SIEMENS

N 146/03

IP-Router Secure

Applikationsprogrammbeschreibung

A6V11656895_de--_a
14.03.2019

Building Technologies
Control Products and Systems

Inhaltsverzeichnis

1 Informationen zum IP-Router Secure und zum Applikationsprogramm

Produktfamilie: Systemgerät

Produkttyp: Koppler

Hersteller: Siemens

Name: IP-Router Secure N 146/03

Bestell-Nr.: 5WG1146-1AB03

Applikation: 091A CO IP-Router Secure 0040 01

Systemvoraussetzung:

- mind. ETS 5.7

1.1 Haftungsausschluss Cyber-Sicherheit

Siemens offeriert ein Portfolio von Produkten, Lösungen, Systemen und Dienstleistungen mit Sicherheitsfunktionen, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Im Geschäftsfeld der Gebäudetechnik umfasst dies Systeme für Gebäudeautomation und -leittechnik, Brandschutz, Sicherheitsmanagement und physische Sicherheitssysteme.

Um Anlagen, Systeme, Maschinen und Netzwerke vor Online-Bedrohungen zu schützen, ist es erforderlich, ein ganzheitliches, dem neuesten Stand der Technik entsprechendes Sicherheitskonzept zu implementieren und stets auf dem aktuellen Stand zu halten. Das Portfolio von Siemens bildet nur einen Bestandteil eines solchen Konzeptes.

Sie sind dafür verantwortlich, unbefugten Zugang zu Ihren Anlagen, Systemen, Maschinen und Netzwerken zu verhindern. Diese sollten nur mit einem Netzwerk oder dem Internet verbunden werden, wenn und soweit die Verbindung erforderlich ist und angemessene Sicherheitsvorkehrungen (z. B. Firewalls bzw. Netzwerksegmentierung) vorhanden sind. Darüber hinaus sind die Sicherheitsempfehlungen von Siemens zu beachten. Für nähere Informationen kontaktieren Sie bitte Ihren Ansprechpartner bei Siemens oder besuchen Sie unsere Webseite https://www.siemens.com/global/de/home/unternehmen/themenfelder/zukunft-der-industrie/industrial-security.html.

Zur Verbesserung der Sicherheit wird das Portfolio von Siemens kontinuierlich weiterentwickelt. Siemens empfiehlt dringend, Updates zu verwenden, sobald diese zur Verfügung stehen, und stets die neusten Versionen zu verwenden. Werden Versionen verwendet, die nicht mehr unterstützt werden, oder werden neueste Updates nicht verwendet, kann sich Ihr Risiko bezüglich Online-Bedrohungen erhöhen. Siemens empfiehlt dringend, Sicherheitsempfehlungen zu den neuesten Sicherheitsgefährdungen, Patches und damit verbundenen Maßnahmen zu befolgen, die unter anderem unter https://www.siemens.com/cert/de/cert-security-advisories.htm veröffentlicht werden.

2 Funktion

2.1 Sicherheitsfunktionen des IP-Routers

Der IP-Router unterstützt den Sicherheitsstandard „**KNX IP Secure**“ und bietet u. a. folgende Sicherheitsfunktionen:

- Verschlüsselte Übertragung von KNX-Telegrammen zwischen IP-Routern im IP-Netzwerk
- Verschlüsselte Übertragung von KNX-Telegrammen zwischen IP-Router und PC-Software
- Gesicherter Zugriff nur von authentifizierten Geräten
- Sichere Inbetriebnahme über ETS

Bei der sicheren Inbetriebnahme über ETS, wird das auf dem Gerät aufgedruckte Gerätezertifikat (FDSK = Factory Default Setup Key) eingelesen und genau für dieses Gerät im ETS-Projekt abgespeichert.

Weitere Informationen zu KNX IP Secure können in der Hilfe der ETS-Software sowie unter folgender Internetadresse nachgelesen werden:
https://support.knx.org

Alternativ ist auch die ungesicherte Inbetriebnahme ohne KNX IP Secure möglich. In diesem Fall ist das Gerät ungesichert und verhält sich wie andere KNX-Geräte ohne IP Secure.

2.2 Funktionen des IP-Routers

Der IP-Router ist ein Reiheneinbaugerät zum Einbau in Verteilungen. Das Gerät nutzt den KNXnet/IP-Standard und verbindet KNX-Linien miteinander über Datennetzwerke unter Nutzung des Internetprotokolls (IP). Zugleich ermöglicht dieses Gerät den Buszugriff von einem PC oder anderen Datenverarbeitungsgeräten.

Anschlüsse und Spannungsversorgung

Die Verbindung zum KNX wird über eine Busanschlussklemme hergestellt (schwarz-rote Klemmen). Die Verbindung zum Datennetzwerk (IP über 10 oder 100BaseT (abhängig vom Switch)) erfolgt über eine RJ45-Buchse.

Für den Betrieb benötigt der IP-Router zusätzlich eine Betriebsspannung. Der IP-Router kann diese Betriebsspannung über die Netzwerkleitung aus „Power over Ethernet“ gemäß IEEE 802.3af beziehen. Alternativ kann die Betriebsspannung über den zweiten Klemmenblock (weiß-gelbe Klemmen) aus einer Sicherheitskleinspannungs-Versorgung AC/DC 24 V oder aus einer Busspannungsversorgung (unverdrosselte Spannung, DC 29 V) bezogen werden. Sobald eine Sicherheitskleinspannungs-Versorgung am zweiten Klemmenblock angeschlossen ist, wird die Betriebsspannung aus dieser bezogen.

Fernzugriff

Auch wenn keine direkte Netzwerkverbindung zwischen einem PC und einem IP-Router besteht, kann durch Verwendung der geeigneten Netzinfrastruktur von Ferne auf eine KNX-Installation zugegriffen werden.

