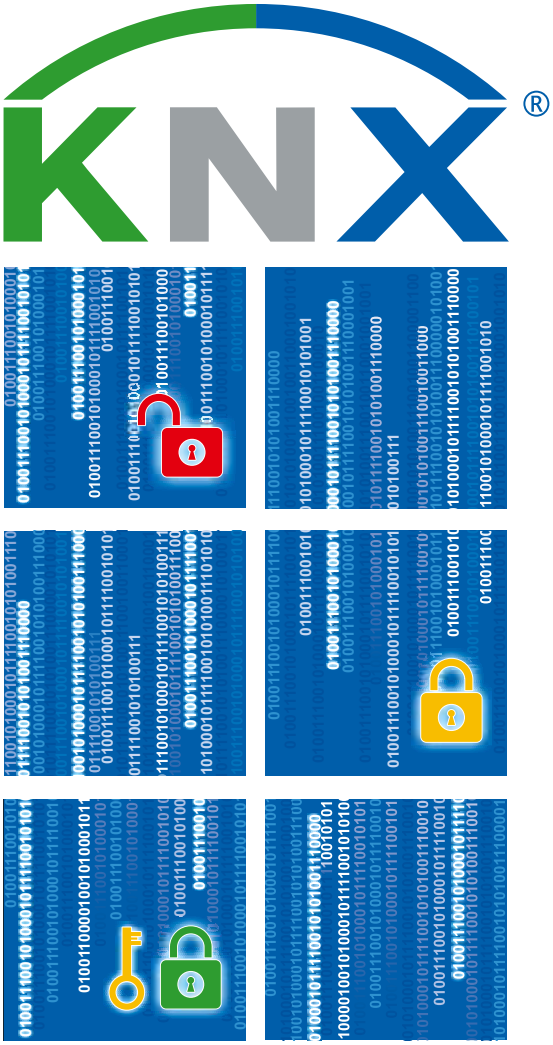


Sécurité KNX
Liste de contrôle

Liste de contrôle pour plus de sécurité dans les installations KNX

1 Les mesures suivantes ont-elles été prises en compte lors de l'installation?

- ☐ Les participants et modules d'applications ont-ils été installés et fixés? Est-il garanti que les participants soient correctement protégés contre le démontage (par exemple grâce à la mise en œuvre de mesures de protection antivol)?
- ☐ Est-il garanti que les personnes non autorisées n'aient qu'un accès limité aux tableaux de distributions contenant des produits KNX (les tableaux sont-ils par exemple toujours fermés à clé ou situés dans des pièces fermées)?
- ☐ Est-il difficile d'accéder aux participants dans les zones extérieures (les participants sont-ils par exemple installés à une hauteur suffisante)?
- ☐ Dans le cas où l'installation KNX peut être utilisée depuis des zones publiques et non surveillées du bâtiment, avez-vous envisagé l'utilisation de modules d'entrées binaires (installés dans les tableaux de distribution) ou d'interfaces de bouton poussoir?

2 Le média de communication est-il de type Paire Torsadée?

- ☐ Le câble installé n'importe où à l'intérieur ou à l'extérieur de la maison ou du bâtiment est-il protégé contre les accès non autorisés?
- ☐ Dans le cas où le câble à paire torsadée est utilisé dans des zones qui nécessitent des mesures de protection additionnelles, avez-vous pris les mesures telles qu'énoncées dans le point 6?

3 Le média de communication est-il de type Courant Porteur?

- ☐ Y a-t-il des filtres d'arrêt de bande?
- ☐ Si le Courant Porteur est également utilisé à l'extérieur du bâtiment, avez-vous pris les mêmes mesures pour le coupleur de média telles qu'énoncées dans le point 6?

4 Le média de communication est-il de type IP?

- ☐ Les paramètres réseau ont-ils été documentés et remis au propriétaire ou à l'administrateur réseau?
- ☐ Les commutateurs et routeurs ont-ils été paramétrés de manière à ce que seules les adresses MAC connues soient en mesure d'accéder au média de communication?
- ☐ Un réseau LAN ou WLAN avec son propre matériel est-il utilisé pour la communication KNX?
- ☐ L'accès aux réseaux IP (KNX) est-il limité aux personnes autorisées via des identifiants appropriés et des mots de passe forts?
- ☐ Pour la communication KNX IP Multicast, une adresse IP différente de l'adresse par défaut devrait être utilisée (normalement 224.0.23.12). Cette adresse IP multicast a-t-elle été modifiée?
- ☐ Le SSID par défaut du point d'accès sans-fil a-t-il été modifié ? La transmission périodique du SSID a-t-elle été désactivée?
- ☐ Les ports des routeurs pour KNX ont-ils été coupés d'internet et la passerelle par défaut du routeur KNXnet/IP a-t-elle été réglée à 0? L'installation (W)LAN a-t-elle été protégée par un pare-feu approprié?
  Si l'accès à Internet pour une installation KNX est nécessaire, vérifiez la possibilité de:
  1. Établir une connexion VPN au routeur Internet.
  2. Utiliser des serveurs d'objets KNX spécifiques au fabricant.

