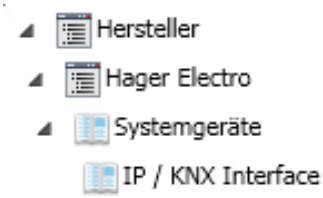


Applikationsbeschreibung

KNX IP Secure Schnittstelle

Elektrische / mechanische Eigenschaften: siehe Produktbeschreibungen

	Bestell nummer	**Produktbezeichnung**	**Ref. Anwendungs software**	**TP-Produkt** **Funk Produkte**
	TYFS120	KNX IP Secure Schnittstelle	STYFS120	▬

6LE008080A

Inhaltsverzeichnis

1. Anwendung

Das KNX IP Interface secure dient als Schnittstelle für PC oder Laptop zum KNX Bus. Von jedem Punkt im LAN kann auf den KNX Bus zugegriffen werden. Das KNX IP Interface secure kann als Programmierschnittstelle für die ETS® verwendet werden. Beim Zugriff über KNXnet/IP Tunneling sind max. 8 Verbindungen gleichzeitig möglich.

Das Gerät unterstützt KNX Security. Die Option kann in der ETS aktiviert werden. Als Secure Interface verhindert das Gerät den unberechtigten Zugriff auf das System.

Die IP-Adresse kann über DHCP oder durch die ETS Konfiguration zugewiesen werden. Das Gerät arbeitet nach der KNXnet/IP-Spezifikation unter Verwendung von Core, Device Management und Tunneling.

Die Spannungsversorgung erfolgt über den KNX Bus.

2. KNX Security

Der KNX Standard wurde um KNX Security erweitert, um KNX Installationen vor unerlaubten Zugriffen zu schützen. KNX Security verhindert zuverlässig sowohl das Mithören der Kommunikation als auch die Manipulation der Anlage.

Die Spezifikation für KNX Security unterscheidet zwischen KNX IP Security und KNX Data Security. KNX IP Security schützt die Kommunikation über IP während auf KNX TP die Kommunikation unverschlüsselt bleibt. Somit kann KNX IP Security auch in bestehenden KNX Anlagen und mit nicht-secure KNX TP Geräten eingesetzt werden.

KNX Data Security beschreibt die Verschlüsselung auf Telegrammebene. Das heißt, dass auch die Telegramme auf dem Twisted Pair Bus verschlüsselt werden.

2.1. KNX IP Security für die Interface Funktion

Bei der Verwendung eines KNX IP Interfaces zum Bus ist ohne Security der Zugriff auf die Installation für alle Geräte möglich, die Zugang zum IP Netzwerk haben. Mit KNX Security ist ein Passwort erforderlich. Bereits für die Übertragung des Passwortes wird eine sichere Verbindung aufgebaut. Die gesamte Kommunikation über IP ist verschlüsselt und abgesichert..

In beiden Modi leitet das Interface sowohl verschlüsselte als auch unverschlüsselte KNX Telegramme weiter. Die Security-Eigenschaften werden vom jeweiligen Empfänger bzw. Tool geprüft.

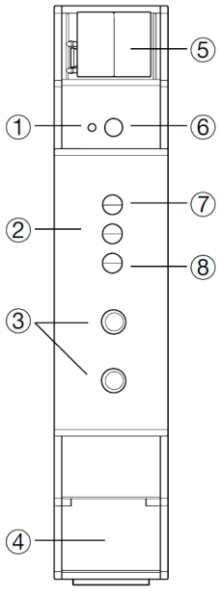
2.2. KNX Data Security für das Gerät

Das KNX IP Interface secure unterstützt auch KNX Data Security, um das Gerät vor unerlaubten Zugriffen aus dem KNX Bus zu schützen. Wird das KNX IP Interface über den KNX Bus programmiert, erfolgt dies mit verschlüsselten Telegrammen.

Verschlüsselte Telegramme sind länger als die bisher verwendeten unverschlüsselten. Deshalb ist es für die sichere Programmierung über den Bus erforderlich, dass das verwendete Interface (z.B. USB) und ggf. dazwischenliegende Linienkoppler die sogenannten KNX Long-Frames unterstützten..

