



Smart home and building solutions.  
Global. Secure. Connected.

# KNX SECURE LISTE DE CONTRÔLE



# LISTE DE CONTRÔLE POUR UN MEILLEUR NIVEAU DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES INSTALLATIONS KNX

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

Le montage des appareils et applications est-il fixe ? Les appareils ont-ils été protégés de manière appropriée contre le démontage (par exemple, utilisation de mesures de protection antivol) ?

S'est-on assuré que les personnes non autorisées n'ont pas accès aux tableaux de distribution sur lesquels des installations KNX sont montées (par exemple, sont-ils toujours verrouillés ou situés dans des salles verrouillées) ?

Est-il difficile d'accéder aux appareils situés à l'extérieur (par exemple, sont-ils situés suffisamment haut) ?

Dans le cas d'une installation KNX utilisable depuis des lieux se trouvant dans des bâtiments publics ou non surveillés, avez-vous envisagé d'utiliser des entrées binaires (montées sur les tableaux de distribution) ou des interfaces à bouton-poussoir ?

Les écrans tactiles sont-ils protégés par des mots de passe (en mode utilisateur, groupe ou invité) ?

## 2. Un câble à paire torsadée est-il utilisé comme média de transmission ?

Le câble est-il partout, à l'intérieur comme à l'extérieur de la maison ou du bâtiment, protégé contre un accès autorisé ?

Si un câble à paire torsadée est utilisé dans des lieux nécessitant des mesures de protection supplémentaires, avez-vous pris les mesures énoncées à la rubrique 6 ?

## 3. Le courant porteur est-il utilisé comme média de transmission ?

Des filtres coupe-bande ont-ils déjà été installés ?

Si le courant porteur est également utilisé à l'extérieur du bâtiment, avez-vous pris les mêmes mesures pour le coupleur multimédia que celles énoncées à la rubrique 6 ?

## 4. L'IP sert-il comme média de transmission ?

Les paramètres réseau ont-ils été documentés et remis au propriétaire de la maison ou à l'administrateur LAN ?

Des commutateurs et des routeurs ont-ils été installés de sorte que seules les adresses MAC connues peuvent accéder au média de transmission ?

Un réseau LAN ou WLAN séparé disposant de son propre matériel est-il utilisé pour la communication KNX ?

L'accès aux réseaux IP (KNX) est-il limité aux personnes autorisées par des noms d'utilisateur appropriés et des mots de passe forts ?

Pour la communication IP KNX multidiffusion, une autre adresse IP telle que l'adresse par défaut doit être utilisée (normalement, 224.0.23.12). Cette adresse IP de multidiffusion 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 après l'installation ?

Les ports des routeurs pour KNX ont-ils été fermés vers Internet et la passerelle par défaut du routeur KNXnet/IP paramétrée à 0 ? L'installation (W)LAN a-t-elle été protégée par un pare-feu approprié ? S'il est nécessaire qu'une installation KNX ait accès à Internet, vérifiez la possibilité de mettre en œuvre ce qui suit :

1. Établissement d'une connexion VPN au routeur Internet
2. Utilisation de serveurs d'objets KNX spécifiques des fabricants

## 5. La radiofréquence est-elle utilisée comme média de transmission ?

Avez-vous pris les mêmes mesures pour le coupleur multimédia que celles énoncées à la rubrique 6 ?

Chaque domaine RF a-t-il une adresse de domaine différente ?

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

Des adresses individuelles d'appareils ont-elles été attribuées selon leur place dans la topologie ?

Empêchez-vous, par l'établissement de paramètres appropriés dans les coupleurs, que des adresses de sources incorrectes soient envoyées à l'extérieur de la ligne ?

Bloquez-vous la communication point à point et en diffusion générale par le biais de coupleurs ?

Les tables de filtrage ont-elles été chargées correctement et les réglages ont-ils été faits de manière à ce que les tables de filtrage soient prises en compte par les coupleurs ?

Avez-vous envisagé les mesures énoncées à la rubrique 7 concernant les coupleurs ?

## 7. Les appareils ont-ils été verrouillés contre une reconfiguration ?

Si tel n'est pas le cas, saisissez une clé BCU 1 dans le projet ETS.

<sup>1</sup> Not all devices can be protected against re-configuration - contact the relevant manufacturer

## 8. Utilisez-vous des appareils KNX Secure<sup>2</sup> ?

Pour la communication de groupe devant être sécurisée, utilisez les mécanismes d'authentification et de cryptage prévus pour l'appareil.

## 9. Soupçonnez-vous un accès non autorisé au bus ?

Enregistrez le trafic des télégrammes et analysez-le. Dans le cas d'appareils KNX Secure, lisez les journaux de défauts.

Consignez l'heure et les effets observés (ce qui s'est produit, ce qui ne s'est pas produit, pourquoi et quand).

Désactivez la connexion Internet du système KNX et vérifiez si des effets disparaissent ou pas.

Contactez l'assistance téléphonique du fabricant : les effets ou les problèmes de sécurité sont-ils connus du fabricant, des mises à jour sont-elles disponibles ?

Lisez le PID\_Device\_Control3 des appareils et vérifiez si les appareils effectuent des envois avec la même adresse individuelle.

Lisez le PID\_Device\_Control3 des appareils et vérifiez si l'appareil a été téléchargé de nouveau après votre configuration.

## 10. Les appareils ont-ils été verrouillés contre une reconfiguration ?

Si du KNX est couplé aux installations de sécurité, cela a-t-il été réalisé de l'une des manières suivantes ?

1. Au moyen d'appareils ou de passerelles KNX couvertes par une compagnie d'assurances de dommages nationale ?
2. Au moyen de contacts libres (entrées binaires, interfaces à bouton-poussoir, etc.) ?
3. Au moyen d'interfaces (RS232, etc.) ou de passerelles : s'est-on assuré que la communication KNX ne puisse pas déclencher de fonctions relatives à la sécurité dans la partie sécurité de l'installation ?

## 11. Mesures de sécurité générale

ETS est-il à jour ?

1. Le PC sur lequel ETS est installé est-il sûr (recherche de virus à jour, système d'exploitation récemment mis à jour) ? Il est recommandé d'utiliser un appareil dédié pour la conception KNX et la mise en service.
2. Lors de l'installation, il faut éviter de brancher d'autres périphériques de stockage de données au PC (clé USB, disque dur externe, etc.).
3. Les extensions et applications ETS doivent être installées de préférence avant l'installation.
4. Sauvegardez le fichier de projet après l'installation (idéalement, sur une clé USB à conserver en lieu sûr) et effacez le projet du PC.

Le firmware des appareils utilisés est-il à jour?

## 12. Autres mesures de confidentialité (RGPD)

L'installateur et le client doivent signer une déclaration de confidentialité.

Afin de répondre aux obligations du RGPD, l'installateur doit remettre une copie du fichier de projet ETS au client.

<sup>2</sup> Disponible à partir de la version ETS 5.5. / <sup>3</sup> Non pris en charge par tous les appareils.