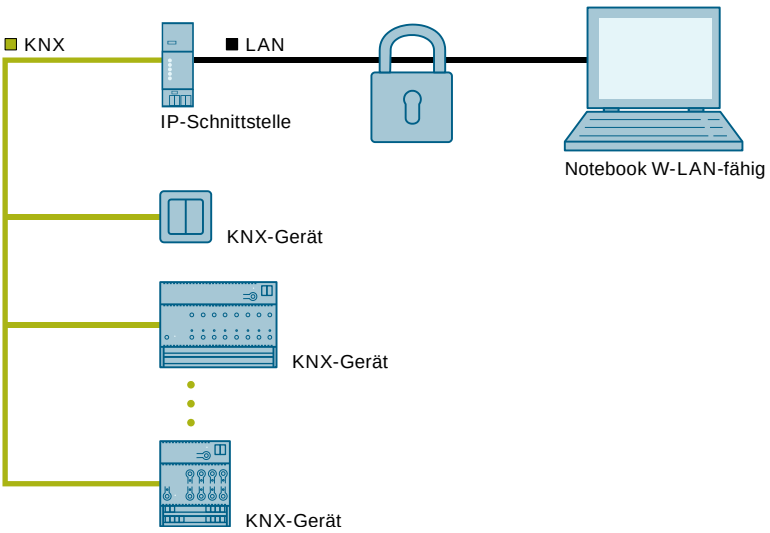

Abb. 1: sicherer Fernzugriff

Weitere Funktionen

Der IP-Router hat folgende Merkmale:

- Einfache Anbindung an übergeordnete Systeme durch Nutzung des Internetprotokolls (IP)
- Gesicherter Zugriff und Datenübertragung über KNXnet/IP Secure
- Direkten Zugriff von jedem Punkt im IP-Netzwerk auf die KNX-Installation (KNXnet/IP-Tunneling)
- Schnelle Kommunikation zwischen KNX-Linien, -Bereichen und -Systemen (KNXnet/IP-Routing)
- Gebäude- und liegenschaftsübergreifende Kommunikation (Vernetzung von Liegenschaften)
- Filtern und Weiterleiten von Telegrammen nach
  - physikalischer Adresse
  - Gruppenadresse
- LED-Anzeigen für
  - Betriebsbereitschaft
  - KNX-Kommunikation
  - IP-Kommunikation
- Einfache Konfiguration mit ETS
- Einfache Anbindung von Visualisierungssystemen und Facility-Management-Systemen
- Slot für SD-Karte (nicht in Verwendung)

2.3 Topologie und Routingfunktion

Der IP-Router Secure kann als Linien- oder Bereichskoppler (KNXnet/IP-Routing) eingesetzt werden.

Dabei werden innerhalb eines Datennetzwerks zwei getrennte KNX-Buslinien datenmäßig miteinander verbunden. Galvanisch bleiben die KNX-Buslinien jedoch getrennt. Dadurch kann jede Buslinie im lokalen Betrieb unabhängig von anderen Linien betrieben werden.

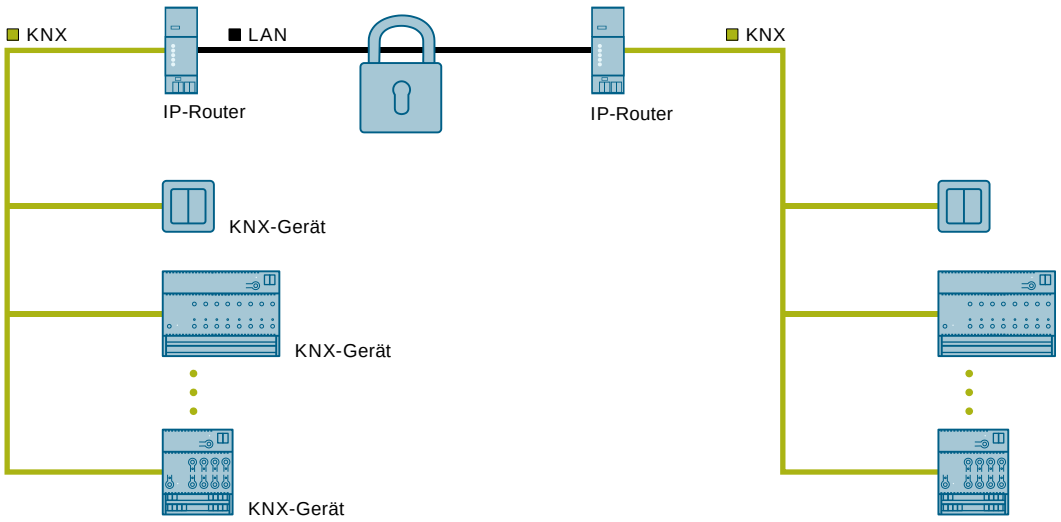

Abb. 2: sicherere Kommunikation im Betrieb

Funktionalitäten bei der Nutzung des IP-Routers als Linien- oder Bereichskoppler

- Schnelle Kommunikation zwischen KNX-Linien
- Möglichkeit der Erweiterung eines bestehenden KNX-Systems über das Gebäude hinaus durch die Nutzung von LAN- und WAN-Verbindungen
- Direkte Weiterleitung von KNX-Daten an jeden Netzwerknutzer
- KNX-Fernkonfiguration von jedem Netzwerkzugangspunkt
- Nutzung in einem neuen oder in einem bestehenden KNX-Netzwerk
- Verringerung der Busbelastung durch Filtertabellen, die bestimmen, welche Bustelegramme von und zur Buslinie weitergeleitet oder gesperrt werden. Die Filtertabelle wird von der ETS-Software bei Parametrierung und Inbetriebnahme des Geräts automatisch erstellt.
- Bei Vergabe der physikalischen Adresse mit Hilfe der ETS wird die Kopplerfunktion automatisch festgelegt (Bereichskoppler: Hauptlinie 1 – 15; Linienkoppler: Linie 1 – 15).

Voraussetzungen für die Nutzung als Linienkoppler

- Netzwerkkomponenten müssen IP Multicasting unterstützen.
- Netzwerk-/LAN-Router müssen so eingestellt sein, dass sie IP-Multicast-Datagramme weiterleiten.
- Die IP-Multicast-Adresse 224.0.23.12 wurde für KNXnet/IP-Routing reserviert.

Bei Einsatz des IP-Routers als Welten-(System-)koppler (0.0.0) und Vollausbau der KNX-Linien inkl. Linienverstärkern können aufgrund des Routingzählers nicht mehr alle Liniensegmente erreicht werden.

Bei der Vergabe der physikalischen Adresse darauf achten, dass IP-Router und Linienkoppler in einer Anlage topologisch korrekte physikalische Adressen erhalten.

Siehe dazu die folgenden Regeln.

Regel für den Einsatz des IP-Routers als Bereichskoppler

Wenn ein IP-Router als Bereichskoppler mit der physikalischen Adresse x.0.0 eingesetzt wird, darf kein weiterer IP-Router topologisch „unterhalb“ dieses IP-Routers, d. h. mit einer physikalischen Adresse x.y.0 (y=1...15), eingesetzt werden.

