtelegramme
	RT multicast: Multicastadresse für Routing-Telegramme

Telnet-Eingabe	Beschreibung
ifconfig [help|dhcp|ip |mask]	Netzwerkparameter über das Telnet-Interface einstellen. Beispiele: Die IP-Adresse per DHCP vergeben: **ifconfig dhcp** Die IP-Adresse statisch auf 192.168.1.2 setzen (in diesem Fall sollte auch Gate-way und Maske angepasst werden, s. u.) **ifconfig ip 192.168.1.2** Das Gateway auf 192.168.1.1 setzen: **ifconfig gw 192.168.1.1** Die Maske auf 255.255.255.0 setzen: **ifconfig mask 255.255.255.0**
tpconfig	Zeigt KNX-Parameter an **KNX bus state.: up** **KNX address...: 15.15.000** **Serial number.: 00-a6-00-00-00-01**
tpconfig [help|set]	KNX-Parameter über das Telnet-Interface einstellen. Die TP-Adresse auf 1.1.0 setzen: **tpconfig set 1.1.0**
progmode [0|1]	Programmiermodus abfragen oder ändern (0 = aus, 1 = ein)
apdu [55..248]	Die maximale Länge der KNX-TP-Telegramme lesen oder konfigurieren. Dies kann notwendig werden, wenn eine fehlerhafte Implementierung eines TP-Stacks vorliegt, sodass die ETS eine Programmierung mit Telegrammen mit 248 Nutzbytes vornimmt, die das TP-Gerät aber nicht verarbeiten kann (z. B. Zennio Z35i). Default ist 248 und sollte nur bei Bedarf verändert werden. **# apdu** **maximal len of a KNX telegram 248.** **Usage: apdu [55 .. 248]**
tpratemax [5..50]	Maximale Telegrammrate (IP => TP) lesen oder konfigurieren; 50 T/s entsprechen 100 % Buslast. **# tpratemax** **no limit, sending with maximum performance to TP.** **Usage: tpratemax [5 .. 50]**
stats	Zeigt diverse Statistiken zu Geräte- und Busstatus **uptime: 114 days, 2:19** **KNX communication statistics:** **TX to IP (all)..: 333729 (ca. 233 t/m)** **TX to KNX.....: 23244 (ca. 16 t/m)** **RX from KNX.....: 94559 (ca. 66 t/m)** **Overflow to IP..: 0** **Overflow to KNX.: 0** **TX tunnel re-req: 260** **TP bus voltage..: 28.95 V** **TX TP rate.....: 50 T/s (= 100 %)** Uptime: Laufzeit der Schnittstelle seit letztem Neustart TX to IP (all): Anzahl aller auf IP verschickten Telegramme TX to KNX: Anzahl der auf den KNX-Bus geschickten Telegramme RX from KNX: Anzahl der vom KNX-Bus empfangenen Telegramme Overflow to IP: Anzahl der Telegramme, die nicht auf IP geschickt werden konnten Overflow to KNX: Anzahl der Telegramme, die nicht auf den KNX-Bus geschickt werden konnten TX tunnel re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten TP bus voltage: Aktuelle Busspannung (zum Zeitpunkt des Aufruf von stats) TX TP rate: maximale Telegrammrate (TP)

Telnet-Eingabe	Beschreibung

`free [clear]`	Zeigt Statistiken über die Speicherauslastung
	
	`Used stack memory...: 14 %`
	`Allocated memory....: 64 %`
	`Unused memory.......: 35 %`
	`TP-Tx buffer........: 0 %`
	`TP-Tx buffer max....: 0 %`
	`TP-Rx buffer max....: 0 %`
	`Tunnel-T8 buffer max: 92 %`
	
	Used stack memory: Funktionsstapelauslastung
	Allocated memory: Allokierter Gerätespeicher
	Unused memory: Nicht genutzter Gerätespeicher
	TP-Tx buffer: Derzeit genutzter TP-Sendepuffer
	TP-Tx buffer max: Max. Auslastung TP-Sendepuffer (IP => TP) seit Systemstart
	TP-Rx buffer max: Max. Auslastung TP-Empfangspuffer (IP <= TP) seit Systemstart
	Tunnel-XX (XX = 1..8) buffer max: Max. Auslastung des Tunneling Buffers. Es werden nur Tunnel angezeigt, deren Puffer überhaupt benutzt wurde.
	
