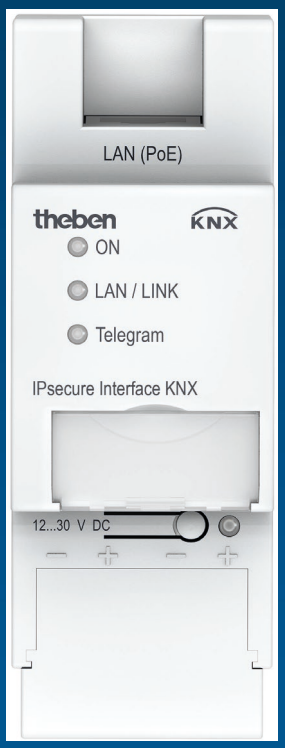
IPsecure Schnittstelle KNX
9070771
Handbuch



Inhalt

Seite

1 Allgemein

Die Theben IPsecure Schnittstelle KNX verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden.

Das Gerät unterstützt das KNX Secure Protokoll (KNXnet/IP Security).

1.1 Nutzung des Produkthandbuches

Das vorliegende Handbuch gibt Ihnen detaillierte technische Informationen über Funktion, Montage und Programmierung des Theben KNX-Geräts. Anhand von Beispielen wird der Einsatz erläutert.

Das Handbuch ist in folgende Kapitel unterteilt:

Kapitel 1	Allgemein
Kapitel 2	Gerätetechnik
Kapitel 3	Inbetriebnahme
Kapitel 4	Planung und Anwendung
Kapitel A	Anhang

1.1.1 Hinweise

In diesem Handbuch werden Hinweise und Sicherheitshinweise folgendermaßen dargestellt:

Hinweis
Bedienungserleichterungen, Bedienungstipps

Beispiele
Anwendungsbeispiele, Einbaubeispiele, Programmierbeispiele

Wichtig
Dieser Sicherheitshinweis wird verwendet, sobald die Gefahr einer Funktionsstörung besteht, ohne Schaden- oder Verletzungsrisiko.

Achtung
Dieser Sicherheitshinweis wird verwendet, sobald die Gefahr einer Funktionsstörung besteht, ohne Schaden- oder Verletzungsrisiko.

 **Gefahr**
Dieser Sicherheitshinweis wird verwendet, sobald bei unsachgemäßer Handhabung Gefahr für Leib und Leben besteht.

 **Gefahr**
Dieser Sicherheitshinweis wird verwendet, sobald bei unsachgemäßer Handhabung akute Lebensgefahr besteht.

1.2 Cyber Security (Netzwerksicherheit)

Die Branche ist verstärkt mit Internetsicherheitsrisiken konfrontiert. Um Stabilität, Sicherheit und Robustheit seiner Lösungen zu erhöhen, hat Theben im Rahmen des Produktentwicklungsprozesses offiziell Robustheitsprüfungen zur Internetsicherheit eingeführt.

Die folgenden Hinweise dienen darüber hinaus als Leitfaden und beschreiben Mechanismen, die verwendet werden können, um die Sicherheit von KNX-Anlagen zu verbessern.

1.3 Verhindern des Zugangs zu den unterschiedlichen Medien

Die Basis jedes Schutz-Konzeptes bildet die sorgfältige Abschottung des Systems gegen unberechtigten Zugriff. Im Falle einer KNX-Anlage gilt, dass nur befugte Personen (Installateur, Hausmeister, Nutzer) physischen Zugang zur KNX-Anlage haben dürfen. Bei der Planung und Installation müssen für jedes KNX-Medium die kritischen Punkte bestmöglich geschützt werden.

Allgemein gilt, dass Anwendungen und Geräte fest installiert werden sollten, um zu verhindern, dass diese leicht entfernt werden und dadurch unbefugte Personen Zugang zur KNX-Anlage erhalten. Unterverteilungen mit KNX-Geräten sollten verschlossen sein oder sich in Räumen befinden, zu denen nur befugte Personen Zugang haben.

1.4 Twisted Pair-Verkabelung

- Die Leitungsenden des KNX-Twisted Pair-Kabels sollten nicht sichtbar sein oder aus der Wand heraustreten, weder im noch außerhalb des Gebäudes.
- Wenn verfügbar sollten die Diebstahlschutzeinrichtungen der Applikationsmodule verwendet werden.
- Busleitungen im Außenbereich stellen ein erhöhtes Risiko dar. Der physische Zugang zum KNX-Twisted Pair-Kabel sollte hier besonders erschwert werden.
- Geräte, die in begrenzt geschützten Bereichen verbaut sind (Außenbereich, Tiefgarage, WC, etc.), können als zusätzlicher Schutz als eigene Linie ausgeführt werden. Durch Aktivierung der Filtertabellen im Linienkoppler (nur KNX) wird verhindert, dass ein Angreifer Zugriff auf die gesamte Anlage erlangen kann.

1.5 IP-Verkabelung innerhalb des Gebäudes

Für die Gebäudeautomation sollte ein getrenntes LAN- oder WLAN-Netzwerk mit eigener Hardware (Router, Switches etc.) verwendet werden.

Unabhängig von der KNX-Anlage sind unbedingt die üblichen Sicherheitsmechanismen für IP-Netzwerke anzuwenden. Diese sind beispielsweise:

- MAC-Filter
- Verschlüsselung von Drahtlosnetzwerken
- Verwendung starker Passwörter und Schutz derselben vor unbefugten Personen

Hinweis
Während eines IP-, TCP- oder UDP-Flooding (Zugriff aus dem Internet) ist das Gerät nicht erreichbar. Um diese Reaktion zu vermeiden, ist eine Datenratenlimitierung auf Netzwerkebene einzustellen. Bitte sprechen Sie dazu mit dem Netzwerkadministrator.

1.6 Anbindung an das Internet

Das Gerät ist nicht zur Verwendung im öffentlichen Internet vorgesehen. Aus diesem Grund dürfen keine Ports von Routern Richtung Internet geöffnet werden; dies verhindert, dass die KNX-Kommunikation im Internet sichtbar wird.

Ein Zugriff auf eine Anlage aus dem Internet kann auf folgende Weise ermöglicht werden:

- Zugang zu KNX-Installationen über VPN-Verbindungen: Dies setzt jedoch einen Router mit VPN-Server-Funktionalität voraus.
- Verwendung von herstellerspezifischen Lösungen oder Visualisierungen, z. B. mit Zugang über https.

1.7 KNXnet/IP Security

Das Gerät sollte immer im KNX-Secure-Modus betrieben werden. So ist sichergestellt, dass die Tunneling-Server und die Inbetriebnahme des Gerätes selbst sicher sind.