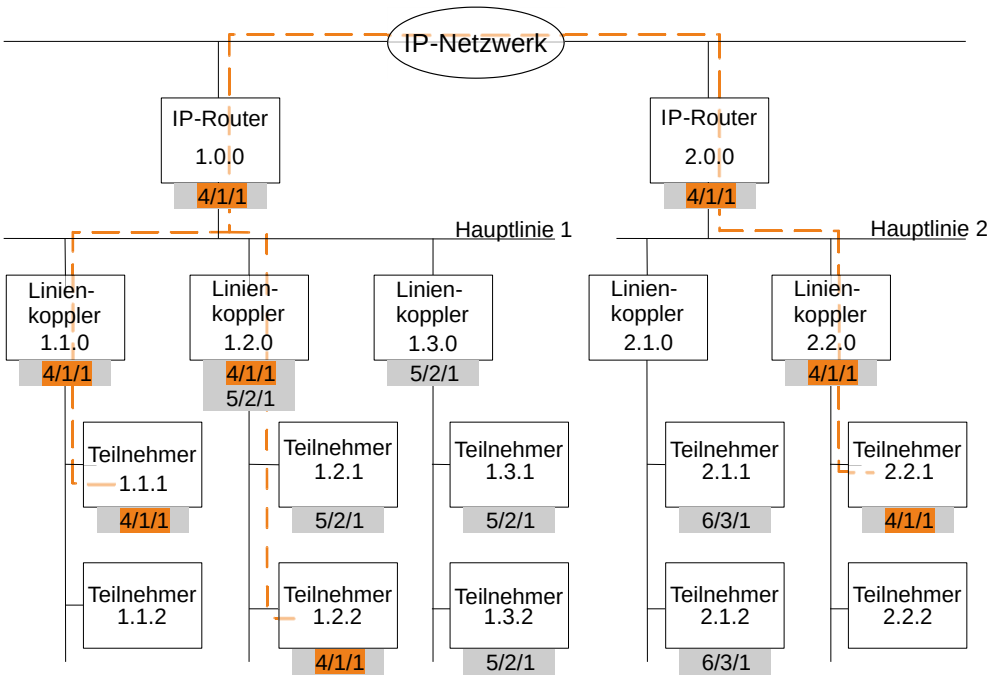

Abb. 3: IP-Router Secure als Bereichskoppler

x/x/x Gruppenadresse

x.x.x Physikalische Adresse (IP-Adresse)

Weg eines Telegramms vom Sender zu den Empfängern (Beispiel)
Telegramme werden nur von Geräten mit der gleichen Gruppenadresse weitergeleitet oder empfangen.

Beispiel: Telegramm wird nur von Geräten mit der Gruppenadresse 4/1/1 weitergeleitet oder empfangen.

Regel für den Einsatz des IP-Routers als Linienkoppler

Wenn ein IP-Router als Linienkoppler (z. B. 1.2.0) eingesetzt wird, darf kein IP-Router mit zugehöriger Bereichskoppleradresse (z. B. 1.0.0) „oberhalb“ im System eingesetzt werden.

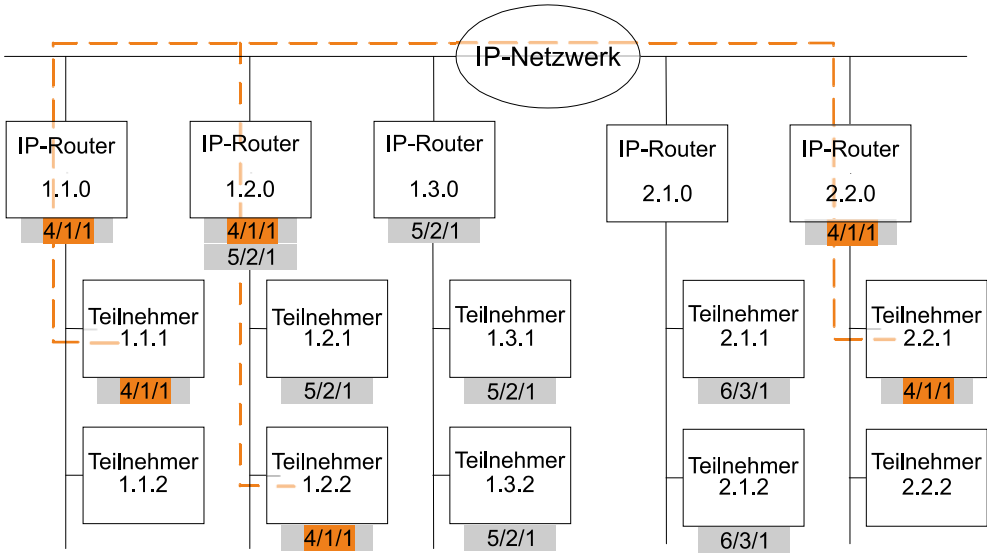

Abb. 4: IP-Router Secure als Linienkoppler

x/x/x Gruppenadresse

x.x.x Physikalische Adresse (IP-Adresse)

Weg eines Telegramms vom Sender zu den Empfängern (Beispiel)
Telegramme werden nur von Geräten mit der gleichen Gruppenadresse weitergeleitet oder empfangen.

Beispiel: Telegramm wird nur von Geräten mit der Gruppenadresse 4/1/1 weitergeleitet oder empfangen.

Regel für den Einsatz des IP-Routers als Bereichs- und Linienkoppler

Der IP-Router kann als Linien- oder Bereichskoppler eingesetzt werden. Die physikalische Adresse hat die Form x.y.0, mit x=1…15 und y=1…15.

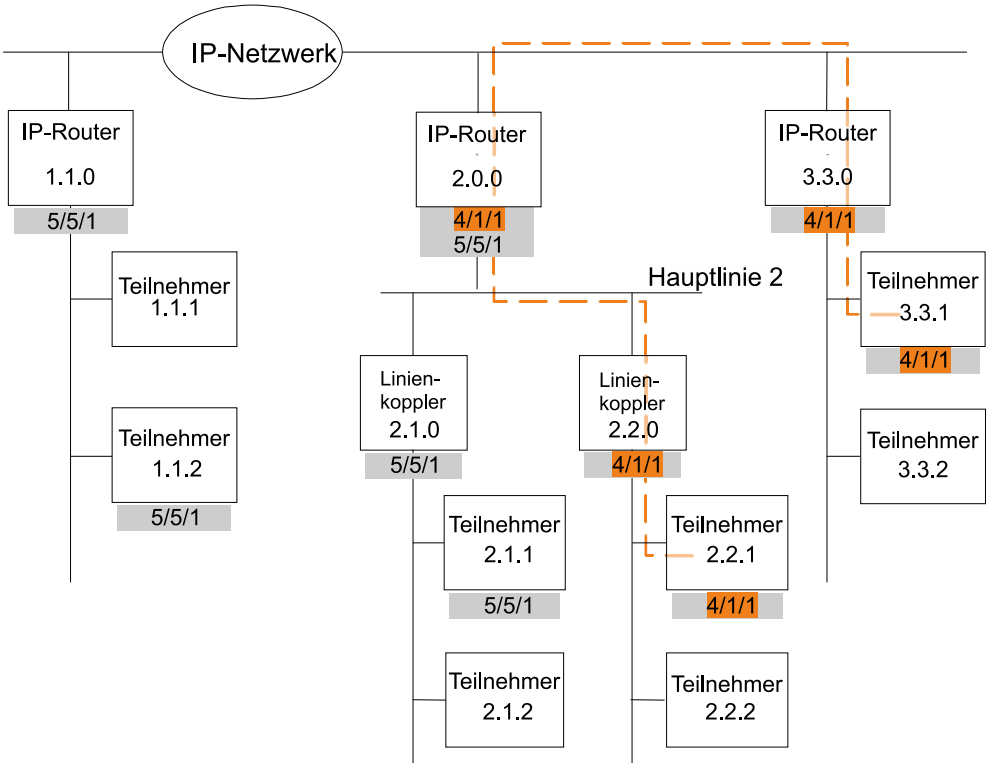

Abb. 5: IP-Router Secure als Bereichs- und Linienkoppler

x/x/x Gruppenadresse

x.x.x Physikalische Adresse (IP-Adresse)