	Löschen der Pufferstatistik:
	`free clear`

Telnet-Eingabe	Beschreibung
tunnel [1..8]	Zeigt aktive Tunnelverbindungen (ohne Argument), bzw. detaillierte Informationen zur angegebenen Tunnelverbindung an (mit Argument 1..8) **# tunnel** **Tunnels open: 1/8** **1: 00.02.246, closed** **2: 00.02.247, open (CCID: 82)** **3: 00.02.248, closed** **4: 00.02.249, closed** **5: 00.02.250, closed** **6: 00.02.251, closed** **7: 00.02.252, closed** **8: 00.02.253, closed** **# tunnel 2** **Tunnel 2.....: open (CCID 82)** **KNX address.....: 00.02.247** **HPAI control.....: 192.168.22.252:4808** **HPAI data.....: 192.168.22.252:4808** **Connect. type.....: TUNNEL_CONNECTION** **Communication.....: UDP CONNECTION** **TX tun req.....: 23169** **TX tun re-req.....: 0** **RX tun req.....: 821** **RX tun re-req (identified): 0** **RX tun req (wrong seq.)...: 0** **Current tunnel buffer.....: 0 %** **Connected since (UTC).....: 16:26:16 29-01-2019** CCID: Verbindungs-ID der Tunnelverbindung KNX address: Tunneladresse HPAI control: Kontrollendpunkt des Verbindungspartners HPAI data: Datenendpunkt des Verbindungspartners Connect. Type: Verbindungstyp Tunnel oder Management-Verbindung Communication: UDP- oder TCP-Verbindung TX tun req: Anzahl der Telegramme, die in die Tunnelverbindungen geschickt wurden TX tun re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten RX tun req: Anzahl der Telegramme, die von der Tunnelverbindungen empfangen wurden RX tun re-req: Anzahl der Telegramme, die von der Tunnelverbindungen doppelt empfangen wurden RX tun req (wrong seq.): Anzahl der Telegramme, die von der Tunnelverbindun-gen mit falscher Sequenznummer empfangen wurden Current tunnel buffer: Auslastung aktuell des IP-Puffers des Tunnels Connected since (UTC): Uhrzeit, seitdem die Tunnelverbindung besteht
version	Firmware-Version abfragen
mask	Masken-Version abfragen
display [0|1]	Displaymodus abfragen oder ändern (0 = Standard, 1 = invertiert)
tunaddr 1..8 address **tunaddr reset** **tunaddr setall** **tunaddr help**	KNX-Adresse eines Tunnels lesen (**tunaddr**) oder ändern, z. B. **tunaddr 1 15.15.240**, alle Tunneladressen fortlaufend ab einer bestimmten Startadresse vergeben (**tunaddr setall 15.15.15**), oder die KNX-Adressen aller Tunnel auf Werkseinstellung zurücksetzen (**tunaddr reset**) **# tunaddr** **1: KNX address: 15.15.010** **2: KNX address: 15.15.011** **3: KNX address: 15.15.012** **4: KNX address: 15.15.013** **5: KNX address: 15.15.014** **6: KNX address: 15.15.015** **7: KNX address: 15.15.016** **8: KNX address: 15.15.017**