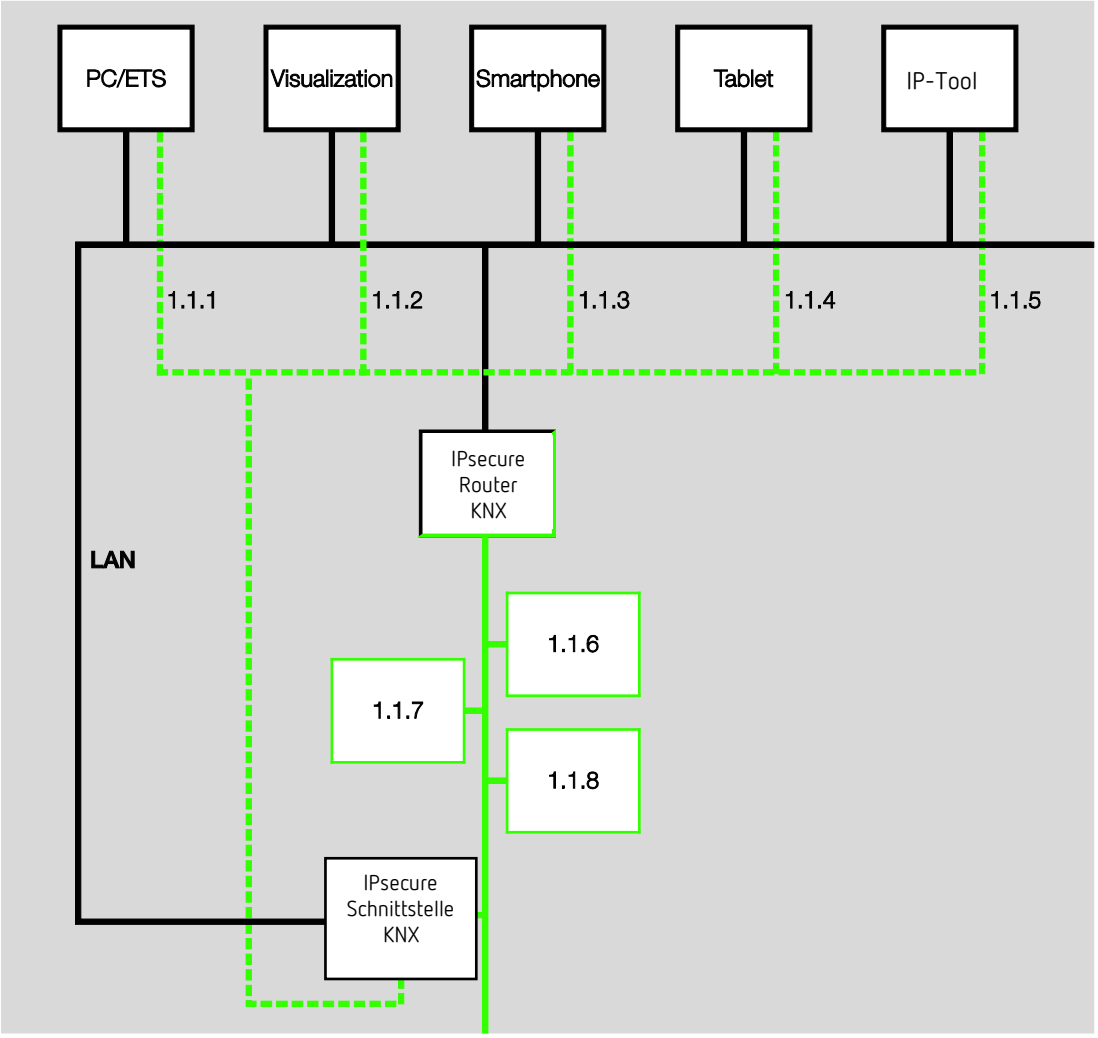
Siehe auch Kapitel 3.5, KNX Secure.

1.8 Produkt- und Funktionsübersicht

Die Theben IPsecure Schnittstelle KNX verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden.

Die Schnittstelle kann als Programmierschnittstelle (ETS) eingesetzt werden und Clients, wie z. B. Visualisierungen, können über die Schnittstelle auf den KNX-Bus zugreifen.

Das Gerät verwendet zur Kommunikation das KNXnet/IP Protokoll sowie das KNXnet/IP Security Protokoll der KNXAssociation (Tunneling).



Die Schnittstelle verfügt über 5 Tunneling Server, siehe Kapitel Die Verwendung der integrierten Tunneling Server. Diese unterstützen sowohl den Busmonitor- als auch den Gruppenmonitorbetrieb. Die Tunneling-Server können im KNX Secure-Modus betrieben werden. Die Spannungsversorgung kann über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 erfolgen oder über eine Versorgungsspannung. Wird beides gleichzeitig angeschlossen, wird PoE verwendet.

Für die IPsecure Schnittstelle steht das Theben IP-Tool zur Verfügung, mit dem die Schnittstellen im Netzwerk gefunden werden können (IP-Discovery).
Für das Firmware Update steht eine ETS App (Theben Update App) zur Verfügung. Sofern der KNX- Secure-Modus bei den Geräten nicht aktiviert ist, kann ein Firmware Update auch mit dem IP-Tool erfolgen.

Während des Updatevorgangs muss zusätzlich zum IP-Netzwerk (LAN) auch der KNX-Bus (TP) angeschlossen sein. Andernfalls schlägt der Updatevorgang fehl. Es muss sichergestellt werden, dass während des Updatevorgangs kein Spannungsausfall (KNX oder IP) auftritt, da ansonsten das Gerät zerstört werden kann.

1.8.1 Übersicht Versionen

Die nachfolgende Tabelle gibt einen Überblick, welche Funktionen mit der IPsecure Schnittstelle KNX und den Applikationsprogrammen *IP-Schnittstelle ETS 3* (ETS 3 und ETS 4), *IP-Schnittstelle* (ab ETS 4) möglich sind.

Gerät	IP-Schnittstelle KNX	
Applikation	IP-Schnittstelle KNX	IPsecure Schnittstelle
ETS	Ab ETS 3	Ab ETS 5
Eigenschaften *IPsecure Schnittstelle KNX*		
Anzahl Tunneling Server	1	5
IP-Discovery (IP-Tool)	■	■
Firmware Update (IP-Tool)	■	■*
Firmware Update mit Theben Update App	-	■
Power over Ethernet	■	■
KNX Secure	-	■

■ = Eigenschaft trifft zu

- = Eigenschaft trifft nicht zu

* Nur, wenn Gerät nicht im KNX Secure-Modus betrieben wird

2 Gerätetechnik

IPsecure Schnittstelle KNX

Die IPsecure Schnittstelle KNX verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden.

Die Schnittstelle kann als Programmierschnittstelle (ETS) eingesetzt werden und Clients, wie z. B. Visualisierungen, können über die Schnittstelle auf den KNX-Bus zugreifen.

Das Gerät verwendet zur Kommunikation das KNXnet/IP Protokoll sowie das KNXnet/IP Security Protokoll der KNX Association (Tunneling).

Die Stromversorgung erfolgt über 12 bis 30 V DC oder PoE (Power over Ethernet) nach IEEE 802.3af Class 1. Wird beides gleichzeitig angeschlossen, wird PoE verwendet.