Weg eines Telegramms vom Sender zu den Empfängern (Beispiel)
Telegramme werden nur von Geräten mit der gleichen Gruppenadresse weitergeleitet oder empfangen.

Beispiel: Telegramm wird nur von Geräten mit der Gruppenadresse 4/1/1 weitergeleitet oder empfangen.

2.4 Verhalten bei Busspannungsausfall und Wiederkehr

Wenn der IP-Router einen Ausfall der Busspannung auf der Buslinie erkennt, so wird dies als Fehler gespeichert. Ebenso wird die Busspannungswiederkehr der Buslinie erkannt und der Fehler intern gelöscht. Je nach Konfiguration werden beide Ereignisse an KNXnet/IP gemeldet.

3 Hinweise zur gesicherten Datenübertragung

- Gerät nur im gesicherten Modus betreiben.
- Gerät nur im gesicherten Modus direkt mit dem Internet verbinden.

  Das Gerät befindet sich im gesicherten Modus, wenn das Gerät über die sichere Inbetriebnahme in Betrieb genommen wurde, Secure Tunnelling aktiviert ist und starke sowie unterschiedliche Passwörter verwendet werden.

Mögliche weitere Sicherheitsmaßnahmen sind unter anderem:

- Gerät im ungesicherten Modus nur in einer sicheren Netzwerkumgebung betreiben.
- Für die KNX-Kommunikation ein separates IP-Netzwerk mit eigener Hardware aufsetzen.
- Zugang zum (KNX-)IP-Netzwerk durch Nutzerkennungen und starke Passwörter auf einen berechtigten Personenkreis einschränken.
- Wenn das Gerät im ungesicherten Modus betrieben wird, Fernzugriffe auf das Gerät zusätzlich über eine VPN-Verbindung absichern.

  (Ein virtuelles privates Netzwerk (VPN) baut eine verschlüsselte und autorisierte Verbindung (VPN-Tunnel) von einem entfernten Ort in ein Netzwerk über das Internet auf. Diese VPN-Verbindung ermöglicht eine sichere und gegen Mithören geschützte Kommunikation zwischen einem entfernten Gerät und der KNX-Installation.)
- Wenn WLAN genutzt wird, voreingestellte SSID vom drahtlosen Access Point ändern. Das WLAN mit einem sicheren Verfahren (zurzeit z. B. WPA2) verschlüsseln.
- Netzwerkeinstellungen dokumentieren und dem Gebäudeeigentümer/-betreiber oder dem LAN-Administrator übergeben.
- Verwaltung von Zugangsrechten zu diesem KNXnet/IP-Gerät in einem IP-Netzwerk mit dem zuständigen IP-Netzwerkadministrator abstimmen.

Maßnahmen nach dem Austausch eines Geräts im Netzwerk

Wenn ein IP-Router oder IP-Interface im gesicherten Modus aus einem Netzwerk gestohlen oder aufgrund eines Defekts ausgetauscht wird, muss für alle anderen Geräte im Netzwerk die sichere Inbetriebnahme erneut durchgeführt werden. Hierzu in den Einstellungen des Projekts die Option "Sichere Inbetriebnahme" für jedes Gerät deaktivieren, wieder aktivieren und die neuen Daten erneut in die Geräte laden. (Das Laden der Daten in das Gerät zwischen der Deaktvierung und erneuten Aktivierung ist nicht erforderlich.)

Diese erneute sichere Inbetriebnahme ist erforderlich, da nicht ausgeschlossen werden kann, dass die Schlüssel, die sich in einem geschützten Bereich des Gerätes befinden, ausgelesen werden können. Durch die erneute Inbetriebnahme werden neue Schlüssel generiert, die alten Schlüssel sind hiermit wertlos. Das entwendete Gerät funktioniert nun nicht mehr im Netzwerk.

Weitere Informationen zur KNX-Sicherheit

Weitere Informationen zu KNX-Sicherheit, wie z. B. eine Sicherheitscheckliste, können auf der Internetseite von KNX (http://www.knx.org) im Bereich „KNX Secure“ nachgelesen werden.

