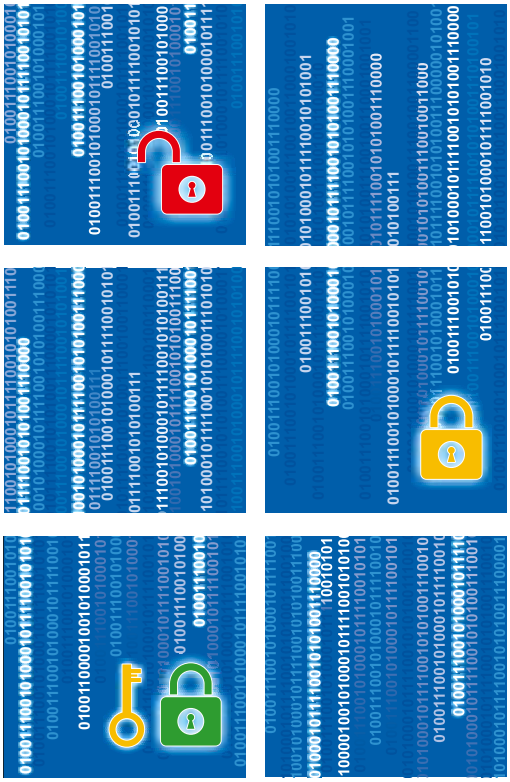


KNX Security Checklist

Checklist for increased security in KNX installations

1 Were the following measures taken into account during installation?

- [ ] Are devices and applications fixed mounted? Is it ensured that devices are properly protected against dismounting (e. g. use of anti-theft protection measures)?
- [ ] Is it ensured that unauthorized persons have limited access to distribution boards with mounted KNX installations (e. g. always locked or located in locked rooms)?
- [ ] Is it difficult to access devices in external areas (e. g. mounted at a sufficient height)?
- [ ] In case the KNX installation can be operated from areas in buildings that are public and not surveilled, did you contemplate the use of binary inputs (mounted in distribution boards) or push button interfaces?

2 Is Twisted Pair used as communication medium?

- [ ] Is the cable anywhere in- or outside the home or the building protected against unauthorized access?
- [ ] In case the twisted pair cable is used in areas requiring extra protection measures, have you taken the measures as given in item 6?

3 Is Powerline used as communication medium?

- [ ] Have band stop filters been installed?
- [ ] If Powerline is also used outside the building, have you taken the same measures for the media coupler as given in item 6?

4 Is IP used as communication medium?

- [ ] Have the network settings been documented and handed over to the home owner or the LAN administrator?
- [ ] Have switches and routers been set in such a way that only known MAC addresses are able to access the communication medium?
- [ ] Is a separate LAN or WLAN network with own hardware used for KNX communication?
- [ ] Is access to the (KNX) IP networks limited to authorized persons via appropriate user names and strong passwords?
- [ ] For KNX IP Multicast communication another IP address as the default address should be used (normally 224.0.23.12). Was this IP multicast address changed?
- [ ] Was the default SSID of the wireless access point changed? Was the periodic transmission of the SSID deactivated?
- [ ] Have ports of routers for KNX been closed towards the internet and was the default gateway of the used KNXnet/IP router set to 0? Was the (W)LAN installation protected by an appropriate firewall? If internet access to a KNX installation is needed, check the possibility to implement:
  1. Establishing a VPN connection to the Internet Router
  2. Use of manufacturer specific KNX Object Servers

5 Is Radio Frequency used as communication medium?

- [ ] Have you taken the same measures for the media coupler as given in item 6?
- [ ] Does each RF domain have a different domain address?

6 Have you used couplers in the installation?

- [ ] Were individual addresses of devices assigned according to their place in the topology?
- [ ] Do you prevent via the setting of appropriate parameters in the couplers that incorrect source addresses are not forwarded outside the line?
- [ ] Do you block Point-to-Point and Broadcast communication across couplers?
- [ ] Have the filter tables been loaded correctly and have settings been made in such a way that filter tables are taken into account by the couplers?
- [ ] Have you considered the measures as given under item 7 for the couplers?

7 Have devices been locked against re-configuration?

- [ ] If not, enter a BCU key[1] in the ETS Project.

8 Do you use KNX Secure[2] devices?

- [ ] For group communication that needs to be secured, use the foreseen authentication and encryption mechanisms of the device.

9 Do you suspect unauthorized access to the bus?

- [ ] Record telegram traffic and analyse it.
- [ ] Read the PID_Device_Control[3] from devices and check whether devices are sending using the same Individual Address.
- [ ] Read the PID_Download_Counter[3] from devices and check whether the device was downloaded again after your configuration.

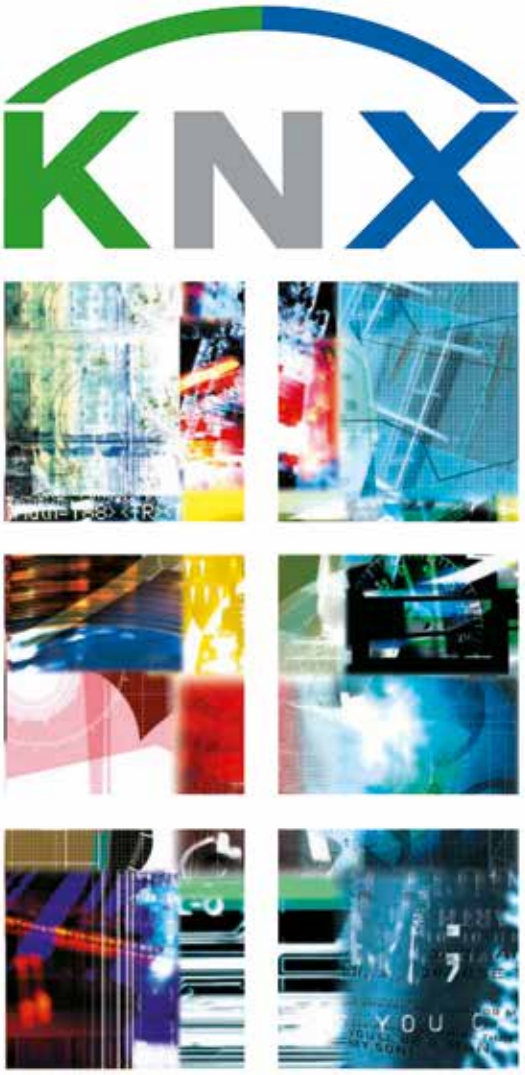
10 Coupling of KNX to security systems?

- [ ] When KNX is coupled to security installations, was this realized in any of the following ways?
  1. Via KNX devices or gateways certified by national loss insurers?
  2. Via potential free contacts (binary inputs, push button interfaces, ...)?
  3. Via appropriate interfaces (RS232, ...) or gateways: was it ensured that KNX communication is unable to trigger security relevant functions in the security part of the installation?

1) Not all devices can be protected against re-configuration – contact the relevant manufacturer

2) Available from ETS 5.5 onwards

3) Is not supported in all devices



www.knx.org