2.1 Technische Daten

Versorgung	Versorgungsspannung U_s	12...30 V DC (+10 % / -15 %) oder PoE (IEEE 802.3af Klasse 1)
	Verlustleistung	Maximal 1,8 W
	Stromaufnahme Hilfsspannung	Maximal 120 mA bei 12 V
	Nennspannung U_n	12 V DC
	Stromaufnahme KNX	< 10 mA
Anschlüsse	KNX	Busanschlussklemme
	Steckklemme für Betriebsspannung	Steckklemme
	LAN	RJ45-Buchse für 10/100BaseT, IEEE 802.3 Netzwerke, AutoSensing
Bedien- und Anzeigeelemente	LED rot und Taste	Zur Vergabe der physikalischen Adresse
	LED grün "On"	Anzeige Betriebsbereitschaft
	LED gelb "LAN/Link"	Anzeige Netzwerkverbindung
	LED gelb "Telegram"	Anzeige KNX-Telegrammverkehr
Schutzart	IP 20	Nach DIN EN 60 529
Schutzklasse	II	Nach DIN EN 61 140
Isolationskategorie	Überspannungskategorie	III nach DIN EN 60 664-1
	Verschmutzungsgrad	2 nach DIN EN 60 664-1
KNX-Sicherheitskleinspannung	SELV 30 V DC	
Temperaturbereich	Betrieb	-5 °C...+45 °C
	Lagerung	-25 °C...+55 °C
	Transport	-25 °C...+70 °C
Umgebungsbedingung	maximale Luftfeuchte	95 %, keine Betauung zulässig
	Luftdruck	Atmosphäre bis 2.000 m

IPsecure Schnittstelle KNX
Gerätetechnik

Design	Reiheneinbaugerät (REG)	Modulares Installationsgerät, Pro*M*
	Abmessungen	90 x 36 x 64 mm (H x B x T)
	Einbaubreite	2 Module à 18 mm
	Einbautiefe	68 mm
Montage	Auf Tragschiene 35 mm	Nach DIN EN 60 715
Einbaulage	Beliebig	
Gewicht	0,1 kg	
Gehäuse, Farbe	Kunststoff, halogenfrei, grau	
Approbation	KNX nach EN 50 090-1, -2	
CE-Zeichen	gemäß EMV- und Niederspannungsrichtlinien	

Gerätetyp	Applikation	maximale Anzahl Kommunikationsobjekte	maximale Anzahl Gruppenadressen	maximale Anzahl Zuordnungen
IPsecure Schnittstelle KNX	IPsecure Schnittstelle/...*	0	0	0

* ... = aktuelle Versionsnummer der Applikation. **Bitte beachten Sie hierzu die Softwareinformationen auf unserer Homepage.**

Hinweis

Für die Programmierung sind die ETS (ETS 5 Version 5.7.4 oder höher) und die aktuelle Applikation des Gerätes erforderlich.

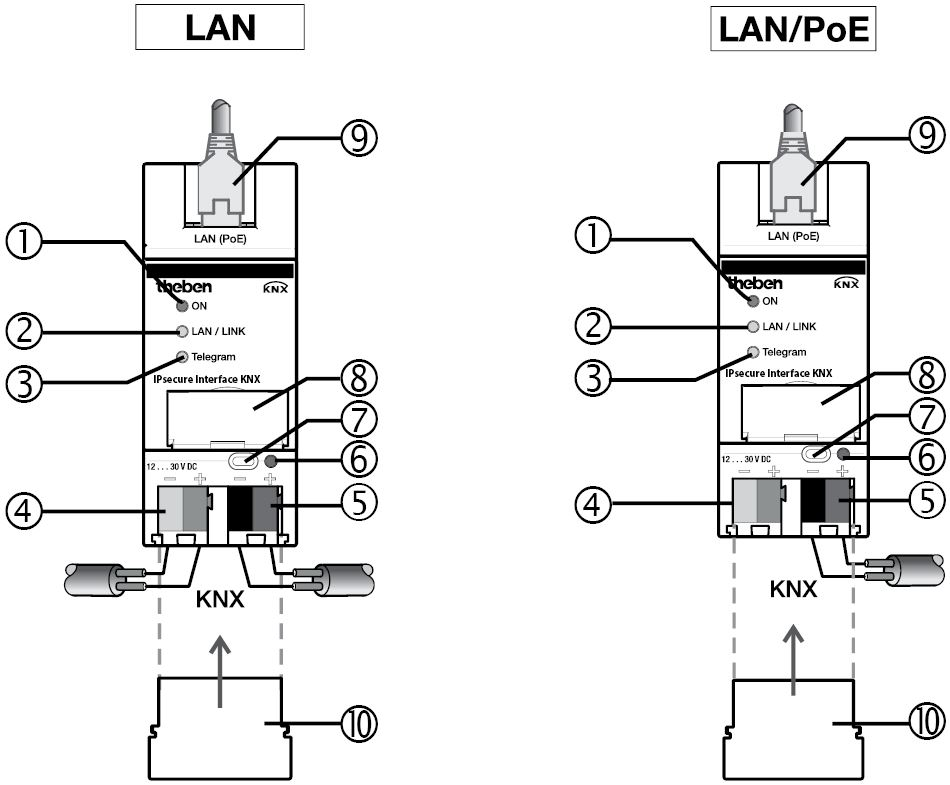
Soll das Gerät im KNX-Secure-Modus betrieben werden, ist zusätzlich der seitlich auf dem Gerät agenbrachte Inbetriebnahmeschlüssel (FDSK, siehe Kapitel KNX Secure) erforderlich.

Die aktuelle Applikation finden Sie mit der entsprechenden Softwareinformation zum Download im Internet unter *www.theben.de/downloads*. Nach dem Import in die ETS liegt das Gerät im Fenster *Kataloge* unter *Theben AG/Systemgeräte/IP-Schnittstellen*.

Das Gerät unterstützt nicht die Verschließfunktion eines KNX-Geräts in der ETS. Falls Sie den Zugriff auf alle Geräte des Projekts durch einen *BCU-Schlüssel* sperren, hat es auf dieses Gerät keine Auswirkung. Es kann weiterhin ausgelesen und programmiert werden.

Ausnahme: Wenn der KNX-Secure-Modus aktiviert ist, kann das Gerät nur mit dem bestehenden Projekt programmiert werden.