4 Gliederung der Einstellmöglichkeiten in ETS

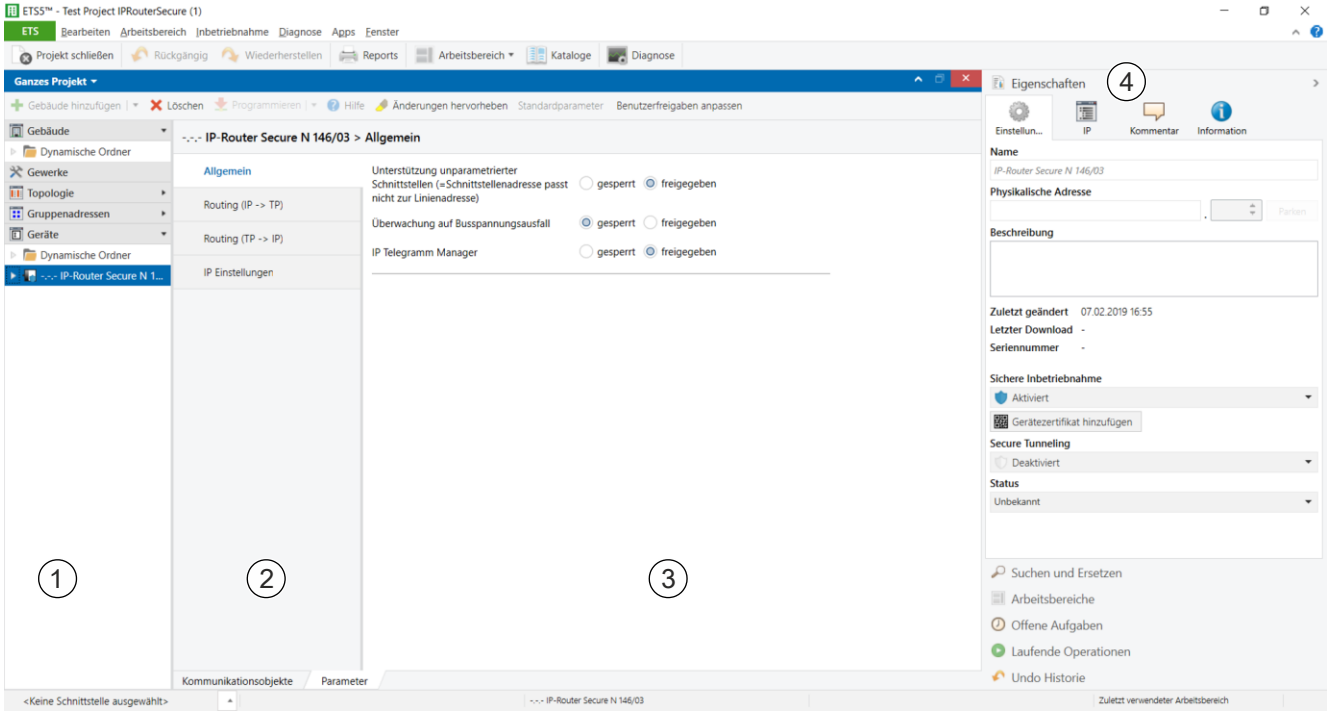

Abb. 6: Übersicht ETS

1 Baumansicht der verschiedenen Abschnitte (z. B. Geräte, Topologie zusätzliche physikalische Adressen)

2 Auflistung der Parameterkarten

3 Parameterbereich. In diesem Bereich werden Parameter eingestellt, freigegeben oder gesperrt.

4 Bereich „Eigenschaften“ (z. B. Konfiguration von IP und Security, zusätzliche physikalische Adressen)

Parameter, die nicht der Standardeinstellung entsprechen, können mit der Schaltfläche ‚Änderungen hervorheben‘ gelb hinterlegt werden.

5 Parameter

5.1 Parameter der Parameterkarte "Allgemein"

Parameter	Einstellungen
Unterstützung unparametrierter Schnittstellen (=Schnittstellenadresse passt nicht zur Linienadresse)	gesperrt freigegeben

Funktion:

Mit diesem Parameter wird eingestellt, ob z. B. Schnittstellen mit topologisch falscher physikalischer Adresse unterstützt werden.

Folgende Einstellungen sind möglich:

- gesperrt:
  Bei der Einstellung ‚gesperrt' werden nicht oder falsch parametrierte Schnittstellen nicht unterstützt.
- freigegeben:
  Bei der Einstellung ‚freigegeben' können z. B. Schnittstellen flexibel zur Parametrierung in mehreren Linien eingesetzt werden, ohne dass die physikalische Adresse jeweils angepasst werden muss.

Parameter	Einstellungen
Überwachung auf Busspannungsausfall	gesperrt freigegeben

Funktion:

Mit diesem Parameter wird eingestellt, ob ein Spannungsausfall und die Spannungswiederkehr der Buslinie über KNXnet/IP gemeldet werden.

Folgende Einstellungen sind möglich:

- gesperrt:
  Informationen über Busspannungsausfall und Busspannungswiederkehr werden nicht weitergegeben.
- freigegeben:
  Informationen über Busspannungsausfall und Busspannungswiederkehr werden über KNXnet/IP weitergegeben.

Parameter	Einstellungen
IP Telegramm Manager	gesperrt freigegeben

Funktion:

Mit dieser Funktion wird der Telegrammpuffer zwischen IP-Routern von Siemens und baugleichen Geräten optimal genutzt und dadurch der Verlust von Telegrammen bei hoher Buslast vermieden.

Hinweis:

Die Funktion muss bei allen verwendeten Geräten verfügbar und eingeschaltet sein. (Bei älteren Geräten von Siemens ist diese Funktion standardmäßig eingeschaltet.)

Bei Mischbetrieb mit anderen Geräten, die diese Funktion nicht haben, diesen Parameter auf „gesperrt" setzen.

Folgende Einstellungen sind möglich:

- gesperrt:
  Die Menge an Telegrammen wird nicht überwacht. Telegramme können verloren gehen.
- freigegeben:
  Die Telegrammrate wird begrenzt. Es wird nur eine bestimmte Menge an Telegrammen versendet.

5.2 Parameter der Parameterkarte "Routing (IP > TP)"

Parameter	Einstellungen
Gruppentelegramme der Hauptgruppen 0 bis 13	alle weiterleiten sperren filtern (normal)

Funktion:

Dieser Parameter bestimmt die Weiterleitung von Telegrammen mit Gruppenadressierung von KNXnet/IP zur Linie.

Folgende Einstellungen sind möglich:

- alle weiterleiten:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme weitergeleitet.
  Diese Einstellung dient zu Testzwecken und muss nach erfolgreichem Test auf die Einstellung „filtern (normal)“ zurückgestellt werden. Ansonsten kommt es zu unnötig höherer Buslast auf allen Linien.
- sperren:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme gesperrt. Diese Einstellung dient z. B. zu Testzwecken während der Inbetriebnahme.
- filtern (normal):
  Bei dieser Einstellung wird vor der Entscheidung, ob das Telegramm an den Bus weitergeleitet werden soll, der Eintrag in der Filtertabelle geprüft. Die von der ETS automatisch erstellte Filtertabelle wird in das Gerät geladen.
  Hinweis: Die Filtertabelle muss manuell nachgeladen werden, sobald Änderungen von linienübergreifenden Gruppenadressen vorgenommen wurden.

Parameter	Einstellungen
Gruppentelegramme der Hauptgruppen 14 bis 31	alle weiterleiten sperren filtern (normal)

Funktion:

Dieser Parameter bestimmt die Weiterleitung von Telegrammen mit Gruppenadressierung von KNXnet/IP zur Linie.

Folgende Einstellungen sind möglich:

- alle weiterleiten:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme weitergeleitet. Diese Einstellung dient zu Testzwecken und muss nach erfolgreichem Test auf die Einstellung „filtern (normal)“ zurückgestellt werden. Ansonsten kommt es zu unnötig höherer Buslast auf allen Linien.
- sperren:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme gesperrt. Diese Einstellung dient z. B. zu Testzwecken während der Inbetriebnahme.
- filtern (normal):
  Bei dieser Einstellung wird vor der Entscheidung, ob das Telegramm an den Bus weitergeleitet werden soll, der Eintrag in der Filtertabelle geprüft. Die von der ETS automatisch erstellte Filtertabelle wird in das Gerät geladen.
  Hinweis: Die Filtertabelle muss manuell nachgeladen werden, sobald Änderungen von linienübergreifenden Gruppenadressen vorgenommen wurden.

