KNX Sicurezza Checklist
## Checklist per una maggiore sicurezza degli impianti KNX

1. **Hai tenuto conto delle seguenti misure durante l’installazione?**

   - I dispositivi e i moduli applicativi sono fissati a parete? Si garantisce che i dispositivi sono opportunamente protetti contro lo smontaggio (esempio con accorgimenti anti taccheggio)?
   - E’ stato assicurato che persone non autorizzate abbiano limitato accesso ai quadri di distribuzione ove sono installati i dispositivi KNX (esempio sono chiusi a chiave o posti in locali chiusi a chiave)?
   - E’ stato assicurato un accesso protetto nelle aree esterne (esempio montando i dispositivi ad una sufficiente altezza)?
   - Se l’impianto KNX è operativo in aree dell’edificio pubbliche e non sorvegliate, è stato previsto l’utilizzo di dispositivi di ingresso montati in quadri di distribuzione o interfacce per pulsanti a incasso?

2. **State usando il bus (Twisted Pair) come tipo di rete?**

   - Il cablaggio interno o esterno all’abitazione o l’edificio è protetto contro accessi non autorizzati?
   - Se il cavo bus intrecciato è usato in aree che richiedono misure di protezione extra, hai tenuto conto degli accorgimenti riportati al punto 6?

3. **State usando le onde convogliate (Powerline) come tipo di rete?**

   - Sono stati installati i filtri di banda?
   - Se le Powerline sono usate anche fuori dall’edificio, avete preso qualche misura per gli accoppiatori di rete come indicato nel punto 6?

4. **State usando una rete IP come mezzo di comunicazione?**

   - Le impostazioni di rete sono state documentate e concordate con il proprietario dell’edificio o l’amministratore della rete LAN?
   - Gli switch e i router sono impostati in modo che solo i MAC address conosciuti sono in grado di accedere alla rete?
   - Viene usata un’rete LAN o WLAN separata con un hardware dedicato per la comunicazione KNX?
   - L’accesso alla rete (KNX) IP è limitato a persone autorizzate tramite una propria user name e password sicuri?
   - Per la comunicazione KNX IP multicast dovrebbe essere usato un altro indirizzo IP rispetto a quello di default (normalmente 224.0.23.12). Questo indirizzo multicast IP è stato cambiato?
   - La chiave alfanumerica SSID di default dell’access point wireless è stato cambiato?
   - La trasmissione periodica del SSID è stata disattivata?
   - Le porte dei router per KNX verso internet sono state chiuse e il gateway di default usato per il router KNXnet/IP impostato a 0? L’installazione su rete (W)LAN è protetta con un firewall appropriato? Se occorre un accesso internet verso l’impianto KNX, verificate la possibilità di:
     1. Stabilire una connessione VPN al Router Internet
     2. Usare specifici KNX Object Servers del costruttore
### 5 State usando la Radio Frequenza come tipo di rete?
- Avete preso le stesse misure per gli accoppiatori di rete come indicato nel punto 6?  
- Ciascun dominio RF ha un indirizzo di dominio differente?

### 6 Avete usato degli accoppiatori nell’impianto?
- Gli indirizzi individuali dei dispositivi sono stati assegnati secondo la loro collocazione topologica corretta?  
- Avete impedito tramite opportune impostazioni dei parametri degli accoppiatori che indirizzi sorgenti errati possano essere spediti fuori la linea?  
- Avete bloccato la comunicazione Punto-Punto o Broadcast attraverso gli accoppiatori?  
- Le tabelle filtro sono state caricate correttamente e impostate in modo che siano abilitate negli accoppiatori?  
- Sono state considerati gli accorgimenti forniti al punto 7 per gli accoppiatori?

### 7 I dispositivi sono stati protetti contro la riconfigurazione?
- Se no, inserire una password BCU\(^1\) nel Progetto ETS.

### 8 Usate dispositivi KNX Sicuri?\
- Per la comunicazione di gruppo che necessita di essere messa in sicurezza, usate i meccanismi di autenticazione e di crittografia previsti per il dispositivo.

### 9 Sospettate che ci possano essere accessi non autorizzati all’impianto bus?
- Registrate il traffico dei telegrammi e analizzateli.  
- Leggere il PID\_Device\_Control\(^2\) dai dispositivi e verificare se i dispositivi stanno trasmettendo usando lo stesso Indirizzo Individuale.  
- Leggete il PID\_Download\_Counter\(^3\) dai dispositivi e verificate se il dispositivo è stato configurato di nuovo dopo la vostra configurazione.

### 10 Il sistema KNX è interfacciato con un sistema di sicurezza (antintrusione) ?
- Se un impianto KNX è interfacciato con un sistema di sicurezza antintrusione, è stato realizzato in uno dei seguenti modi?  
  1. Tramite dispositivi KNX o gateway certificati da compagnie assicurative nazionali?  
  2. Tramite contatti liberi da potenziale (ingressi binari, interfacce contatti, ...)?  
  3. Tramite interfacce appropriate (RS232, ...) o gateway: è stato assicurato che la comunicazione KNX non attivi volontariamente o involontariamente funzioni rilevanti nel sistema di sicurezza integrato nell’impianto?

---

1) Non tutti i dispositivi possono essere protetti contro la riconfigurazione - contattare il costruttore di riferimento  
2) Disponibile da ETS 5.5 in avanti  
3) Non supportato da tutti i dispositivi