2.2 Anschlussbild



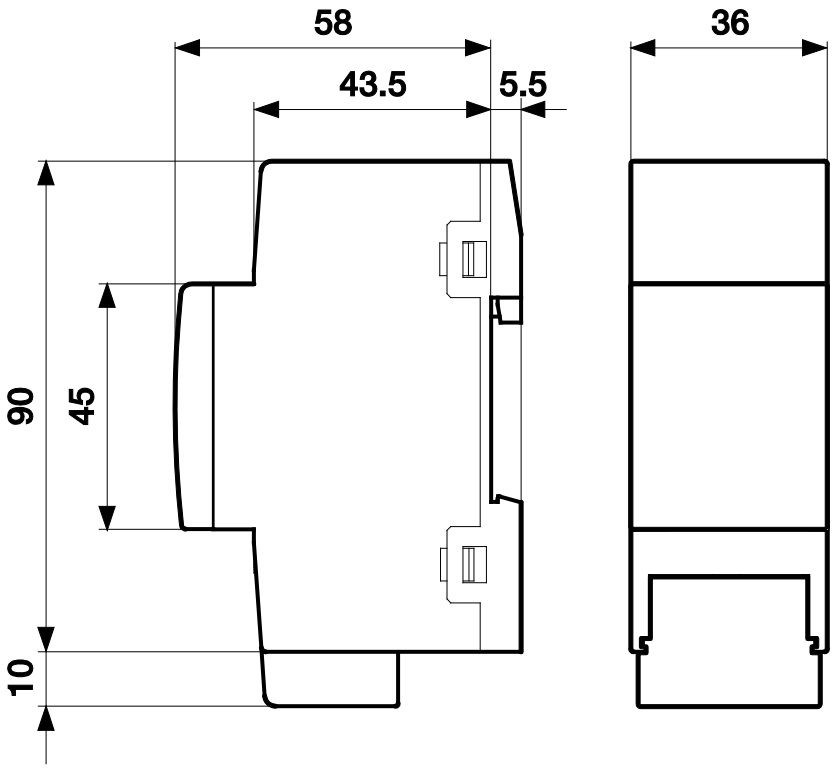
IPsecure Schnittstelle KNX

Legende

1	LED ON	6	LED Programmieren
2	LED LAN/LINK	7	Taste Programmieren
3	LED Telegramm	8	Schildträger
4	Anschluss Versorgungsspannung	9	Anschluss LAN bzw. LAN/PoE
5	Anschluss KNX	10	Abdeckkappe

Hinweis
Es ist auch möglich, die Schnittstelle über den unverdrosselten Spannungsausgang einer Theben KNX-Spannungsversorgung zu versorgen. Dadurch reduziert sich die Anzahl der KNX-Geräte, die an die Theben KNX-Spannungsversorgung angeschlossen werden können, entsprechend.

2.3 Maßbild



IPsecure Schnittstelle KNX

2.4 Montage und Installation

Das Gerät ist ein Reiheneinbaugerät zum Einbau in Verteilern zur Schnellbefestigung auf 35-mm-Tragschienen nach DIN EN 60 715.

Das Gerät kann in jeder Einbaulage montiert werden.

Die Verbindung zum Bus erfolgt über die mitgelieferte Busanschlussklemme. Die Klemmenbezeichnung befindet sich auf dem Gehäuse.

Das Gerät ist betriebsbereit, nachdem die Busspannung und die Hilfsspannung angelegt wurden.

Die Zugänglichkeit des Geräts zum Betreiben, Prüfen, Besichtigen, Warten und Reparieren muss gemäß DIN VDE 0100-520 sichergestellt sein.

Inbetriebnahmevoraussetzung

Um das Gerät in Betrieb zu nehmen, werden ein PC mit der ETS (ETS 5 Version 5.7.4 oder höher) sowie eine Versorgungsspannung von 12 bis 30 V DC benötigt. Alternativ kann die Versorgung über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 erfolgen.

Mit dem Anlegen der Busspannung und der Hilfsspannung ist das Gerät betriebsbereit.

Montage und Inbetriebnahme dürfen nur von Elektrofachkräften ausgeführt werden. Bei der Planung und Errichtung von elektrischen Anlagen sowie von sicherheitstechnischen Anlagen für Einbruch- und Branderkennung sind die einschlägigen Normen, Richtlinien, Vorschriften und Bestimmungen des jeweiligen Landes zu beachten.

- Gerät bei Transport, Lagerung und im Betrieb vor Feuchtigkeit, Schmutz und Beschädigung schützen!
- Gerät nur innerhalb der spezifizierten technischen Daten betreiben!
- Gerät nur im geschlossenen Gehäuse (Verteiler) betreiben!
- Vor Montagearbeiten ist das Gerät spannungsfrei zu schalten.

Gefahr

Um gefährliche Berührungsspannung durch Rückspeisung aus unterschiedlichen Außenleitern zu vermeiden, muss bei einer Erweiterung oder Änderung des elektrischen Anschlusses eine allpolige Abschaltung vorgenommen werden.

Auslieferungszustand

Das Gerät wird mit der physikalischen Adresse 15.15.255 und 5 weiteren physikalischen Adressen 15.15.100 für Tunneling-Verbindungen ausgeliefert.

Die IP-Adresse ist auf automatische Vergabe (DHCP/AutoIP) eingestellt.

Vergabe der physikalischen Adresse

In der ETS erfolgt die Vergabe und Programmierung der physikalischen Adressen und Parameter.

Das Gerät besitzt zur Vergabe der physikalischen Adresse eine Taste *Programmieren*. Nachdem die Taste betätigt wurde, leuchtet die rote LED *Programmieren* auf. Sie erlischt, sobald die ETS die physikalische Adresse vergeben hat oder die Taste *Programmieren* erneut betätigt wurde.

Downloadverhalten

Das Gerät kann auf unterschiedliche Arten programmiert werden: Über einen der integrierten Tunneling Server ("lokaler Download") oder über eine weitere Programmierschnittstelle (USB oder IP).

Hinweis
Wird für die Programmierung eines KNX-Secure-Gerätes eine USB-Schnittstelle verwendet, muss diese „Long Frames" unterstützen. Geeignet ist z. B. eine USB-Schnittstelle von Theben.

Damit das Gerät programmiert werden kann, muss eine Verbindung zum KNX-TP (Twisted Pair) bestehen.

Nach erfolgtem Download startet das Gerät neu und schließt alle offenen Tunneling-Verbindungen. Sofern beim Download die IP-Adresse des Gerätes geändert wurde, müssen die Tunneling-Verbindungen manuell in den Tunneling Clients neu konfiguriert werden. Tunneling Clients stellen die Verbindung zum Server über die IP-Adresse her.

Die Übernahme der mit der ETS parametrierten Daten erfolgt ca. 30-60 Sekunden nach dem Download.

Entladen des Gerätes und Rücksetzen auf Werkseinstellungen

Das Gerät kann auf Werkseinstellungen zurückgesetzt werden. Da es sich um ein Secure-Gerät handelt, ist folgendes zu beachten:

Im KNX-Secure-Modus-Betrieb kann das Gerät über die ETS nur dann zurückgesetzt werden, wenn die ETS das Projekt verwendet, mit dem das Gerät parametriert wurde, bzw. wenn im Projekt der Inbetriebnahmeschlüssel vorhanden ist.

Über einen Rechtsklick auf das Gerät in der ETS kann das Gerät entladen werden.

Option: Applikation entladen

- Die IP-Adresse und IP-Konfiguration bleiben erhalten.
- Die Passwörter und IP-Adressen der Tunnelingserver werden gelöscht.
- Der von der ETS vergebene Tool Key bleibt erhalten, d. h.für die erneute Programmierung ist der FDSK nicht erforderlich.
- Die physikalische Adresse bleibt erhalten.