Parameter	Einstellungen
Physikalisch adressierte Telegramme	sperren filtern (normal)

Funktion:

Mit diesem Parameter wird die Filterfunktion der physikalisch adressierten Telegramme eingestellt.

Folgende Einstellungen sind möglich:

- sperren:
  Bei dieser Einstellung werden physikalisch adressierte Telegramme nicht weitergeleitet.
  Diese Einstellung muss verwendet werden, wenn KNX-Installationen in unterschiedlichen KNX-Projekten in Betrieb genommen werden und trotzdem die gruppenadressierten Telegramme übertragen werden sollen (Welten- /Systemkoppler).
- filtern (normal):
  Bei dieser Einstellung werden die Telegramme in Abhängigkeit von der physikalischen Adresse des IP-Routers gefiltert.
  Es werden nur Telegramme weitergeleitet, die in der nachfolgenden Linie ihr Ziel haben. Alle anderen Telegramme werden nicht weitergeleitet.

Parameter	Einstellungen
Broadcasttelegramme	weiterleiten sperren

Funktion:

Mit diesem Parameter wird die Filterfunktion der Broadcasttelegramme eingestellt.

Unabhängig von dieser Einstellung werden Broadcasttelegramme vom IP-Router selbst immer akzeptiert.

Folgende Einstellungen sind möglich:

- weiterleiten:
  Bei dieser Einstellung werden die Telegramme in Abhängigkeit von der physikalischen Adresse des IP-Routers weitergeleitet.
  Es werden nur Telegramme weitergeleitet, die in der nachfolgenden Linie ihr Ziel haben. Alle anderen Telegramme werden nicht weitergeleitet.
- sperren:
  Bei dieser Einstellung werden Broadcasttelegramme nicht weitergeleitet.
  Diese Einstellung muss verwendet werden, wenn KNX-Installationen in unterschiedlichen KNX-Projekten in Betrieb genommen werden und trotzdem die gruppenadressierten Telegramme übertragen werden sollen (Welten- /Systemkoppler).

5.3 Parameter der Parameterkarte "Routing (TP > IP)"

Parameter	Einstellungen
Gruppentelegramme der Hauptgruppen 0 bis 13	alle weiterleiten sperren filtern (normal)

Funktion:

Dieser Parameter bestimmt die Weiterleitung von Telegrammen mit Gruppenadressierung von der Linie zu KNXnet/IP.

Folgende Einstellungen sind möglich:

- alle weiterleiten:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme weitergeleitet. Diese Einstellung dient zu Testzwecken und muss nach erfolgreichem Test auf die Einstellung „filtern (normal)“ zurückgestellt werden. Ansonsten kommt es zu unnötig höherer Buslast auf allen Linien.
- sperren:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme gesperrt. Diese Einstellung dient z. B. zu Testzwecken während der Inbetriebnahme.
- filtern (normal):
  Bei dieser Einstellung wird vor der Entscheidung, ob das Telegramm an den Bus weitergeleitet werden soll, der Eintrag in der Filtertabelle geprüft. Die von der ETS automatisch erstellte Filtertabelle wird in das Gerät geladen.
  Hinweis: Die Filtertabelle muss manuell nachgeladen werden, sobald Änderungen von linienübergreifenden Gruppenadressen vorgenommen wurden.

Parameter	Einstellungen
Gruppentelegramme der Hauptgruppen 14 bis 31	alle weiterleiten sperren filtern (normal)

Funktion:

Dieser Parameter bestimmt die Weiterleitung von Telegrammen mit Gruppenadressierung von der Linie zu KNXnet/IP.

Folgende Einstellungen sind möglich:

- alle weiterleiten:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme weitergeleitet. Diese Einstellung dient zu Testzwecken und muss nach erfolgreichem Test auf die Einstellung „filtern (normal)“ zurückgestellt werden. Ansonsten kommt es zu unnötig höherer Buslast auf allen Linien.
- sperren:
  Bei dieser Einstellung werden alle gruppenorientierten Telegramme gesperrt. Diese Einstellung dient z. B. zu Testzwecken während der Inbetriebnahme.
- filtern (normal):
  Bei dieser Einstellung wird vor der Entscheidung, ob das Telegramm an den Bus weitergeleitet werden soll, der Eintrag in der Filtertabelle geprüft. Die von der ETS automatisch erstellte Filtertabelle wird in das Gerät geladen.
  Hinweis: Die Filtertabelle muss manuell nachgeladen werden, sobald Änderungen von linienübergreifenden Gruppenadressen vorgenommen wurden.

Parameter	Einstellungen
Gruppentelegramme bestätigen	immer nur bei Weiterleitung

Funktion:

Mit diesem Parameter kann eingestellt werden, wann Gruppentelegramme vom Router bestätigt werden.

Folgende Einstellungen sind möglich:

- immer:
  Gruppentelegramme werden immer vom Router bestätigt, auch wenn sie nicht auf KNXnet/IP weitergeleitet werden.
- nur bei Weiterleitung:
  Gruppentelegramme werden nur bestätigt, wenn diese auf KNXnet/IP weitergeleitet werden.

Parameter	Einstellungen
Physikalisch adressierte Telegramme	sperren filtern (normal)

Funktion:

Mit diesem Parameter wird die Filterfunktion der physikalisch adressierten Telegramme eingestellt.

Folgende Einstellungen sind möglich:

- sperren:
  Bei dieser Einstellung werden physikalisch adressierte Telegramme nicht weitergeleitet.
  Diese Einstellung muss verwendet werden, wenn KNX-Installationen in unterschiedlichen KNX-Projekten in Betrieb genommen werden und trotzdem die gruppenadressierten Telegramme übertragen werden sollen (Welten-/Systemkoppler).
- filtern (normal):
  Bei dieser Einstellung werden die Telegramme in Abhängigkeit von der physikalischen Adresse des IP-Routers gefiltert.
  Es werden nur Telegramme weitergeleitet, die in der nachfolgenden Linie ihr Ziel haben. Alle anderen Telegramme werden nicht weitergeleitet.

Parameter	Einstellungen
Broadcasttelegramme	weiterleiten sperren

Funktion:

Mit diesem Parameter wird die Filterfunktion der Broadcast-Telegramme eingestellt.

Unabhängig von dieser Einstellung werden Broadcast-Telegramme vom IP-Router selbst immer akzeptiert.