3. Installation und Inbetriebnahme

Das KNX IP Interface secure wird auf einer Hutschiene montiert und hat einen Platzbedarf von 1 TE (18 mm). Es besitzt folgende Bedienelemente und Anzeigen::



① LED für die physikalische Adressierung
② Betriebsmodus-LED
③ Taste für Verbindungsauswahl (Tunnel)
④ RJ45 Netzwerk-Verbindung
⑤ KNX-Bus-Verbindung
⑥ Taste für die physikalische Adressierung
⑦ LED für KNX-Bus-Status
⑧ LED für Ethernet/IP-Status

Das KNX IP Interface secure wird aus dem KNX Bus versorgt. Der Anschluss einer externen Versorgungsspannung ist nicht erforderlich.

Bei fehlender Busspannung ist das Gerät ohne Funktion.

3.1. Programmiermodus

Der KNX Programmiermodus wird über den versenkten KNX-Programmiertaster ⑥ oder über gleichzeitigen Druck der Tasten ③ ein- bzw. ausgeschaltet.

3.2. Statusanzeige

Die KNX LED ⑦ leuchtet grün bei vorhandener KNX Busspannung. Bei Flackern dieser LED findet Telegrammverkehr auf dem KNX Bus statt.

Fehler in der Kommunikation (z.B. Telegrammwiederholungen oder Telegrammfragmente) werden durch einen kurzzeitigen Farbwechsel zu Rot angezeigt..

LED Verhalten ⑦	Bedeutung
LED leuchtet grün	KNX Busspannung vorhanden.
LED flackert grün	Telegrammverkehr auf dem KNX Bus.
LED kurzzeitig rot	Fehler in der Kommunikation auf dem KNX Bus.

Table 1 - Zusammenfassung der Zustände der KNX LED

Die IP LED ⑧ leuchtet bei einem aktiven Ethernet-Link. Diese LED ist grün, wenn das Gerät gültige IP Einstellungen (IP Adresse, Subnetz und Gateway) hat. Bei ungültigen bzw. nicht vorhandenen IP Einstellungen ist diese LED rot. Dies ist z.B. auch der Fall, wenn das Gerät die IP Einstellungen vom DHCP Server noch nicht erhalten hat. Bei Flackern dieser LED findet IP Telegrammverkehr statt.

LED Verhalten ⑧	Bedeutung
LED leuchtet grün	Das Gerät hat einen aktiven Ethernet-Link und gültige IP Einstellungen.
LED leuchtet rot	Das Gerät hat einen aktiven Ethernet-Link und ungültige IP Einstellungen oder noch keine IP Einstellungen vom DHCP Server erhalten..
LED flackert grün	IP-Telegrammverkehr

Table 2 - Zusammenfassung der Zustände der IP LED

Mit der Mode LED ② kann der Status jeder KNXnet/IP Tunneling Verbindung angezeigt werden.

Dazu kann mit den Tastern Conn Up/Dn ③ die jeweilige Verbindung ausgewählt werden. Conn Up ③ zählt die Verbindungsnummer hoch, Conn Dn ③ herunter. Die aktuelle Verbindungsnummer wird durch 1 bis 5-faches Blitzen der Mode LED ②angezeigt. Eine verfügbare KNXnet/IP Tunneling Verbindung wird grün angezeigt, eine belegte KNXnet/IP Tunneling Verbindung orange.

Über die Escape-Funktion (Esc) kann durch gleichzeitiges Betätigen der Taster Conn Up/Dn ③ diese Anzeige beendet werden.

Sind weder Programmiermodus noch Handbedienung aktiv, kann die Mode LED ② Konfigurationsfehler anzeigen.

LED Verhalten ②	Bedeutung
LED leuchtet grün	Das Gerät arbeitet im normalen Betriebsmodus.
LED leuchtet rot	Der Programmiermodus ist aktiv.
LED blitzt 1x..8x grün	Der Programmiermodus ist nicht aktiv. Handbedienung (Statusanzeige) aktiv: Der angewählte Tunnel (1..8) ist frei.
LED blitzt 1x…8x orange	Der Programmiermodus ist nicht aktiv. Handbedienung (Statusanzeige) aktiv: Der angewählte Tunnel (1..8) ist belegt.
LED blinkt rot	Der Programmiermodus ist nicht aktiv. Der Handbedienung ist nicht aktiv. Das Gerät ist nicht korrekt geladen. z.B. nach Abbruch eines Downloads.

