KNX – A Secure Standard
KNX – the worldwide standard

You can rely on KNX if you want to live and work smart. This bus system is the global uniform standard for fitting private and commercial buildings with future-proof building system technology. The unique KNX technology enables central and individual linking and control of the house and building automation components. As a founding member of the KNX Association, JUNG has supported this highly intelligent technology from the beginning.

The most intelligent worldwide standard for modern building that enables investors and owners, as well as planners, architects and electrical installers, to have long-term security. From the easy to use control elements to complex systems, the JUNG KNX components provide comprehensive, future-proof solutions for control, visual display and organisation of building system technology. Areas such as lighting, shade, heating and air conditioning, surveillance, security and multimedia are completely covered here.
The advantages of KNX at a glance

FOR USERS
- A large selection of products
- Great convenience, high operational reliability
- Coordinated interlinking of the devices and functions
- Multifunctional use of multiple devices
- A modular, scalable system
- Easy to upgrade or adapt for changing needs
- Independence from individual manufacturers
- Increased value of the building

FOR INSTALLERS
- Easier, faster device mounting and cabling
- Quick connection technology that covers all manufacturers
- High quality and reliability of products
- Commissioning using manufacturer-independent software (ETS)
- Speed and flexibility for expansions and modifications
- Remote access for maintenance and diagnostics
- 412 training centres worldwide

FOR DESIGNERS
- Can be used in any type of building
- With the KNX standard, more than 9,000 devices from more than 412 manufacturers from 41 countries can communicate with each other.
- Constant expansion of functions and applications
- Commissioning using manufacturer-independent standard software (ETS)
- Easy realisation of orders, operations, surveillances and displays
- Connection possible to many other systems, protocols and standards
- Easy logic connections between functions and devices
- Certified and trained installers

Vitra Design Museum
JUNG KNX technology stands for intelligent networking and operation of building functions in aesthetic design. Aspects such as convenient operation, security and energy efficiency are effortlessly met – particularly in a demanding museum construction. Technology itself has become the design object as realised with the classic range LS 990.
High tech at all levels

Energy efficiency, economy and security – and not just under aspects of medical care; clinic construction has also taken up a key position in terms of technical equipment. Lighting, shade and temperature can now be regulated through a networked KNX system from JUNG. In a clearly arranged design, the devices all fit seamlessly into their surroundings.
Professional Smart Home

Smart building technology – prestigious architecture. The smart KNX solutions combine convenience, security and energy efficiency. So building owners throughout the world can rely on KNX technology from JUNG for their homes. Uniquely furnished in the classic LS 990 switch design in the Les Couleurs® Le Corbusier colours. Exclusive worldwide from JUNG.
Networked convenience

To adjust air conditioning, shade or light, the JUNG building automation responds to hotel guests’ individual wishes and ensures energy efficient operation at the same time. The electrical installations in the diverse JUNG switch design fit seamlessly into any exclusive atmosphere. This turns pure aesthetics into cultivated objectivity.
Intelligently into the future

KNX building technology from JUNG – simply child’s play to operate. That is why KNX has already become the worldwide standard for high-class construction. The well-thought-out JUNG solutions combine function, design and intuitive ease of operation, ensuring maximum convenience, safety and security.
A secure solution

Mature KNX technology means a plus in security. To effectively safeguard the infrastructure against attacks, particularly in hotels and public buildings, in a professional installation, measures need to be carried out at hardware and software level.

**SECURITY THROUGH DISMANTLING PROTECTION**

Protection with special screws

To prevent any direct manipulation of the devices, JUNG recommends the deployment of dismantling protection. Special screws are used here to make it harder to access the KNX bus.

**SECURITY THROUGH NETWORK ARCHITECTURE**

Each room is executed as a separate “KNX island”. KNX IP routers connect these rooms via a fast IP backbone. Thanks to the integrated filter tables, you can, for example, display the status of each room in the central visualization. However, a simple manipulation of the room is prevented.
Checklist for increased security in KNX installations.

**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?

**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?

**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?

**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 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?

**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?

**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?

**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?

**HAVE DEVICES BEEN LOCKED AGAINST RE-CONFIGURATION?**

- If not, enter a BCU key¹ in the ETS Project.

**DO YOU USE KNX SECURE² DEVICES?**

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

**DO YOU SUSPECT UNAUTHORIZED ACCESS TO THE BUS?**

- Record telegram traffic and analyse it.
- Read the PID, Device, Control³ from devices and check whether devices are sending using the same individual Address.
- Read the PID, Download, Counter³ from devices and check whether the device was downloaded again after your configuration.

**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?

**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?

**HAVE DEVICES BEEN LOCKED AGAINST RE-CONFIGURATION?**

- If not, enter a BCU key¹ in the ETS Project.

**DO YOU USE KNX SECURE² DEVICES?**

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

**DO YOU SUSPECT UNAUTHORIZED ACCESS TO THE BUS?**

- Record telegram traffic and analyse it.
- Read the PID, Device, Control³ from devices and check whether devices are sending using the same individual Address.
- Read the PID, Download, Counter³ from devices and check whether the device was downloaded again after your configuration.

**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
ALBRECHT JUNG GMBH & CO. KG
P.O. Box 1320
58569 Schalksmühle
Germany
Phone  +49 2355 806-553
Fax    +49 2355 806-254
mail.vka@jung.de

For sales contacts in your country see:
www.jung-salescontact.com