KNXGuard

The invisible guardian for your EIB installation.

Highlights

- Protects your EIB system from unwanted programming access
- Alarming
- Can be used as an ACK device
- No physical address needed

The different KNXGuard types:

To program a bus device, a point-to-point connection has to get established (physical telegrams), to „open" the device and send the physical programming telegrams.

KNXGuard type "Highest security"
The „Highest security" KNXGuard will prevent any physical telegrams on the EIB. That way it is impossible to change anything in any device.

KNXGuard type "High security"
Some physical telegrams will be allowed on the bus: the reading telegrams. Therefore devices can get read or polled, but still no physical write-telegrams are possible.

KNXGuard type "User defined"
It is having the same functionality as the „High security" device, but you can activate/deactive this type of KNXGuard by sending special telegrams (using the EIBDoktor). The telegrams will be send to the broadcast address 15/7/255, inside the telegram is the serial number of the KNXGuard and a special security code, using an RSA algorithm: even if somebody else is able to protocol the telegrams to deactivate the KNXGuard, sending them later will be useless, since the telegrams are only correct at a special time. Trying to send the deactivation telegram on a later time will have no effect at all.

Requirements for all KNXGuard devices:

You have to install an KNXGuard into every line you want to protect: security on the „backbone" will not grant security in lower lines most times.

Alarming: You can define an „Alarming group address", the KNXGuard will send a telegram to this address each time somebody is trying to do an illegal access. This telegram can be used to display a warning inside a visualization software, for example.

ACK functionality: The KNXGuard also acts as an „ACK device", which means that it will acknowledge all groupaddress-telegrams, and prevents unneccessary busload this way. This will not affect the function of the EIB, damaged telegrams will still get repeated.

No physical address: The KNXGuard acts as an „invisible" device, it will not get used inside the ETS project. The ETS is also not able to detect the KNXGuard. Therefore the KNXGuard does not need a physical address.

b+b Automations- und Steuerungstechnik GmbH
Klingenweg 17 · 64385 Reichelsheim · Tel. 0(049) 6164/912057 · Fax 0(049) 6164/912058
www.bb-steuerungstechnik.de · E-mail: info@bb-steuerungstechnik.de