# IPR/S 3.5.1: Sichere Inbetriebnahme
## Drei Begriffe zum Thema KNX IP-Secure

| GPG BUILDING AUTOMATION | | | | | |
|---|---|---|---|---|---|
| Dok.-Typ: | Schritt-für-Schritt Anleitung | Dok.-Nr. | 9AKK107492A6838 | Revision: | A |
| Abteilung: | BA Engineering | Autor: | Engineering Team BA/DESTO | | |
| System: | i-bus KNX | Produkt: | IPR/S 3.5.1 | | |
| Seite: | 1/7 | Datum: | 07. Aug. 2019 | | |


### Haftungsausschluss:

Dieses Dokument dient zur technischen Information und soll Anregungen zum Einsatz geben.

Es ersetzt nicht die technischen Informationen zur Projektierung, Montage und Inbetriebnahme des Produkts. Technische Änderungen und Irrtümer sind vorbehalten.

Trotz Überprüfung des Inhalts dieser Druckschrift auf Übereinstimmung mit der Hard- und Software können Abweichungen nicht vollkommen ausgeschlossen werden. Daher können wir hierfür keine Gewähr übernehmen. Notwendige Korrekturen fließen in neue Versionen des Dokuments ein.

## Einführung

Bei den neuen ABB i-bus® IP-Router Secure IPR/S 3.5.1 Geräten unterscheidet man zwischen drei verschiedenen Secure Begriffen. Sichere Inbetriebnahme, Secure Tunneling und Backbone IP-Secure. Diese werden, bei der Inbetriebnahme des Routers, jedem Systemintegrator begegnen.

## Ziel des Dokuments

- Die drei Begriffe und insbesondere das Handling innerhalb der ETS zu den Einstellungen einfach darstellen und erklären.
- Praxisnahe Tipps und Tricks zur Inbetriebnahme aus Sicht des technischen Supports vermitteln.

## Inhalt

### 1. Sichere Inbetriebnahme

Der IPR/S 3.5.1 unterstützt das KNXnet/IP Security Protokoll und kann daher auch sicher in Betrieb genommen werden, siehe Abb. 1. Nach dem Einfügen des Gerätes aus dem Produktkatalog in die ETS ist der IPR/S 3.5.1 standardmäßig in der aktivierten sicheren Inbetriebnahme. Kopiert man jedoch z.B. ein Gerät mit deaktivierter Einstellung, wird diese Eigenschaft mit kopiert.

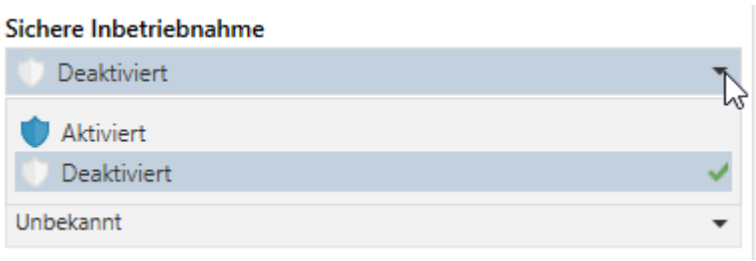


Abb. 1 Sichere Inbetriebnahme Einstellung

Wenn „Sichere Inbetriebnahme“ aktiviert ist, wird das Gerät mit verschlüsselten Telegrammen in Betrieb genommen. Ein Mitlesen des Telegrammverkehrs auf dem Bus lässt keine Rückschlüsse zur Geräteparametereinstellung zu. Mit dieser Einstellung ist erst einmal gewährleistet, dass der IPR/S 3.5.1 in der Inbetriebnahmephase gesichert mit der ETS kommuniziert (FDSK und Seriennummer → erster Download).

**Hinweis:** Es ist ratsam, die Reihenfolge der Inbetriebnahme beim Einsatz von IPR/S 3.5.1 zu beachten. Es gilt, dass immer von „Nah“ nach „Fern“ am sinnvollsten ist, d.h. der Schnittstellen nahe IPR/S 3.5.1 zuerst. Der Grund ist der Folgende: Setzt man den fernen IP-Router zuerst auf Secure ist dieser Router und alle dahinter befindlichen Geräte nicht mehr erreichbar. Ursache dafür ist der **lokale** IP-Router, welcher noch keinen Backbone Key verwendet und damit den **entfernten** IP-Router per Multicast Routing nicht mehr erreichen kann!
Das Gleiche gilt auch für den Wechsel der Multicast Routing Adresse!