Table 3 - Zusammenfassung der Zustände der Mode LED

4. Werkseinstellungen

Ab Werk ist folgende Konfiguration voreingestellt:

Physikalische Adresse des Gerätes:	**15.15.255**
Konfigurierte KNXnet/IP Tunneling Verbindung:	**1**
Physikalische Adr. der Tunneling Verbindung:	**15.15.240**
IP Adressen Vergabe:	**DHCP**
Initialer Schlüssel (FDSK) :	**aktiv**
Security Modus :	**nicht aktiv**

Zurücksetzen auf Werkseinstellungen (Master-Reset)

Es besteht die Möglichkeit, das Gerät auf diese Werkseinstellungen zurückzusetzen :

- KNX Bus Anschluss ⑤ vom Gerät trennen
- KNX Programmiertaster ⑥ drücken und gedrückt halten
- KNX Bus Anschluss ⑤ zum Gerät wieder herstellen
- Programmiertaster ⑥ mindesten noch 6 Sekunden gedrückt halten
- Ein kurzes Aufblinken aller LEDs (①②⑦⑧) signalisiert die erfolgreiche Rücksetzung auf Werkseinstellung.

5. ETS Datenbank

Die ETS Datenbank (ab ETS 5.7) kann auf der Produkt Website KNX IP Interface secure oder im KNX Online-Katalog der ETS heruntergeladen werden.

Wenn Sie nicht an der KNX IP Secure Funktion Interesse haben, haben Sie immer noch die Möglichkeit, eine non-Secure Version der Applikation zu verwenden, um Ihr Gerät zu konfigurieren.

Wenn Sie die Secure Version der Applikation verwenden, müssen die folgenden Schritte durchgeführt werden.

Wird das erste Produkt mit KNX Security in ein Projekt eingefügt, fordert die ETS dazu auf, ein Projektpasswort einzugeben.

Figure 1 – Projektpasswort ändern

Dieses Passwort schützt das ETS Projekt vor unberechtigtem Zugriff. Dieses Passwort ist kein Schlüssel, der für die KNX Kommunikation verwendet wird. Die Eingabe des Passwortes kann mit „Abbrechen“ umgangen werden, dies wird aus Sicherheitsgründen aber nicht empfohlen.

Für jedes Gerät mit KNX Security, das in der ETS angelegt wird, benötigt die ETS ein Gerätezertifikat. Dieses Zertifikat beinhaltet die Seriennummer des Gerätes sowie einen initialen Schlüssel (FDSK = Factory Default Setup Key).

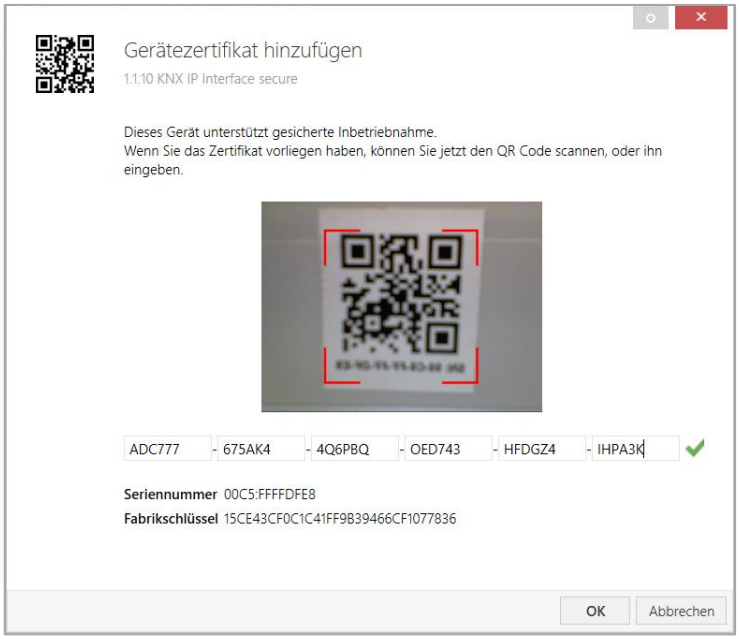


Figure 2 – Gerätezertifikat hinzufügen

Das Zertifikat ist als Text auf dem Gerät aufgedruckt. Es kann auch bequem über eine Webcam vom aufgedruckten QR-Code abgescannt werden.

Die Liste aller Gerätezertifikate kann im ETS-Fenster Übersicht - Projekte – Sicherheit verwaltet werden.