Option: Physikalische Adresse und Applikation entladen

- Das Gerät wird auf Werkszustand zurück gesetzt.
- Für die erneute Inbetriebnahme ist der FDSK notwendig, sofern er nicht von der ursprünglichen Inbetriebnahme noch im ETS-Projekt vorhanden ist.

Das Zurücksetzen auf Werkseinstellungen kann auch direkt am Gerät vorgenommen werden. Dies stellt kein Sicherheitsrisiko dar, da das Gerät anschließend nicht mehr Teil der Anlage ist.

- Drücken der Programmiertaste bei nicht verbundenem KNX-Bus.
- Programmiertaste gedrückt halten und Busklemme aufstecken. Die Programmier-LED blinkt (2 Hz).
- Taste mindestens 5 s gedrückt halten und dann loslassen. Die Programmier-LED erlischt, das Gerät startet neu mit Werkseinstellungen.

Verbindet sich nach dem Rücksetzen die ETS mit dem Gerät und der FDSK Schlüssel des Gerätes ist der ETS noch bekannt, kann die Schnittstelle erneut programmiert werden. Die ETS meldet, dass das Gerät zurückgesetzt wurde.

Weitere Hinweise zum FDSK (Factory Default Setup Key), siehe Kapitel KNX Secure.

Reinigen

Das Gerät ist vor dem Reinigen spannungsfrei zu schalten. Verschmutzte Geräte können mit einem trockenen oder leicht mit Seifenlauge angefeuchteten Tuch gereinigt werden. Auf keinen Fall dürfen ätzende Mittel oder Lösungsmittel verwendet werden.

Wartung

Bei Schäden, z. B. durch Transport und/oder Lagerung, dürfen keine Reparaturen vorgenommen werden. Bitte halten Sie die Firmware des Gerätes aktuell, siehe Kapitel Firmware Update.

2.5 Beschreibung der Ein- und Ausgänge

Versorgungsspannungseingang 12 bis 30 V DC

Am Eingang für die Versorgungsspannung darf nur eine Gleichspannung von 12 bis 30 V angeschlossen werden. Wir empfehlen die Verwendung der Netzteile Spannungsversorgung 640 mA S KNX aus unserem Sortiment. Es ist auch möglich, die Schnittstelle über den unverdrosselten Spannungsausgang einer Theben KNX-Spannungsversorgung zu versorgen.

Achtung
Die Versorgungsspannung muss 12 bis 30 V DC betragen, oder das Gerät wird über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 versorgt. Bei Anschluss des Gerätes an eine Spannung außerhalb des zulässigen Bereiches kann das Gerät zerstört werden!

KNX-Anschluss

Zum Anschluss an den KNX-Bus wird die mitgelieferte Busanschlussklemme verwendet.

Hinweis
Zur Programmierung ist die ETS (ETS 5 Version 5.7.4 oder höher) erforderlich.

LAN-Anschluss

Die Netzwerkanbindung erfolgt über eine Ethernet-RJ45-Schnittstelle für LAN-Netzwerke. Die Netzwerkschnittstelle kann mit einer Übertragungsgeschwindigkeit von 10/100 MBit/s betrieben werden. Die Netzwerkaktivität wird durch die LED LAN/LINK auf der Gehäusefrontseite angezeigt.

2.6 Bedienelemente

Es befinden sich keine Bedienelemente an der IPsecure Schnittstelle KNX.

2.7 Anzeigeelemente

Auf der Frontseite des Gerätes befinden sich drei LED zur Anzeige:

ON LAN/LINK Telegram

ON

- Die LED leuchtet wenige Sekunden nach Zuschalten der Hilfsspannung.
- Die LED leuchtet nach dem Zuschalten der Hilfsspannung zunächst dauerhaft. Nach ca. 40 Sekunden fängt die LED an zu blinken, bis der Startvorgang vollständig abgeschlossen ist und die LED wieder dauerhaft leuchtet.

LAN/LINK

- Die LED leuchtet, wenn die Hilfsspannung vorhanden ist und die Schnittstelle an ein Ethernet-Netzwerk angeschlossen ist.
- Die LED blinkt, wenn das Gerät Aktivität auf dem Netzwerk erkennt, z. B. wenn Daten ausgetauscht werden.

Telegram

- Die LED leuchtet, wenn die Schnittstelle an ein TP-Netzwerk angeschlossen ist und der Startvorgang (siehe LED "On") vollständig abgeschlossen ist.
- Die LED blinkt, wenn das Gerät Aktivität auf der KNX-Sublinie TP1 (Twisted Pair 1) erkennt, z. B. wenn Daten ausgetauscht werden.

3 Inbetriebnahme

Die Parametrierung der IPsecure Schnittstelle KNX erfolgt mit der Applikation und der Engineering Tool Software ETS.

Die Applikation ist unter *Theben AG/Systemgeräte/IP-Schnittstellen* zu finden.

Für die Parametrierung wird ein PC oder Laptop mit der ETS und eine Anbindung an den KNX-Bus benötigt.

3.1 Überblick

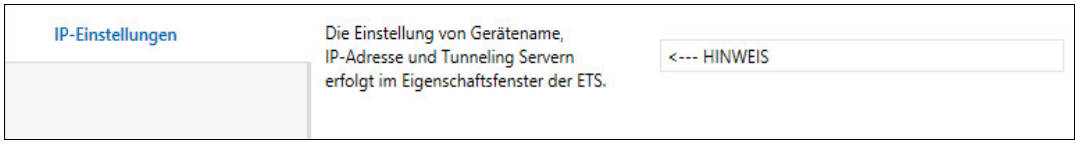
Die Parametrierung der IPsecure Schnittstelle KNX erfolgt mit der Engineering Tool Software (ETS 5 Version 5.7.4 oder höher).

3.2 Parameter

Dieses Kapitel beschreibt die Parameter der IPsecure Schnittstelle KNX anhand der Parameterfenster.

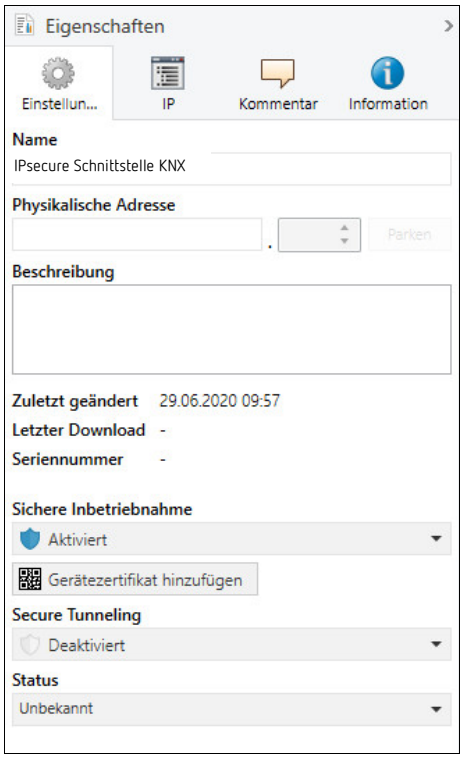
Parameterfenster *IP-Einstellungen*

Bei dem Gerät werden alle Parameter im Eigenschaftsfenster der ETS eingestellt.



