

DU KOMMST HIER NICHT REIN - wie verschliessen Sie Ihre KNX-Installation?

KNX Guard - der Sicherheitsbaustein

Stellen Sie sich bitte folgende Situation vor: Ein Hotelgast betritt sein Zimmer, legt sein Gepäck ab, packt sein Notebook aus, zieht die Tasterabdeckung ab und ist im Handumdrehen auf Ihrer KNX-Installation. Eine Umparametrierung Ihres Systems ist für eine KNX-geübte Person nun problemlos möglich – ist das in Ihrem Sinne? Wahrscheinlich nicht!



Um genau dies zu verhindern, entwickelte die Firma b+b Automations- und Steuerungstechnik GmbH den KNX-Guard. Der KNX-Guard schützt Ihre KNX-Installation vor Umprogrammierung und vor dem Eindringen Unbefugter. Er belegt dabei keine physikalische Adresse und ist in der ETS nicht auffindbar.

Um einen Busteilnehmer zu parametrieren, wird eine Punkt-zu-Punkt-Verbindung hergestellt über physikalische Telegramme. Der Teilnehmer wird „geöffnet“ und ist in Ihrer Installation ohne KNX-Guard frei zu programmieren. Exakt dieser Vorgang wird durch den KNX-Guard verhindert. Die Kommunikation über physikalische Telegramme ist nun nicht mehr möglich. Geräteüberwachungen auf Gruppenadressebene sind selbstverständlich weiterhin realisierbar. Um eine 100%ige Absicherung zu erzielen, sollte ein KNX-Guard in jeder Linie installiert sein, da ein auf dem „Backbone“ installierter KNX-Guard nichts von einem Zugriffsversuch auf einer untergeordneten Linie mitbekommt.

Auf Wunsch kann bei „Anschlagen“ des KNX-Guard eine Alarmgruppenadresse angesprochen werden, sobald der KNX-Guard einen unerlaubten Zugriff abwehrt. Mittels eines übergeordneten „Leitsystems“ können somit Zugriffsversuche visualisiert und ausgewertet werden.

Alle 3 KNX-Guard Varianten verfügen außerdem über eine ACK-Baustein-Funktionalität. Somit wird mit dem gleichen Baustein zusätzlich noch die Buslast reduziert, da unnötige Telegrammwiederholungen verhindert werden. Die Sicherheit und Funktion des KNX-Busses werden dadurch nicht beeinträchtigt. Gestörte Telegramme werden weiterhin wiederholt.

Folgende KNX-Guard Typen sind verfügbar:

KNX-Guard „Höchste Sicherheit“: Schreib- und Lesezugriffe auf physikalischer Telegrammebene sind nur möglich, wenn der KNX-Guard aus der Hardware-Installation entfernt wird

KNX-Guard „Hohe Sicherheit“: Geräteüberwachung (Lesezugriff) ist auf physikalischer Telegrammebene weiterhin möglich. Schreibzugriffe werden geblockt und sind möglich bei Entfernen des KNX-Guard aus der Installation

KNX-Guard „benutzerdefinierte Sicherheit“: Dieser Typ wird über den Bus mittels des EIBDoktors parametriert/aktiviert/deaktiviert. Hierzu wird über die KNX-Broadcastadresse 15/7/255 mit RSA-Verschlüsselung kommuniziert. Mitgeloggte Telegramme sind nicht reproduzierbar aufgrund des falschen (verschlüsselten) Zeitstempels. Zusätzlich wird der Zugriff über die Verifizierung der Seriennummer und die Eingabe eines PINs gesichert.

Einsatzgebiete:

Sicherung von EIB-Installationen gegen Manipulation

Vorteile:

Sichert die EIB-Installation gegen Umparametrierung
Sichert die EIB-Installation gegen Auslesen
Belegt keine physikalische Adresse

Info: www.bb-steuerungstechnik.de

Vefasser: Alexander Beck