Dieser initiale Schlüssel wird benötigt, um ein Gerät von Anfang an sicher in Betrieb zu nehmen. Selbst wenn der ETS-Download von einem Dritten mitgeschnitten wird, hat dieser anschließend keinen Zugriff auf die gesicherten Geräte. Während dem ersten sicheren Download wird der initiale Schlüssel von der ETS durch einen neuen Schlüssel ersetzt, der für jedes Gerät einzeln erzeugt wird. Somit wird verhindert, dass Personen oder Geräte, die den initialen Schlüssel eventuell kennen, Zugriff auf das Gerät haben. Der initiale Schlüssel wird erst bei einem Master-Reset wieder aktiviert.

Durch die Seriennummer im Zertifikat kann die ETS während eines Downloads den richtigen Schlüssel zu einem Gerät zuordnen.

In der ETS werden einige Einstellungen zusätzlich zum Parameterdialog im Eigenschaftendialog (am Bildschirmrand) angezeigt. So können hier die IP-Einstellungen vorgenommen werden. Die zusätzlichen Adressen für die Schnittstellen-Verbindungen werden in der Topologie-Ansicht angezeigt.

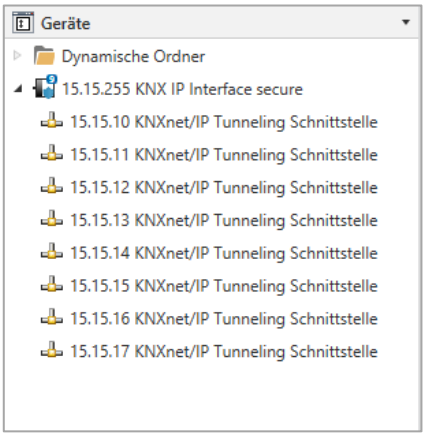


Figure 3 – Geräte

Um die einzelnen Adressen zu ändern, ist der entsprechende Eintrag in der Liste zu markieren und im Textfeld die gewünschte Adresse einzugeben. Sollte der Rahmen des Textfeldes, nach Eingabe, seine Farbe auf Rot wechseln weist dies darauf hin, dass die eingegebene Adresse bereits verwendet wird.

Stellen Sie sicher, dass keine der oben angegebenen Adressen bereits in Ihrer KNX Installation verwendet wird.

Durch Markieren des KNX IP Interface secure in der Baumstruktur der Topologie Ansicht des ETS Projekts, erscheint auf der rechten Seite des ETS Fensters die Übersicht „Eigenschaften“. Unter Eigenschaften Menüpunkt „Einstellungen“ kann der Gerätename des KNX IP Interface secure geändert werden.

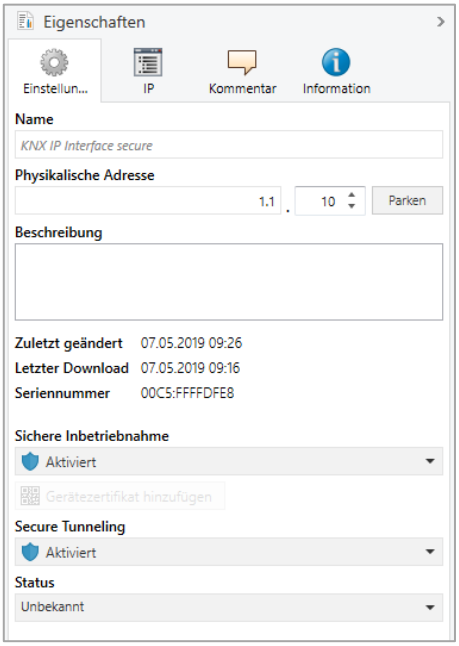


Figure 4 – Eigenschaften

Wenn Secure Tunneling aktiviert ist, wird automatisch ein Passwort für jeden Tunnel vergeben. Dieses Passwort wird unter Menüpunkt „Einstellungen“ angezeigt, wenn ein Tunnel ausgewählt ist.

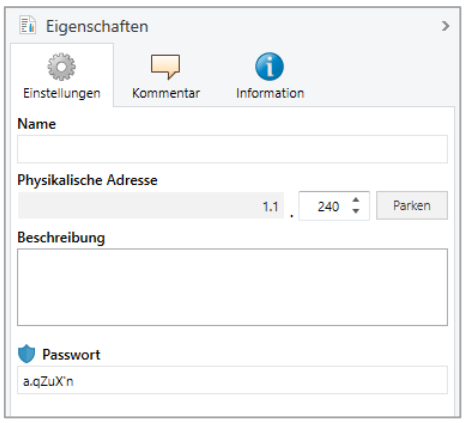


Figure 5 – Eigenschaften

Unter Eigenschaften Menüpunkt „IP“ können die IP spezifischen Optionen des KNX IP Interface secure geändert werden.