Hinweis
Die Einstellung von Gerätename, IP-Adresse und Tunneling Servern erfolgt im Eigenschaftsfenster der ETS.

Die Konfiguration der IP-Parameter (Gerätename, Zuweisung der IP-Adresse per DHCP oder fest) erfolgt im entsprechenden Eigenschaftenfenster der ETS.



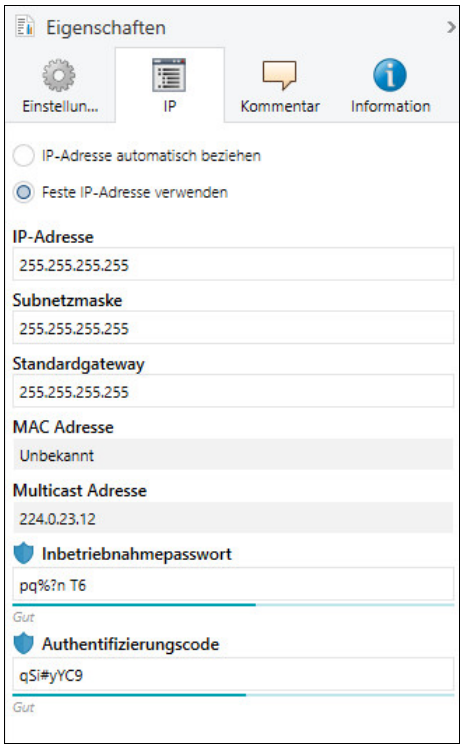
Im Eigenschaftsfenster *Einstellungen* kann der Gerätename eingetragen werden. Im Feld *Name* kann der Gerätename, der ins Gerät geladen wird, geändert werden.

Der Gerätename dient der Identifizierung des Geräts im LAN. Bei einer Suchanfrage, z. B. durch die ETS, meldet jedes KNXnet/IP-Gerät seinen Namen und kann darüber zugeordnet werden. So kann z. B. durch den Namen IPsecure Schnittstelle, EG, UV7 auch der Einbauort des Geräts mitgeteilt werden.

Hinweis
Bei Auslieferung lautet der Gerätename standardmäßig "IPsecure Schnittstelle". Nach dem ersten Download wird der Gerätename, der im Eigenschaftsfenster der ETS eingetragen wird, ins Gerät geladen.

Achtung
Es werden nur die ersten 30 Zeichen des Gerätenamens ins Gerät geladen, der Rest wird abgeschnitten.

Im Eigenschaftsfenster *IP* kann die IP-Adresse definiert werden.



Für die Einstellung der IP-Adresse stehen folgende Optionen zur Verfügung:

Optionen: IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden

- *IP-Adresse automatisch beziehen:* In der Standardeinstellung erwartet die IPsecure Schnittstelle die Zuweisung einer IP-Adresse durch einen DHCP-Server (dynamic host configuration protocol). Dieser Server vergibt auf Anfrage eine freie IP-Adresse an das Gerät. Ist kein DHCP-Server im Netzwerk verfügbar, so startet das Gerät eine Auto-IP-Prozedur. Es vergibt sich selbst eine Adresse aus dem reservierten Bereich für Auto-IP-Adressen (169.254.1.0 bis 196.254.254.255).

  Zu DHCP: siehe Kap. Vergabe der IP-Adresse.

- *Feste IP-Adresse verwenden:* Ist kein DHCP-Server im Netzwerk installiert oder soll die IP-Adresse immer gleich sein, so kann sie auch fest vergeben werden.
  Bei der Vergabe von festen IP-Adressen ist darauf zu achten, dass jedes Gerät eine unterschiedliche IP-Adresse erhält.

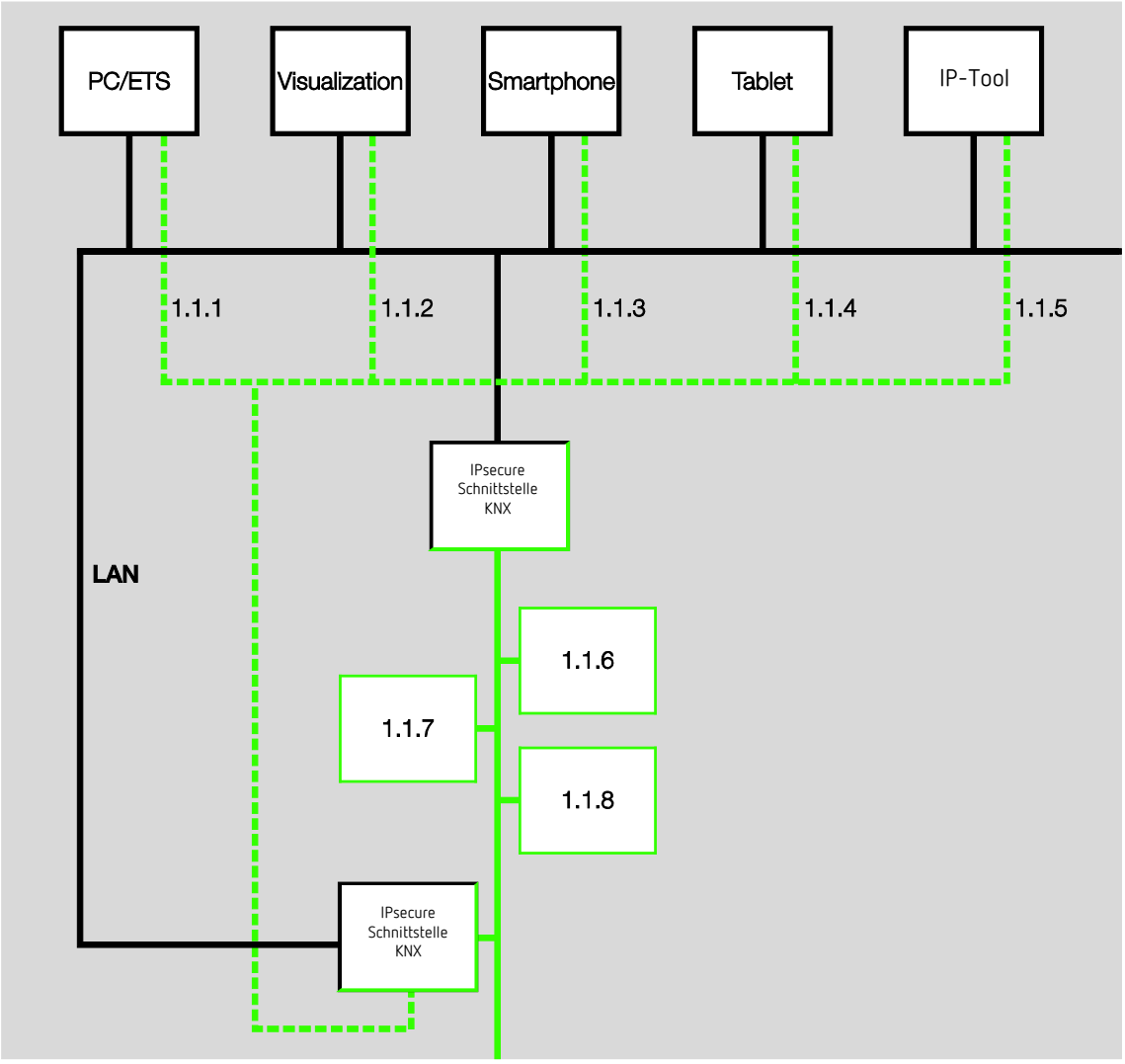
Hinweis
Die MAC-Adresse wird nach einem Download aus dem Gerät ausgelesen. Zusätzlich ist die MAC-Adresse auf dem Gerät aufgebracht und kann alternativ über das IP-Tool ermittelt werden.

