

KNXGuard – The security element

KEEPING INTRUDERS OUT – Locking your KNX system!

Imagine the following situation: A guest in a hotel enters his room, puts his luggage away, opens his laptop - and enters your KNX installation system by pressing a few keys. For any person that has ever worked with KNX, changing the parameter settings of your system is a simple task. Are you protected against such interference? – Probably not.

To prevent such incidents, b+b Automations- und Steuerungstechnik GmbH has developed the KNXGuard.

It protects your KNX installation against attacks from unauthorised persons and against inadvertent or intentional reprogramming. As it does not occupy a physical address, the guard cannot be located in the ETS.



In order to parameterise a bus subscriber in an unprotected system, a point-to-point connection is established by means of physical telegrams. The subscriber is thus "opened" and can be reprogrammed without any restrictions. With the KNXGuard, this type of access is prevented.

As a result, communication by means of physical telegrams is not possible. Device monitoring at group address level remains however available without restrictions. To achieve 100% protection, each line should be equipped with a KNXGuard, as a KNXGuard installed in the backbone cannot prevent unauthorised access to a line at a lower level.

On request, the KNXGuard can be configured to generate a signal to an alarm group address as soon as an unauthorised attempt to access the system is detected.

Such attempts can be visualised and evaluated by means of a superimposed control system.

All 3 KNXGuard models are equipped with an ACK component functionality. The same component thus helps reduce the bus load, as no unnecessary repeat telegrams are sent. The availability and functionality of the KNX bus is however not in any way impaired, and corrupted telegrams are still repeated.

Available KNXGuard models:

KNXGuard "highest security": Read and write access to the physical telegram level is only possible after the KNXGuard has been removed from the hardware installation.

KNXGuard "high security": This solution permits read access (device monitoring) at the physical telegram level. Write access is however only possible after the KNXGuard has been removed from the hardware installation.

KNXGuard "user specific": This model can be parameterised/ activated/deactivated via the bus with the EIBDoctor. For this purpose, the system communicates with RSA encryption via the KNX broadcast address 15/7/255. Logged telegrams cannot be reproduced, as they contain an incorrect (encrypted) time stamp. Access is made safe by verification of the serial number and a PIN.

Applications:

Protection of EIB installations against manipulation

Benefits:

Protects the EIB installation against reconfiguration

Protects the EIB installation against reading

No physical address needed

Info: www.bb-steuerungstechnik.de

Alexander Beck