Durch Umschalten von „IP-Adresse automatisch beziehen (über DHCP) auf „Folgende IP-Adresse verwenden“ (statische IP Adresse) kann die IP-Adresse, Subnetzmaske und das Standardgateway frei gewählt werden.

Die vorgenommenen Änderungen in den Eigenschaften Menüs werden erst nach einem Applikationsdownload wirksam.

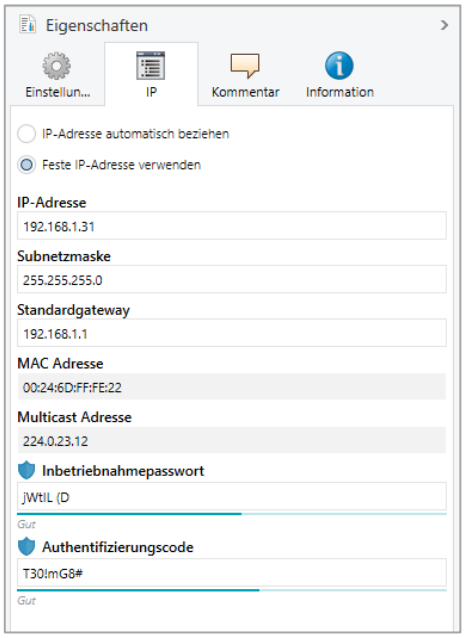


Figure 6 – Eigenschaften

- **IP-Adresse**

Hier ist die IP-Adresse des KNX IP Interface secure einzutragen. Diese dient der Adressierung des Gerätes über das IPNetzwerk (LAN). Die IP-Adressierung sollte mit dem Administrator des Netzwerks abgestimmt werden.

- **Subnetzmaske**

Hier ist die Subnetz-Maske anzugeben. Diese Maske dient dem Gerät festzustellen, ob ein Kommunikationspartner sich im lokalen Netz befindet. Sollte sich ein Partner nicht im lokalen Netz befinden, sendet das Gerät die Telegramme nicht direkt an den Partner, sondern an das Gateway, das die Weiterleitung übernimmt.

- **Standardgateway**

Hier ist die IP-Adresse des Gateways anzugeben, z.B. der DSLRouter der Installation.

- **Beispiel zur Vergabe von IP-Adressen:**

Mit einem PC soll auf das KNX IP Interface secure zugegriffen werden :

IP-Adresse des PCs: 192.168.1.30

Subnetz des PCs: 255.255.255.0

Das KNX IP Interface secure befindet sich im selben lokalen LAN, d.h. er verwendet das gleiche Subnetz. Durch das Subnetz ist die Vergabe der IP-Adresse eingeschränkt, d.h. in diesem Beispiel muss die IP-Adresse des IP Interfaces 192.168.1.xx betragen, xx kann eine Zahl von 1 bis 254 sein (mit Ausnahme von 30, die schon verwendet wurde). Es ist darauf zu achten, keine Adressen doppelt zu vergeben.

IP-Adresse des IP Interface: 192.168.1.31

Subnetz des IP Interface: 255.255.255.0

6. ETS Parameterdialog

Mit der ETS können folgende Parameter gesetzt werden.

6.1. Allgemeine Einstellungen

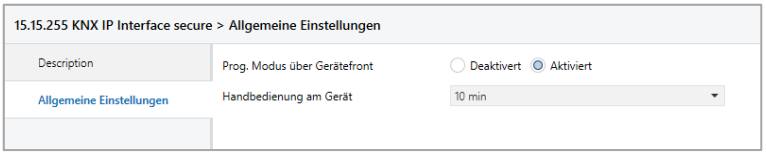


Figure 7 – Allgemeine Einstellungen

6.2. Prog. Modus an Gerätefront

Zusätzlich zur normalen Programmiertaste ⑥ ermöglicht das Gerät die Aktivierung des Programmiermodus an der Gerätefront, ohne die Schalttafelabdeckung zu öffnen. Der Programmiermodus kann durch gleichzeitiges Drücken der Tasten ③ aktiviert und deaktiviert werden.

