

CHECKLIST: KNX SECURE PROJECT

for System Integrators and Planners

1. Project Start & Planning

- Have security-critical areas been identified (e.g. remote access, personal data)?
- Has the choice of communication media (Twisted Pair, IP, RF) been made with intent?
- Is the system planned as a fully Secure installation or a mixed setup?
- Has the possibility of tamper-resistant installation in outdoor or public areas been assessed (e.g. concealed operation)?
- Is the physical security concept defined: mounting height, anti-removal protection, secure distribution boards?
- Are all stakeholders aware of the key and access management concept?

2. Device Selection & Procurement

- Are all planned devices KNX Secure-capable (Data Secure, IP Secure)?
- Do all devices come with valid KNX Secure certificates (e.g. with QR codes)?
- Have devices been selected with consideration for FDSK and BCU Key requirements?
- Is it ensured that no non-Secure devices are used in security-critical communication groups?

3. ETS Project Structure & Configuration

- Is ETS version 5.7 or higher being used?
- Have all Secure devices been correctly integrated (FDSKs imported, keyring maintained)?
- Are individual addresses logically assigned (topology-based)?
- Is data flow across lines/segments properly filtered (filter tables, point-to-point blocking)?
- Are group addresses segmented appropriately – e.g. by critical / non-critical areas?
- Are Secure and non-Secure devices kept in separate communication structures?

4. Key Management & Backup

- Are all KNX Secure certificates (FDSKs) stored securely, both digitally and physically?
- Is there a transparent key management strategy (access roles, key assignment)?
- Is the ETS project backed up in multiple locations (locally, externally, encrypted)?
- Has the project been removed from the working device after completion?
- Is there a handover document including password protection and key details?

5. Network Security (for KNX IP / WLAN)

- Are dedicated networks used for KNX communication (LAN / WLAN)?
- Have all network parameters been documented and securely handed over?
- Are routers and switches configured to allow only known MAC addresses?
- Are WLAN SSIDs changed and hidden from public visibility?
- Are IP multicast addresses customised and unused ports blocked from external access?
- Is a VPN required and used for remote access?
- Is a firewall active?

6. Media Integration & Coupling

- Are powerline installations protected using band-stop filters?
- Do KNX RF domains have unique domain addresses?
- Are communication paths across couplers controlled (e.g. address forwarding, filter rules)?
- Is it ensured that broadcasts or point-to-point communication are not unintentionally passed across line boundaries?

7. Commissioning & Handover

- Have all devices been commissioned in encrypted mode?
- Has a full system test been carried out (group addresses, telegram flow, line transitions)?
- Has the ETS password been set and documented?
- Has the ETS project file been verified, finalised and securely handed over?
- Does a handover protocol exist, including all device information and certificates?

8. Diagnostics & Tamper Protection

- Has telegram traffic been analysed – using failure logs if necessary?
- Have **PID_Device_Control** and **PID_Download_Counter** been checked?
- Is the ETS password documented and securely stored?
- Are escalation procedures with the device manufacturer known in case of security anomalies?
- Is there a documented response plan in case of suspected attacks (e.g. disconnect internet, secure logs)?

9. Data Protection & Legal Compliance (GDPR)

- Has a data protection agreement been signed between the installer and the client?
- Has the client received a copy of the final ETS project file?