3.3 Kommunikationsobjekte

Die IPsecure Schnittstelle KNX hat keine KNX-Kommunikationsobjekte.

3.4 Die Verwendung der integrierten Tunneling-Server

Die IPsecure Schnittstelle bietet 5 zusätzliche physikalische Adressen, die für eine Tunneling-Verbindung verwendet werden können. Diese sogenannten Tunneling Server können mit der ETS als Programmierschnittstelle oder mit einem anderen Client, z. B. einer Visualisierung, verwendet werden.



Beim Tunneling verbindet sich ein Client mit einer Buslinie. Das Tunneling-Verfahren verwendet UDP, beinhaltet aber eine Sicherungsschicht, so dass im Fehlerfall Telegramme wiederholt werden. Ab ETS 5 wird Tunneling V2 unterstützt. Hier wird anstatt UDP TCP verwendet und die Sicherungsschicht des TCP für die Übertragung verwendet.

Hinweis
Die physikalische Adresse für die Tunneling-Verbindung muss in die Topologie passen. Daher müssen die Adressen aus dem Adressbereich der Linie gewählt werden. Bei Auslieferung haben alle Tunneling Server die Adresse 15.15.100. Die Parametrierung der Tunneling-Verbindungen hängt von der verwendeten ETS-Version ab. • In der ETS 4 und ETS 5 werden die ersten 5 freien Adressen in der Linie vergeben, nachdem die Schnittstelle in eine Linie eingefügt wurde. • In der ETS 3 steht 1 Tunneling-Verbindung zur Verfügung.

Die Tunneling Server können auch mit KNX Secure verschlüsselt werden. Ist der KNX Secure-Modus aktiviert, benötigt ein Client das in der ETS vergebene Passwort.

Details siehe Kapitel KNX Secure.

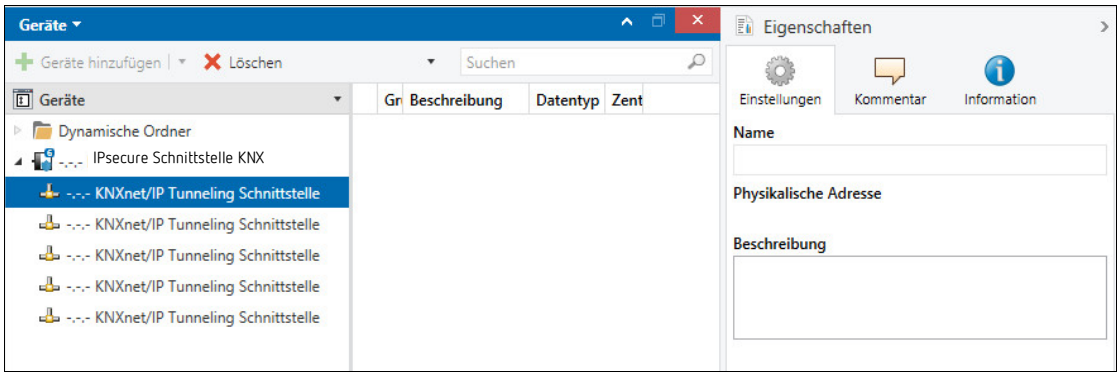
3.4.1 Einstellungen der Tunneling Server

In der ETS steht für die Einstellung der zusätzlichen physikalischen Adressen ein zusätzliches Eigenschaftenfenster zur Verfügung.

Die ETS reserviert automatisch nach Einfügen der Schnittstelle in die Linie die ersten fünf freien Adressen dieser Linie für die Tunneling Server der Schnittstelle. Dies ist eine Eigenschaft der ETS und kann nicht geändert werden.

Nach dem ersten Download stehen die Adressen im Gerät zur Verfügung.

Ist dies nicht erwünscht, kann die Einstellung manuell im Eigenschaftenfenster geändert werden:



Zum Ändern der Adresse die aktuelle Geräteadresse bzw. zusätzliche Adresse markieren und mit den Pfeiltasten nach oben oder unten die gewünschte Ziffer auswählen. Durch Markieren einer anderen Adresse wird die geänderte Adresse gespeichert.

Die geänderten Adressen werden erst nach einem Download vom Gerät übernommen.

Parken

Ist für einen Tunnel die Option *Parken* aktiviert, so erhält dieser Tunnel die Adresse 15.15.255.

Sofern bei allen Tunneling-Servern die Option *Parken* gewählt wird, erhalten alle Tunneling-Server die Adresse 15.15.255. Damit ist nur ein Tunneling-Server verfügbar.

3.5 KNX Secure

Die Theben IPsecure Schnittstelle KNX ist ein KNX-Gerät nach dem KNX-Secure-Standard. D. h. das Gerät kann sicher in Betrieb genommen werden und die Tunneling-Verbindungen sind verschlüsselt.

Bei der Inbetriebnahme des Geräts ist daher folgendes zu berücksichtigen:

- Sobald ein KNX-Secure-Gerät in ein Projekt importiert wird, muss zwingend ein Projektpasswort vergeben werden. Das Projekt ist damit gegen unbefugten Zugriff geschützt.
  Das Passwort muss sicher aufbewahrt werden – ohne dieses Passwort ist ein Zugriff auf das Projekt nicht möglich (auch nicht durch die KNX Association oder durch Theben)!
- Bei der Inbetriebnahme eines KNX-Secure-Gerätes (erster Download) ist ein Inbetriebnahmeschlüssel erforderlich. Dieser Schlüssel (FDSK = Factory Default Setup Key) ist auf einem Aufkleber seitlich auf dem Gerät aufgebracht und muss vor dem ersten Download in die ETS importiert werden.
  - Beim ersten Download des Gerätes öffnet sich in der ETS ein Fenster, das zur Eingabe des Schlüssels auffordert. Das Zertifikat kann alternativ auch mit einem QR-Code-Scanner eingelesen werden (empfohlen).
  - Alternativ können auch die Zertifikate aller Secure-Geräte vorab in die ETS eingegeben werden. Dies erfolgt auf der Projektübersichtsseite auf dem Reiter „Sicherheit".
  - Der FDSK Aufkleber ist doppelt auf dem Gerät aufgebracht. Ein Teil kann für die Projektdokumentation verwendet werden, der andere kann auf dem Gerät verbleiben.
    Ohne den FDSK kann das Gerät nach einem Reset nicht mehr im KNX-Secure-Modus betrieben werden!