Diese Funktion kann über den Parameter „Prog. Modus an Gerätefront“ ein- und ausgeschaltet werden. Die vertiefte Programmiertaste ⑥ (neben der Programmier-LED ①) ist immer aktiviert und wird von diesem Parameter nicht beeinflusst.

6.3. Handbedienung am Gerät

Die Handbedienung des KNX IP Interface secure beinhaltet nur die Statusanzeige. Dieser Parameter stellt die Dauer des Handbedienungsmodus ein. Bei Beendigung wird der normale Anzeigemodus wiederhergestellt.

7. Programmierung

Das KNX IP Interface secure kann über verschiedene Wege von der ETS programmiert werden:

7.1. Über den KNX bus

Dazu muss das Gerät nur mit dem Bus verbunden sein. Die ETS benötigt eine zusätzliche Schnittstelle (z.B. USB) zum Bus. Über diesen Weg kann sowohl die physikalische Adresse als auch die gesamte Applikation inklusive IP Konfiguration programmiert werden. Die Programmierung über den Bus wird empfohlen, wenn keine IP Verbindung hergestellt werden kann.

7.2. Über KNXnet/IP Tunnelling

Hierbei ist keine zusätzliche Schnittstelle erforderlich. Die Programmierung über KNXnet/IP Tunnelling ist möglich, wenn das Gerät bereits eine gültige IP Konfiguration besitzt (z.B. über DHCP). In diesem Fall wird das Gerät bei den Schnittstellen in der ETS angezeigt und muss ausgewählt werden. Der Download erfolgt aus dem ETS Projekt heraus wie bei anderen Geräten auch.

7.3. Über direkte IP Verbindung

Während KNXnet/IP Tunneling auf die Geschwindigkeit von KNX TP begrenzt sind, kann über eine direkte IP Verbindung das Gerät mit hoher Geschwindigkeit geladen werden. Die direkte IP Verbindung ist möglich, wenn das Gerät bereits sowohl eine gültige IP Konfiguration als auch eine physikalische Adresse besitzt. Dazu muss im ETS Menü bei „Bus - Verbindungen – Optionen“ die Auswahl „Direkte IP-Verbindung verwenden wenn möglich“ angewählt werden. Der Download erfolgt dann direkt in das Gerät und ist nicht im ETS Gruppenmonitor sichtbar.

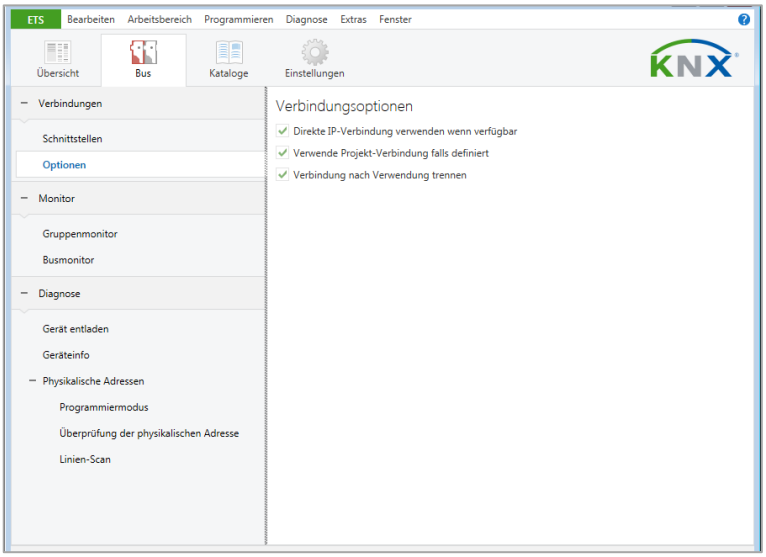


Figure 8 – Verbindungsoptionen

Aufgrund der deutlich kürzeren Übertragungszeiten wird empfohlen, Downloads über IP durchzuführen.

8. Schnittstelleneinstellungen in der ETS

Das KNX IP Interface secure dient als Programmierschnittstelle. Die ETS kann mit dieser Funktion über IP eine Verbindung in die jeweilige TP Linie aufbauen.

In der ETS können Schnittstellen über das ETS Menü „Bus - Schnittstellen“ ausgewählt und konfiguriert werden.