## 2. Secure Tunneling

Hat man die „Sichere Inbetriebnahme“ aktiviert, erscheint zusätzlich in dem ETS Eigenschaftenfenster des IP-Router Secure das „Secure Tunneling“ Feld (siehe Abb. 2). Es dient z.B. zur sicheren Kommunikation zwischen einer Visualisierung und der Router.

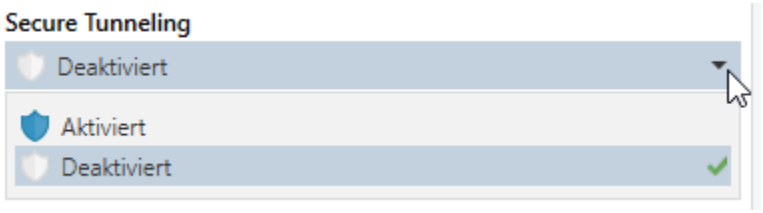


Abb. 2 Secure Tunneling Einstellung

Aktiviert man das „Secure Tunneling“ bekommen alle verfügbaren Tunneling Server (ob geparkt oder nicht) ein eigenes, von der ETS erstelltes Passwort (siehe Abb. 3). Ändern kann man das Passwort im Eigenschaftenfenster der jeweiligen Tunneling Schnittstelle.

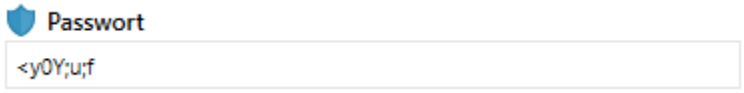


Abb. 3 Passwort für Tunneling Schnittstelle

**Wichtig:** Jedes Passwort kann individuell, ohne Einschränkung, angepasst werden. Es können auch fünf gleiche Passwörter für fünf Tunneling Schnittstellen vergeben werden. Zu sehen in der Report Funktion der ETS unter dem Reiter „Projekt-Sicherheit“ (siehe Abb. 4 und 5).

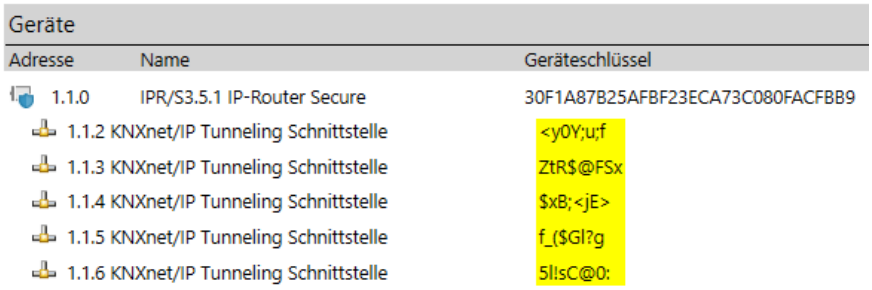


Abb. 4 Tunneling Passwörter ETS Variation

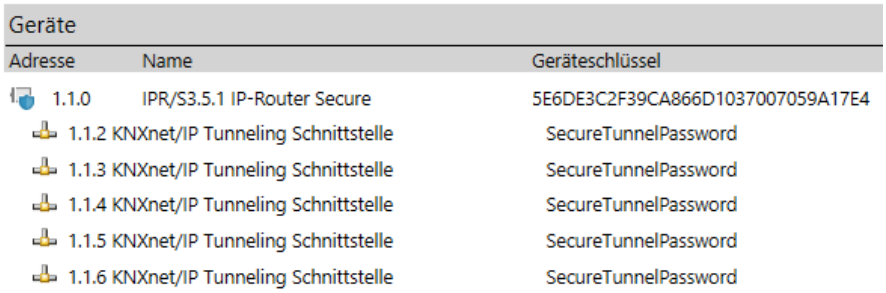


Abb. 5 Angepasste Tunneling Passwörter

## 3. Backbone IP-Secure

Der Backbone IP ist, bei einer Topologie mit klassischen IP-Routern, immer ungesichert und sieht in der ETS wie folgt aus (siehe Abb. 6). Zu finden unter der Schaltfläche „Topologie Backbone“ im Topologie Fenster der ETS. Hier einfach mit einem Linksklick draufklicken.