Der FDSK wird nur für die Erstinbetriebnahme benötigt. Danach vergibt die ETS neue Schlüssel. Der FDSK wird erst wieder benötigt, wenn das Gerät auf Werkseinstellungen zurückgesetzt wurde (z. B. wenn das Gerät in einer anderen Anlage mit einem anderen ETS Projekt verwendet werden soll).

Die ETS erzeugt für jeden Tunneling-Server separate Passwörter. Die Passwörter können bei Bedarf geändert werden.
Die Schlüssel werden von der ETS erzeugt und verwaltet. Bei Bedarf können Schlüssel und Passwörter exportiert werden (z. B. falls ein Client auf einen der Tunnel zugreifen möchte).

Sofern erforderlich, kann die Schnittstelle auf Werkseinstellungen zurückgesetzt werden, siehe Kapitel Entladen des Gerätes und Rücksetzen auf Werkseinstellungen.

4 Planung und Anwendung

4.1 Die IPsecure Schnittstelle KNX im Netzwerk

Die IPsecure Schnittstelle ist für den Einsatz in 10/100-BaseT-Netzwerken nach IEEE 802.3 ausgelegt. Das Gerät besitzt eine AutoSensing-Funktion und stellt die Übertragungsgeschwindigkeit (10 oder 100 MBit) automatisch ein.

4.1.1 Vergabe der IP-Adresse

DHCP/AutoIP

Die IP-Adresse des Geräts kann von einem DHCP-Server bezogen werden. Dazu ist die Einstellung einer automatischen Vergabe der IP-Adresse in der ETS nötig, siehe Parameterfenster IP-Einstellungen. Wird bei dieser Einstellung kein DHCP-Server gefunden, startet das Gerät eine AutoIP-Prozedur und vergibt sich selbständig eine IP-Adresse aus dem Bereich 169.254.xxx.yyy.

Die IP-Adresse, die das Gerät beim Starten erhält (per DHCP oder AutoIP), wird beibehalten bis

- zum nächsten Neustart (Aus-/Einschalten oder Neuprogrammierung)
- ein DHCP-Server verfügbar ist
- zum Ablauf des des DHCP-Lease

Beim Starten ist kein DHPC-Server vorhanden

Sollte beim Starten der IPsecure Schnittstelle kein DHCP-Server vorhanden sein, vergibt sich das Gerät selbst eine AutoIP-Adresse. Die Schnittstelle sucht dann zyklisch (drei Telegramme im Abstand von 3 Sekunden, anschließend 20 Sekunden Pause) nach einem DHCP-Server. Sobald wieder ein Server vorhanden ist, wird die vom DHCP-Server zugeteilte Adresse verwendet.

DHCP-Server fällt aus (Gerät hat IP-Adresse bereits von DHCP-Server bezogen)

Jede von einem DHCP-Server zugeteilte IP-Adresse hat eine Gültigkeitsdauer zur Nutzung (Lease Time). Diese Gültigkeitsdauer wird vor Ablauf durch eine Anfrage vom Gerät an den DHCP-Server verlängert. Bekommt das Gerät die Nutzungszeit nicht verlängert, sucht sich das Gerät nach Ablauf der Gültigkeitsdauer eine AutoIP-Adresse.

Feste IP-Adresse

Soll die IP-Adresse der IPsecure Schnittstelle fest zugeordnet sein, so kann in der ETS eine feste IP-Adresse (sowie Subnet-Maske und Standard Gateway) eingestellt werden, siehe Parameterfenster IP-Einstellungen.

Steht kein Standard-Gateway zur Verfügung, muss der Wert auf 0.0.0.0. gesetzt werden.

4.1.2 Überwachung einer IPsecure Schnittstelle KNX

Soll das Gerät durch eine Visualisierung überwacht werden, welche eine Tunneling-Verbindung zu dem Gerät unterhält, so sollte die aktive Tunneling-Verbindung auch zur Überwachung vewendet werden.

Soll das Gerät durch einen Überwachungsbaustein überwacht werden, so sollte die Überwachung auf die Geräteadresse erfolgen, nicht auf eine der Tunneling-Verbindungen.

4.2 Das IP-Tool

4.2.1 Discovery

Die IPsecure Schnittstellen können im Netzwerk mit dem IP-Tool gefunden werden.

Wählen Sie in der Multifunktionsleiste den Modus *Discovery*. Diese Funktion dient zum Auffinden und Anzeigen von Theben IP-Geräten im Netzwerk.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des IP-Tools zu finden.

4.2.2 Firmware Update

Die Firmware des Gerätes sollte immer aktuell gehalten werden. Theben stellt Tools bereit, mit denen der Firmwarestatus des Gerätes geprüft werden kann.

Für ein Firmware Update im non secure-Modus kann das Theben IP-Tool verwendet werden.
Das finden Sie zum kostenlosen Download auf unserer Internetseite.

Im KNX-Secure-Modus kann das Gerät nicht mit dem IP-Tool aktualisiert werden.

Das Firmware Update kann in diesem Fall nur mit der ETS App „Theben Update App" erfolgen, die kostenlos aus dem KNX Online Shop geladen werden kann.

Wichtig
Während des Updatevorgangs muss zusätzlich zum IP-Netzwerk (LAN) auch der KNX-Bus (TP) angeschlossen sein, damit die KNX-Parameter korrekt wiederhergestellt werden können. Andernfalls schlägt der Updatevorgang fehl. Es muss sichergestellt werden, dass während des Updatevorgangs kein Spannungsausfall (KNX oder IP) auftritt, da ansonsten das Gerät zerstört werden kann.

5 Kontakt

Theben AG
Hohenbergstraße 32
72401 Haigerloch
DEUTSCHLAND

Tel.: +49 7474 692-0
Fax: +49 7474 692-150
E-Mail: info@theben.de
Internet: www.theben.de

Hinweis:
Technische Änderungen der Produkte sowie Änderungen im Inhalt dieses Dokuments behalten wir uns jederzeit ohne Vorankündigung vor.
Bei Bestellungen sind die jeweils vereinbarten Beschaffenheiten maßgebend. Die Theben AG übernimmt keinerlei Verantwortung für eventuelle Fehler oder Unvollständigkeiten in diesem Dokument.

6 Open Source-Softwarekomponenten (OSS)

Eine Liste der verwendeten Open Source-Komponenten ist im Internet unter folgendem Link zu finden:

https://www.theben.de/OSS