Telnet-Eingabe	Beschreibung
tunmode [std/tpblk]	Tunnelmodus lesen (ohne Parameter) oder setzen (**tp** bzw. **tpblk**); **tunmode tpblock**: IP => KNX bei gleicher Backbone Line Frame an TP weiterleiten KNX => IP bei gleicher Sub Line Frame an TP weiterleiten
lock [0|1]	Lock-Status abfragen (ohne weiteren Parameter) oder ändern (0 = aus, 1 = ein). Einstellung ist identisch zu Programmiersperre TP-Seite, Abbildung 13. Ein Router kann durch das Filtern das Weiterleiten von physikalisch adressierten Telegrammen unterbinden, d. h. das Umprogrammieren von Geräten über eine Linie hinweg ist nicht möglich. Dies wird bei Verwendung von Linien im Außenbereich interessant. Allerdings kann z. B. eine KNX-USB-Schnittstelle auf eine Außenlinie direkt an den Bus angeschlossen werden und der Router in der Außenlinie selbst umprogrammiert werden, sodass er die physikalisch adressierten Telegramme weiterleitet. Mit dieser Telnet-Funktion kann dies unterbunden werden. Setzt man per Telnet „lock“ auf 1, so kann der Router nicht mehr über die KNX-Linie programmiert werden und entsprechende Aktivierung des Weiterleitens über KNX TP ist nicht mehr möglich.
topology [0|1]	„Überprüfung der Topologie“ abfragen oder ändern (0 = aus, 1 = ein). Einstellung ist identisch zu „Überprüfung der Topologie“, Abbildung 15 **Subline Topology has been violated with 1.2.3** **Last logged at 18:28:31 09-11-2018** **Mainline Topology has been violated with 1.2.3** **Last logged at 18:24:31 09-11-2018**
Tunneltime [1.0..8.0]	Timeout für Tunnelverbindung abfragen oder ändern (1.0 bis 8.0). Einstellung ist identisch zu „Langsame Verbindung“, Abbildung 14
tunudp	Typ der Tunnelverbindung für die ETS abfragen oder ändern (0 = Standard, 1 = Nur UDP).
date	Datum und Uhrzeit anzeigen
sntp [query|server IP]	Anfrage an den NTP-Server schicken (**sntp query**) oder IP des NTP-Servers einstellen (**sntp server 1.2.3.4**)
logmem	Ereignisspeicher im Gerät. Geeignet für die Entwicklung von Clients. Bei Supportanfragen auslesen.
passwd oldpw newpw **passwd oldpw** **passwd newpw**	Ändert das aktuelle Telnet-Passwort (passwd alt neu), löscht das aktuelle Passwort (passwd alt) oder setzt ein neues Passwort, falls momentan keines gesetzt ist (passwd neu).
factory_reset	Auf Werkseinstellungen zurücksetzen und neustarten
reboot	Neustart
logout	Telnet-Session beenden

7.3.2 KNX IP-Router

Telnet-Eingabe	Beschreibung

`lcconfig`	`Coupler type..: line coupler`
	`IP -> KNX:`
	`GA  0-13......: route`
	`GA 14-15......: filter`
	`GA 16-31......: block`
	`Ph. addr......: filter`
	`Broadcast.....: route`
	`KNX -> IP:`
	`GA  0-13......: route`
	`GA 14-16......: filter`
	`GA 16-31......: block`
	`Ind.addr......: filter`
	`Broadcast.....: route`
	`Check IA rout.: disabled`
	`Ind.Addr.tlg..: individually addressed telegrams are 3 times repeated`

`systembc [0|1]`	Bestimmte Bits im System Broadcast setzen, sodass IP-Routing auch über ältere Geräte möglich ist. Standardmäßig ist dieser Kompatibilitätsmodus eingeschaltet. `Wrong handling of bits in system broadcasts is 1 (on)`
`sendack [0|1]`	„Jedes Telegramm bestätigen (ACK)“ abfragen oder ändern. Einstellung ist identisch zur Dokumentation zu Abbildung 13.
`blockfilter [0|1]`	Sämtliche Gruppenadressfilter deaktivieren (d. h. alles weiterleiten), unabhängig von den Einstellungen der ETS. Abfragen oder ändern (0 = aus, 1 = ein).
`routingcounter [0|1]`	Routingcounterhandling abfragen oder ändern (0 = Standard, 1 = Verhalten vor 2018). Diese Einstellung ist identisch zu Aktivierung Routing Algorithmus <2018, Abbildung 15