Folgende Einstellungen sind möglich:

- weiterleiten:
  Bei dieser Einstellung werden die Telegramme in Abhängigkeit von der physikalischen Adresse des IP-Routers weitergeleitet.
  Es werden nur Telegramme weitergeleitet, die in der nachfolgenden Linie ihr Ziel haben. Alle anderen Telegramme werden nicht weitergeleitet.
- sperren:
  Bei dieser Einstellung werden Broadcast-Telegramme nicht weitergeleitet
  Diese Einstellung muss verwendet werden, wenn KNX-Installationen in unterschiedlichen KNX-Projekten in Betrieb genommen werden und trotzdem die gruppenadressierten Telegramme übertragen werden sollen (Welten /Systemkoppler).

6 Inbetriebnahme

6.1 Funktion im Auslieferungszustand

Die Funktion „KNXnet/IP-Routing“ ist im Auslieferungszustand bereits aktiv. Wenn zwei IP-Router über ein LAN-Kabel oder mehrere IP-Router über einen Hub/Switch miteinander verbunden werden, werden Bustelegramme über die IP-Router ohne weitere Eingriffe weitergeleitet.

Die Konfigurationsparameter sind im Auslieferungszustand wie folgt eingestellt:

- Physikalische Adresse des IP-Routers: Einstellung: „15.15.0“ (= FF00 hex)
  - Namen und physikalische Adresse des Geräts festlegen [→ 18]
- Gruppentelegramme: Einstellung jeweils: „filtern (normal)“
  - Parameter: Gruppentelegramme der Hauptgruppen 0 bis 13 (IP – TP) [→ 13]
  - Parameter: Gruppentelegramme der Hauptgruppen 0 bis 13 (TP – IP) [→ 15]
  - Parameter: Gruppentelegramme der Hauptgruppen 14 bis 31 (IP – TP) [→ 13]
  - Parameter: Gruppentelegramme der Hauptgruppen 14 bis 31 (TP – IP) [→ 15]
- Bestätigung von weitergeleiteten Telegrammen: Einstellung „nur bei Weiterleitung“
  - Parameter: Gruppentelegramme bestätigen (Bus - IP) [→ 16]
- Unterstützung nicht parametrierter Schnittstellen: Einstellung: „freigegeben“
  - Parameter: Unterstützung nicht parametrierter Schnittstellen [→ 12]
- Filtern von physikalisch adressierten Telegrammen: Einstellung: „filtern (abhängig von Ziel- und Koppleradresse)“
  - Parameter: Physikalisch adressierte Telegramme (IP – TP) [→ 14]
  - Parameter: Physikalisch adressierte Telegramme (TP – IP) [→ 16]
- Weiterleitung von Broadcast-Telegrammen: Einstellung: „weiterleiten“
  - Parameter: Broadcast-Telegramme (IP – TP) [→ 14]
  - Parameter: Broadcast-Telegramme (TP – IP) [→ 16]
- Überwachung der Buslinie auf Spannungsausfall: Einstellung: „gesperrt“
  - Parameter: Überwachung auf Busspannungsausfall [→ 12]
- IP-Adresszuweisung: Einstellung: „IP-Adresse automatisch beziehen“
  - IP-Adresse zuweisen [→ 19]

6.2 Lage QR-Code des Gerätezertifikats

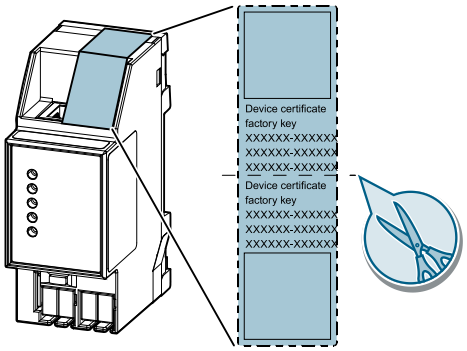

Abb. 7: Gerätezertifikat

Der QR-Code des Gerätezertifikats ist auf dem Gerät aufgeklebt. Der QR-Code ist doppelt vorhanden und kann daher zur einfacheren Inbetriebnahme abgetrennt werden.

6.3 Gerät in Betrieb nehmen

Gerät mit „KNX IP Secure“ in Betrieb nehmen

▷ Ein Projekt ist in ETS geöffnet.

1. Gerät zum Projekt hinzufügen.
   ⇨ Falls das Projekt noch nicht mit einem Passwort geschützt ist, wird das Fenster ‚Projektpasswort setzen‘ angezeigt.
2. Passwort in den Eingabefeldern ‚Neues Passwort‘ und ‚Passwort bestätigen‘ eingeben und mit ‚OK‘ bestätigen.
   ⇨ Das Fenster ‚Gerätezertifikat hinzufügen‘ wird angezeigt.
3. Falls eine Webcam vorhanden ist, Schaltfläche ‚…‘ drücken und den am Gerät aufgeklebten QR-Code einscannen.
4. Falls keine Webcam vorhanden ist oder der QR-Code nicht gelesen werden kann, auf dem Gerät aufgeklebten 6x6-stelligen Zertifikatsschlüssel eingeben.
   ⇨ Bei korrekt eingegebenem Zertifikatsschlüssel erscheint am Ende der Zeile ein grüner Haken. Zusätzlich werden die Seriennummer und der Fabrikschlüssel des Geräts angezeigt.
5. Angezeigte Seriennummer mit der auf dem Gerät aufgeklebten Seriennummer vergleichen.
   ⇨ Falls die Seriennummer nicht übereinstimmt, wurde der Zertifikatsschlüssel eines anderen Geräts eingegeben und die Übertragung von Daten wird später nicht funktionieren.
6. Eingaben mit ‚OK‘ bestätigen.
   ⇨ Das Gerät wurde zum Projekt hinzugefügt. Sicherheitsfunktionen von „KNX IP Secure“ sind automatisch aktiviert.

Gerät ohne „KNX IP Secure“ in Betrieb nehmen

Inbetriebnahme ohne „KNX IP Secure“

Alternativ kann das Gerät auch ohne KNX IP Secure in Betrieb genommen werden. In diesem Fall ist das Gerät ungesichert und verhält sich wie andere KNX-Geräte ohne die Funktion KNX IP Secure.

Zur Inbetriebnahme des Geräts ohne KNX IP Secure Gerät im Abschnitt ‚Topologie‘ oder ‚Geräte‘ markieren und im Bereich ‚Eigenschaften‘ in der Registerkarte ‚Einstellungen‘ die Option ‚Sichere Inbetriebnahme‘ auf ‚Deaktiviert‘ setzen.

6.4 Namen und physikalische Adresse des Geräts festlegen

Ein eindeutiger Name des Geräts hilft dabei, das Gerät in einer KNXnet/IP-Visualisierung oder innerhalb eines Projekts in ETS eindeutig wiederzuerkennen und zu finden.

▷ Das Gerät wurde zum Projekt hinzugefügt.