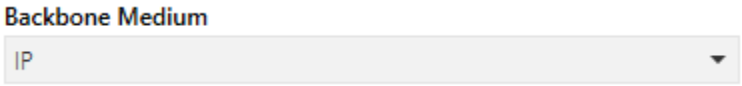


Abb. 6 Backbone Medium ohne Secure

Sind jetzt, alle im Projekt befindlichen IPR/S 3.5.1 auf den KNX Secure Modus eingestellt, ist automatisch der Backbone IP auch Secure (siehe Abb. 7).

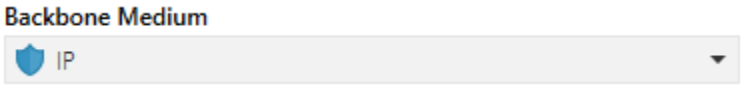


Abb. 7 Backbone Medium mit Secure

Im Hintergrund wird für alle IP-Router Secure ein gemeinsamer Sicherheitsschlüssel (Backbone Key) vergeben, der jedoch in der ETS Oberfläche nicht sofort sichtbar ist. Er ist in der Reportfunktion der ETS unter „Projekt-Sicherheit“ zu finden, siehe Abb.8.


Abb. 8 Projekt-Sicherheit Report

Dieser Schlüssel dient zur sicheren Multicast Kommunikation. Der Schlüssel wird dann bei der Inbetriebnahme des Routers in das Gerät geladen. Es können also erst alle Geräte miteinander über einen verschlüsselten Backbone kommunizieren, wenn alle am Backbone beteiligten Geräte fertig in Betrieb genommen sind.

## 4. Ausnahmen mit IPR/S 3.1.1 und IPR/S 3.5.1

Zunächst einmal ist es wissenswert, dass die standardmäßige Einstellung eines ETS Projektes sicherheitstechnisch auf dem Modus „Automatisch“ ist (siehe Abb. 9). Dieser Modus hat auf die Gerätesicherheit der IP-Router Secure erhebliche Auswirkungen. Das heißt, dass beim Einfügen eines IP-Router Secure zunächst kein Unterschied zu einem normalen IP-Router (IPR/S 3.1.1) zu sehen sein wird. Denn dieser wird auch standardmäßig in der unsicheren Einstellung dem ETS Projekt hinzugefügt.

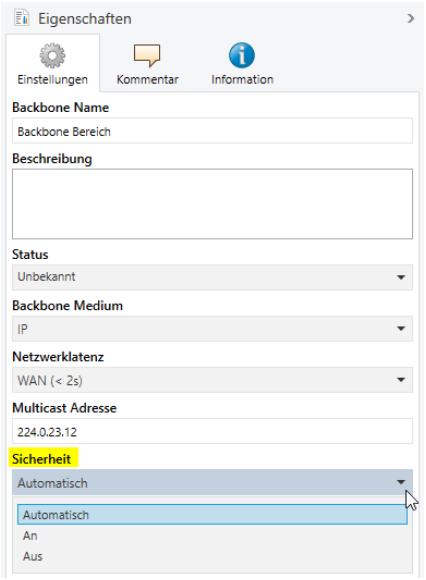


Abb. 9 Sicherheitseinstellung Backbone Bereich

In der Einstellung „An“ muss beim erstmaligen Einfügen eines IPR/S 3.5.1 bzw. KNX IP-Secure Gerätes - in ein leeres Projekt - ein Projektpasswort vergeben werden. Weiterhin kann dann z.B. kein IPR/S 3.1.1 mehr dem ETS Projekt hinzugefügt werden, da er kein IP-Secure Gerät ist (siehe Abb. 10).