8 Begriffe

Begriff	Beschreibung
Backbone	Bei IP-Routern und IP-Schnittstellen ist dies immer das IP-Netzwerk.
Backbonekey, Backboneschlüssel	Das Routingprotokoll kommuniziert bei KNX IP Secure verschlüsselt. Der Schlüssel muss bei allen Teilnehmern gleich sein und wird in das Gerät geladen. Die ETS generiert einen möglichst sicheren Schlüssel selbstständig.
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.
Multicast	Eine IP Adresse im Netzwerk, über die alle Router bzw. Schnittstellen eines Backbones kommunizieren. Tunnelverbindungen benötigen diese Adresse nicht. Multicast-Verbindungen erfolgen immer über das UDP Protokoll. Anders als bei der TCP-Kommunikation kann ein Telegramm grundsätzlich verloren gehen. Dies ist z. B. bei WLAN-Verbindungen mit hoher Wahrscheinlichkeit der Fall. Daher sollte das Routing-Backbone immer über eine Ethernet-Kabelverbindung realisiert werden, da diese zu fast 100 % übertragungssicher ist.
Tunneling	Eine KNX-Punkt-zu-Punkt-Verbindung auf dem TCP/IP Netzwerk, die entweder per UDP- oder TCP-Protokoll aufgebaut wird. Tunneling 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. Dieser Timeout kann im erweiterten Setup angepasst werden.
Secure Tunneling	Secure Tunnelling oder Sicheres Tunnelling bedeutet, dass die Tunnelverbindung verschlüsselt übertragen wird.
Telnet	Ein einfacher TCP-Server auf Port 23, der direkte textbasierte Kommunikation mit dem IP-Gerät ermöglicht. Telnet ist ein de facto Standard, der auf der Windowsebene z. B. mit „PuTTY“ angesprochen 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.

9 Technische Daten

Symbole	 Darf nicht über den Hausmüll entsorgt werden.
Nennspannung KNX	DC 21 ... 32 V SELV
Anschluss KNX	Anschlussklemme
Stromaufnahme	max. 20 mA
Leistungsaufnahme	max. 1 W
IP-Kommunikation	Ethernet 10/100 BaseT (10/100 Mbit/s)
Anschluss IP	1 x RJ45
Auflösung	128 x 64, OLED-Display
KNX-Funktionen	KNX IP-Router und KNX IP-Schnittstelle: • KNX IP Secure Tunneling • Bis zu 48 Telegramme pro Sekunde • AES 128-Verschlüsselung • Asymmetrischer Schlüsselaustausch für Tunnelverbindungen • UDP- und TCP-Kommunikation • Bis zu 8 Tunnelverbindungen • Bis zu 62 Gruppenadressfilter • APDU 248, parametrierbar zwischen 55 und 248 • TP-Telegrammratenbegrenzung • TP-Busspannungsmessung (Anzeige Telnet bzw. Display) KNX IP-Router: • KNX IP Secure Routing
Umgebungstemperatur	−5 ... +45 °C
Lager-/ Transporttemperatur	−25 ... +70 °C
Relative Feuchte	max. 95 %
Einbaubreite	36 mm (2 TE)
Abmessungen	35,0 mm x 89,6 mm x 62,9 mm (L x B x H)

10 Gewährleistung

Die Gewährleistung erfolgt im Rahmen der gesetzlichen Bestimmungen über den Fachhandel.

11 Open Source Software

Dieses Produkt verwendet Software aus dritten Quellen folgender Autoren:

Adam Dunkels adam@sics.se
Marc Boucher <marc@mbsi.ca> and David Haas dhaas@alum.rpi.edu
Guy Lancaster <lancasterg@acm.org>, Global Election Systems Inc.
Martin Husemann <martin@NetBSD.org>
Van Jacobson (van@helios.ee.lbl.gov)
Paul Mackerras, paulus@cs.anu.edu.au,
Christiaan Simons christiaan.simons@axon.tv
Jani Monoses jani@iv.ro
Leon Woestenberg <leon.woestenberg@gmx.net>

11.1 LWIP

Quelle: https://savannah.nongnu.org/projects/lwip/