Die ETS kann auf konfigurierte IP Schnittstellen auch ohne Datenbankeintrag zugreifen. Entspricht die Konfiguration nicht den Gegebenheiten der Installation, muss diese über das ETS Projekt konfiguriert werden. Siehe dazu den Abschnitt ETS Datenbank.

Ist im KNX IP Interface der Security-Modus aktiviert, ist ein Passwort erforderlich, um eine Verbindung herzustellen.

Im Auslieferungszustand erfolgt die Zuweisung der IP-Adresse automatisch über DHCP, d.h. es sind keine weiteren Einstellungen dafür notwendig. Um diese Funktion nutzen zu können, muss sich ein DHCP-Server im LAN befinden (z.B. haben viele DSL-Router einen DHCP-Server integriert).

Wenn das KNX IP Interface an das LAN angeschlossen wurde und eine gültige IP Adresse hat, sollte es von der ETS automatisch im Menüpunkt „Bus“ unter „gefundene Schnittstellen“ erscheinen.

Durch Anklicken der gefundenen Schnittstelle wird diese als aktuelle Schnittstelle ausgewählt. Auf der rechten Seite des ETS Fensters erscheinen dann verbindungsspezifische Informationen und Optionen.

Der angezeigte Gerätename und die „Host Physikalische Adresse“ (physikalische Adresse des Gerätes) kann nur innerhalb Ihres ETS Projekts geändert werden.

Das KNX IP Interface secure verfügt wie alle programmierbaren KNX Geräte über eine physikalische Adresse, mit der das Gerät angesprochen werden kann. Diese wird zum Beispiel von der ETS beim Download des Interfaces über den Bus verwendet.

Für die Interface-Funktion verwendet das Gerät zusätzliche physikalische Adressen, die in der ETS eingestellt werden können. Sendet ein Client (z.B. ETS) über das KNX IP Interface Telegramme auf den Bus, so enthalten diese als Absende- Adresse eine der zusätzliche Adressen. Jede Adresse ist einer Verbindung zugeordnet. Somit können Antworttelegramme eindeutig zum jeweiligen Client weitergeleitet werden.

Die zusätzlichen physikalischen Adressen müssen aus dem Adressbereich der Bus-Linie sein, in der sich das Interface befindet und dürfen nicht von einem anderen Gerät verwendet werden..

Beispiel:

Geräteadresse	1.1.10	(Geräteadresse in der Topologie)
Verbindung 1	11.1.240	(1. zusätzliche Adresse)
Verbindung 2	11.1.241	(2. zusätzliche Adresse)
Verbindung 3	11.1.242	(3. zusätzliche Adresse)
Verbindung 4	11.1.243	(4. zusätzliche Adresse)
Verbindung 5	11.1.244	(5. zusätzliche Adresse)
Verbindung 6	11.1.245	(6. zusätzliche Adresse)
Verbindung 7	11.1.246	(7. zusätzliche Adresse)
Verbindung 8	11.1.247	(8. zusätzliche Adresse)

Im Abschnitt “Physikalische Adresse” kann die physikalische KNX Adresse der aktuell verwendeten KNXnet/IP Tunneling Verbindung ausgewählt werden.

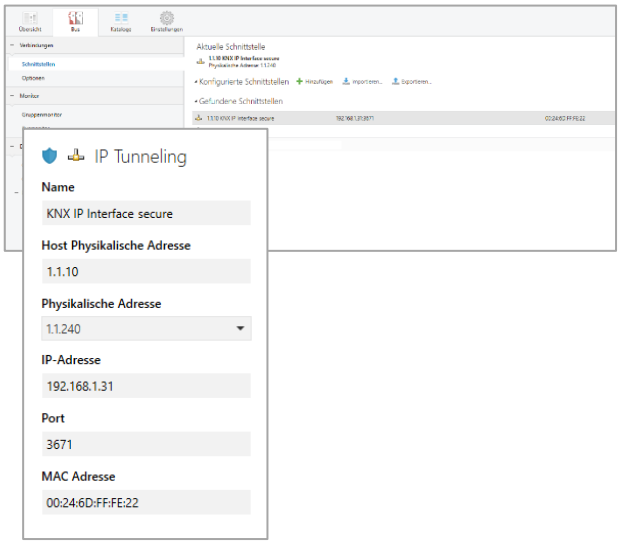


Figure 9 – IP Tunneling

Die physikalische KNX Geräteadresse sowie die physikalischen KNX Adressen für die zusätzlichen Tunneling Verbindungen können innerhalb des ETS Projekts geändert werden, nachdem das Gerät dem Projekt hinzugefügt wurde.