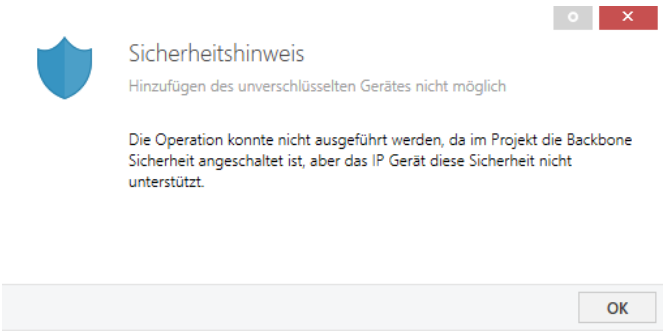


Abb. 10 Sicherheitseinstellung "An"

In der Einstellung „Aus“ ist genau das Gegenteil der Fall. Geräte werden, trotz vorhandener IP-Secure Technik, nicht sicher betrieben. Ein Sonderfall wäre ein Bestandsprojekt mit gemischten Geräten (IPR/S 3.5.1 und IPR/S 3.1.1), dann wäre beim Umstellen auf „An“ folgende Meldung in der ETS sichtbar (siehe Abb. 11).

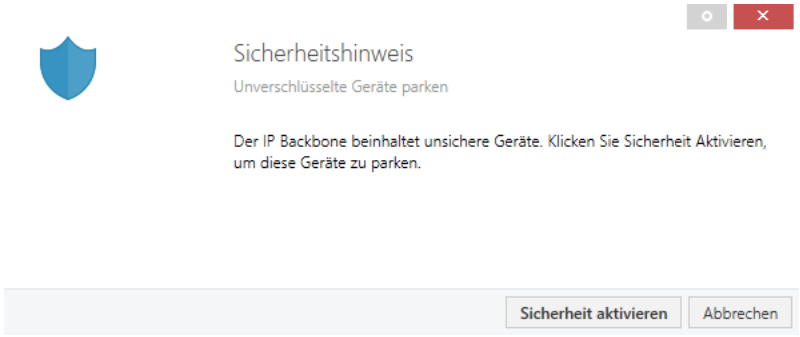


Abb. 11 Sicherheitseinstellung Wechsel

Ein weiteres Beispiel wäre ein Bestandsprojekt mit einem oder mehreren IPR/S 3.5.1 (Secure Modus). Ändert man jetzt die Einstellung von „Automatisch“ auf „Aus“ wird folgende Meldung erscheinen und der IP Backbone wird die sichere Einstellung verlieren, d.h. das blaue Schild wird in der ETS nicht mehr sichtbar sein (Abb. 6)

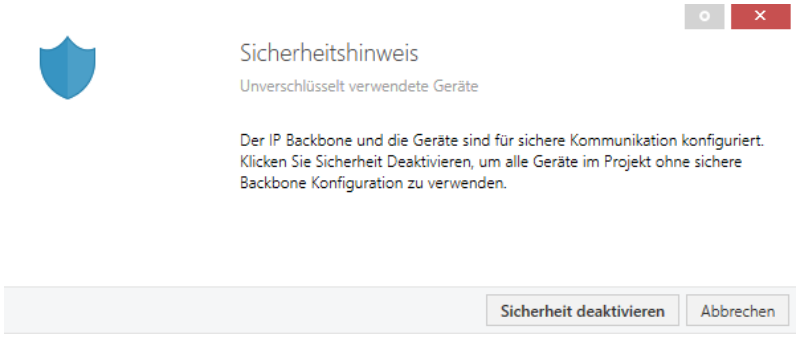


Abb. 12 Wechsel "Automatisch" zu "Aus"

Eine letzte Ausnahme ist folgende Konstellation: IPR/S 3.5.1 (Secure Modus) und sicherer Backbone. Beim Einfügen eines IPR/S 3.1.1 in das Projekt wird bei der Sicherheitseinstellung „Automatisch“ folgende Meldung erscheinen. Auch hier ist der Backbone danach nicht mehr sicher.


Abb. 13 Import IPR/S 3.1.1

## Verweise auf andere Dokumente

- FAQ Home and Building Automation
- Engineering Guide Database
- Video: IP-Router Secure Inbetriebnahme