1. Gerät im Abschnitt ‚Topologie' oder ‚Geräte' auswählen.
2. Im Bereich ‚Eigenschaften' in die Registerkarte ‚Einstellungen' wechseln.
3. Im Eingabefeld ‚Name' einen eindeutigen Namen mit maximal 30 Zeichen für das ausgewählte Gerät eingeben.
4. Im Eingabefeld ‚Physikalische Adresse'e die physikalische Adresse des Geräts eingeben. Die Adresse darf noch nicht vergeben sein.

   ⇨ Die Einstellungen werden automatisch gespeichert.

6.5 IP-Adresse zuweisen

Für Details zur IP-Adresse und weiteren Netzwerkeinstellungen lokalen Netzwerkadministrator kontaktieren.

▷ Das Gerät wurde zum Projekt hinzugefügt.

1. Gerät im Abschnitt ‚Topologie' oder ‚Geräte' auswählen.
2. Im Bereich ‚Eigenschaften' in die Registerkarte ‚IP' wechseln.
3. Einstellungen zur IP-Adresse wie gewünscht vornehmen.

   ⇨ Die Einstellungen werden automatisch gespeichert.

Folgende Einstellungen sind möglich:

- **IP-Adresse automatisch beziehen**
  Bei Auswahl dieser Option wird dem Gerät automatisch eine IP-Adresse zugewiesen. Dies geschieht entweder über einen DHCP-Dienst im Netzwerk oder, falls kein DHCP-Dienst konfiguriert wurde, über das Gerät selbst (AutoIP). Die zur Konfiguration des DHCP-Diensts benötigte MAC-Adresse des Geräts kann unterhalb dieser Einstellmöglichkeit oder direkt am Gerät von einem Aufkleber abgelesen werden.
- **Feste IP-Adresse verwenden**
  Bei Auswahl dieser Option werden weitere Eingabefelder eingeblendet, in denen die gewünschte IP-Adresse für das Gerät sowie die Subnetzmaske und der Standardgateway eingegeben werden können.

6.6 Multicast-Adresse einrichten

Genauso wie bei KNX (Telegramme mit Gruppenadressen) gibt es bei IP die Möglichkeit, eine Nachricht gleichzeitig an mehrere Empfänger zu senden. Diese Form der IP-Kommunikation wird „Multicast" genannt und setzt voraus, dass Sender und Empfänger Mitglied derselben Multicast-Gruppe sind und dieselbe Multicast-Adresse als Zieladresse verwenden. Nachrichten werden also an alle Geräte weitergeleitet, die dieselbe Multicast-Adresse verwenden.

Speziell für KNXnet/IP ist die Multicast-Adresse 224.0.23.12 reserviert.

Für die allgemeine Nutzung in einem Netzwerk können die Multicast-Adressen 224.0.0.0 bis 239.255.255.255 verwendet werden. (Für Byte 1 der IP-Routing-Multicast-Adresse sind nur Werte zwischen 224 und 239 zulässig, da KNXnet/IP-Routing bei anderen Werten nicht funktioniert.)

1. In ETS den Abschnitt ‚Topologie' auswählen.
2. Im Bereich ‚Eigenschaften' in die Registerkarte ‚Einstellungen' wechseln.
3. Im Eingabefeld ‚Multicast Adresse' die gewünschte Multicast-Adresse eingeben.

   ⇨ Die Einstellungen werden automatisch gespeichert.

6.7 Zusätzliche physikalische Adressen einrichten

Für eine stabile Kommunikation des Geräts über KNXnet/IP-Tunneling muss das Gerät für jede Verbindung eine eigene physikalische Adresse verwenden.

Diese zusätzlichen Adressen dürfen nicht mit der physikalischen Adresse des Geräts identisch sein und dürfen auch von keinem anderen Busgerät verwendet werden.

Beim Einfügen des Geräts in ein Projekt in ETS werden automatisch zusätzliche physikalische Adressen für das Gerät angelegt, die bei Bedarf geändert werden können.

Weitere Informationen zur Vergabe und zur Änderung von physikalischen Adressen können in der Hilfe der ETS-Software nachgelesen werden.

Das Zurücksetzen der physikalischen Adressen erfolgt bei der Zurücksetzung des gesamten Geräts in den Auslieferungszustand: Gerät in den Auslieferungszustand zurücksetzen [➞ 23]

7 Hilfe bei Fehlern und Problemen

7.1 Häufige Fragen

Häufige Fragen

Für häufige Fragen zum Produkt und deren Lösung siehe:
https://support.industry.siemens.com/cs/ww/en/ps/faq

7.2 Mögliche Fehler

Fehler	Abhilfe
Gerätezertifikate sind fehlerhaft	Gerätezertifikate überprüfen [→ 22]
Physikalische Adressen wurden mehrfach verwendet	Physikalische Adressen prüfen und/oder zurücksetzen und neu vergeben Zusätzliche physikalische Adressen einrichten [→ 20] Fehleranalyse mit Hilfe von ETS [→ 21]

Tab. 1:

7.3 Fehleranalyse mit Hilfe von ETS

Zur Fehleranalyse in ETS gibt es u. a. folgende Möglichkeiten:

Bereich ‚Diagnose'

In diesem Bereich können u. a. physikalische Adressen, der Gruppenmonitor und der Busmonitor überprüft werden.

Bereich ‚Reports':

In diesem Bereich können Details zu verschiedenen Bereichen des Projekts als Datei exportiert oder direkt gedruckt werden.

Für weitere Informationen zu ETS siehe Online-Hilfe der ETS-Software.

7.4 Gerätezertifikate überprüfen

1. Schaltfläche ‚ETS' in der Menüleiste drücken.
2. Projekt aus der Liste auswählen.
   ⇨ Auf der rechten Seite werden Details zum Projekt angezeigt.
3. Registerkarte ‚Sicherheit' auswählen.
   ⇨ Eine Liste der zum Projekt gehörenden Gerätezertifikate wird angezeigt.

8 Gerät in den Auslieferungszustand zurücksetzen

!	*HINWEIS*
	Datenverlust durch Zurücksetzen des Geräts! Beim Zurücksetzen des Geräts werden alle eingegebenen Parameter und vorgenommenen Einstellungen gelöscht. • Sicherstellen, dass das Gerät wirklich zurückgesetzt werden soll.

Gerät in den Auslieferungszustand zurücksetzen

- Lerntaste drücken, bis die Programmier-LED anfängt schnell zu blinken (mindestens 20 Sekunden).

⇨ Die Programmier-LED blinkt für 8 Sekunden.

⇨ Das Gerät wurde in den Auslieferungszustand zurückgesetzt. Alle Parametereinstellungen wurden gelöscht.

Stichwortverzeichnis

Herausgegeben von
Siemens Schweiz AG
Building Technologies Division
International Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies

Dokument-ID: A6V11656895_de--_a
Ausgabe: 14.03.2019