9. Fernzugriff

9.1. Network Address Translation (NAT)

NAT (Network Address Translation) ist ein Verfahren, um externe IP-Adressen auf interne umzusetzen. Dies wird vor allem in Routern (z.B. DSL-Routern) verwendet.

WARNING

Bitte beachten Sie, dass der Fernzugriff über NAT ohne weitere Schutzmaßnahmen erhebliche Gefahren birgt. Durch die ungeschützte Portfreigabe wird ein allgemeiner Zugang in Ihr lokales IP Netzwerk und in Ihr KNX System möglich.

Jeder Internetnutzer weltweit kann den freigegebenen Port an Ihrer festen, öffentlichen IP Adresse finden und damit z.B. über die ETS Software auf Ihr KNX Netzwerk zugreifen. Wir raten dringend, den Zugang über NAT nur temporär zu Test- oder Diagnosezwecken zu öffnen und anschließend den Port umgehend wieder zu schließen, um Missbrauch zu verhindern.

Sollte der Fernzugriff über NAT realisiert werden, raten wir Ihnen dringend, nicht den Standard-Port 3671 in Richtung Internet anzugeben. Da es sich bei Port 3671 um den offiziellen Port für efcp – eFieldControl(EIBnet) der KNX Association handelt, kann dieser leichter von Unbefugten ermittelt werden. Bitte verwenden Sie einen Port aus dem nicht reservierten Bereich zwischen Port 50000 und Port 60000.

Ein dauerhafter Fernzugriff sollte nur geschützt eingerichtet werden! Dazu empfehlen wir den Fernzugriff über VPN (Virtual Private Network). Die VPN Funktion ist in vielen DSL Routern bereits integriert.

9.2. Fernzugriff über ein VPN

Ein VPN ist eine Erweiterung privater Netzwerke. Über ein VPN lassen sich Fernzugriff (Site-To-End) und Kopplung privater Netzwerke (Site-To-Site) über das Internet realisieren.

Site-to-end

Mit einem Site-To-End VPN kann ein Zugriff auf ein internes Netz aufgebaut werden. Beispielsweise können sich so Mitarbeiter von außerhalb in das Netz ihrer Firma einwählen.

Site-to-site

Mit einem Site-To-Site VPN können private Netze untereinander gekoppelt werden. Beispielsweise erlaubt ein Site-To-Site VPN die Kopplung zweier entfernter Firmennetze.

Die IP-Schnittstelle wird nicht automatisch gefunden. Sie muss manuell konfiguriert werden.

Der Haken „Verbinden im NAT-Modus“ ist zwingend zu setzen. Die Verbindung wird dennoch nicht im NAT-Modus aufgebaut. Durch diese Aktivierung wird eine wichtige Initialisierung durchgeführt, die bedingt durch den IP-Aufsatz nötig ist.

9.3. Fernzugriff und KNX secure

Aus den verschiedenen Arten auf das Gerät zuzugreifen und der Möglichkeit KNX secure oder KNX unsecure zu benutzen, ergeben sich folgende Möglichkeiten.

	NAT	VPN
KNX unsecure	Warnung! ungeschützt	OK
KNX secure	OK	optimaler Schutz

Ein Fernzugriff über NAT und KNX unsecure ist vollkommen ungeschützt und sollte auf keinen Fall verwendet werden. Ein optimaler Schutz ergibt sich aus der gleichzeitigen Verwendung von KNX Security und VPN.

10. Open Source Lizenzen

Die in diesem Produkt eingesetzte Firmware basiert auf folgendem Open-Source Softwarepaket:

curve25519-donna: Curve25519 elliptic curve, public key function

Quelle: http://code.google.com/p/curve25519-donna/

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WARNUNG

- Das Gerät darf nur von einer zugelassenen Elektrofachkraft installiert und in Betrieb genommen werden.
- Die geltenden Sicherheits- und Unfallverhütungsvorschriften sind zu beachten.
- Das Gerät darf nicht geöffnet werden.
- Bei der Planung und Errichtung von elektrischen Anlagen sind die einschlägigen Richtlinien, Vorschriften und Bestimmungen des jeweiligen Landes zu beachten.

Hager Electro SAS
132 Boulevard d'Europe
BP3
67210 OBERNAI CEDEX
hager.com

6LE008080A