5 Le média de communication est-il de type Radio?

- [ ] Avez-vous pris les mêmes mesures pour le coupleur de média telles qu'énoncées dans le point 6?
- [ ] Chaque domaine RF a-t-il une adresse de domaine différente?

6 Avez-vous utilisé des coupleurs dans l'installation?

- [ ] Les adresses individuelles des participants ont-elles été assignées conformément à la disposition des participants dans la topologie?
- [ ] Empêchez-vous via le réglage des paramètres dans les coupleurs que les adresses sources erronées soient transmises en dehors de la ligne?
- [ ] Avez-vous bloqué les communications de type Point-to-Point et Broadcast dans les coupleurs?
- [ ] Les tables de filtrage ont-elles été chargées correctement et les paramètres ont-ils été réglés de sorte que les tables de filtrage soient prises en compte par les coupleurs?
- [ ] Avez-vous considéré les mesures telles qu'énoncées dans le point 7 pour les coupleurs?

7 Les participants ont-ils été protégés contre la reprogrammation?

- [ ] Si non, entrez un mot de passe BCU[1] dans le Projet ETS.

8 Utilisez-vous des participants KNX Secure[2]?

- [ ] Pour les communications de groupe qui ont besoin d'être sécurisées, utilisez les authentifications et les mécanismes de chiffrement prévus des participants.

9 Suspectez-vous un accès non autorisé au bus?

- [ ] Enregistrez le trafic de télégrammes et analysez-le.
- [ ] Lisez le PID_Device_Control[3] des participants et vérifiez si des participants émettent en utilisant la même Adresse Individuelle.
- [ ] Lisez le PID_Download_Counter[3] des participants et vérifiez si l'appareil a été re-téléchargé après votre configuration.

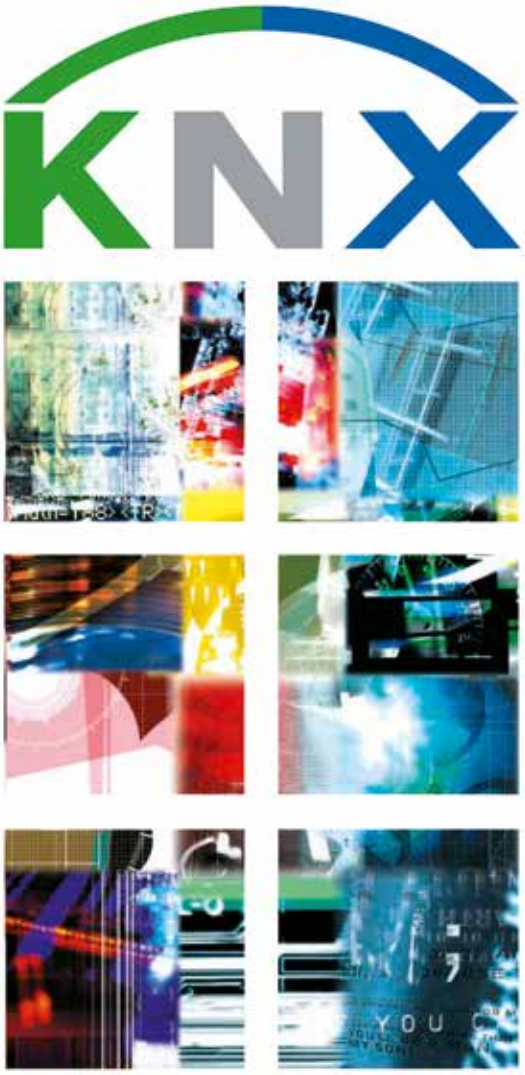
10 Couplage de KNX aux systèmes de sécurité?

- [ ] Quand KNX est couplé aux installations de sécurité, cela a-t-il été réalisé de l'une des manières suivantes?
  1. Via des participants ou passerelles KNX certifiées par les compagnies d'assurances nationales?
  2. Via des contacts libres de potentiel (entrées binaires, interfaces de bouton poussoir, …)?
  3. Via des interfaces appropriées (RS232, …) ou des passerelles : a-t-il été garanti que la communication KNX ne soit pas capable de déclencher des fonctions relatives à la sécurité dans la partie sécurisée de l'installation?

1) Tous les participants ne peuvent pas être protégés contre la reprogrammation

2) Disponible à partir d'ETS5.5

3) N'est pas supporté par tous les participants.



www.knx.org