KNX NATIONAL SWISS

SÉCURITÉ DE L'INFORMATIQUE ET DE LA TECHNIQUE DES BÂTIMENTS

Guide KNX SWISS sur la sécurité de l'automatisation des bâtiments et des locaux basée sur des réseaux KNX et IP

Remarques

Informations techniques
Les informations et données publiées dans cette brochure ont été établies en toute bonne foi. Sous réserve d'erreurs et de modifications techniques.

Exclusion de responsabilité
KNX Swiss décline toute responsabilité en cas de dommages liés à l'utilisation de la présente publication. Toute responsabilité en cas de dommages liés directement ou indirectement à l'utilisation de l'information contenue dans ce document est exclue.

Document disponible au téléchargement à l'adresse suivante :
www.knx.ch/secure

Table des matières

Version 1.1 | 01/2023

1 Raison d'être et finalité du document

1.1 Situation initiale

Les bâtiments intelligents régulant leur énergie en toute autonomie, intégrés à un système énergétique de plus grande envergure, communiquant avec le smartphone des utilisateur-rice-s des locaux, voire échangeant des données avec d'autres bâtiments, constituent la clé du futur intelligent du parc immobilier suisse et une plateforme d'expansion de la numérisation et la durabilité de l'économie et de la société.

La numérisation et la mise en réseau rendent possible l'automatisation. Ceci dit, les nouvelles possibilités qui en résultent, les nouveaux accès de et vers l'extérieur et le recours à l'intelligence artificielle créent également des points vulnérables. Que les cybercriminels se font un plaisir d'exploiter. Le risque de perte de données, de chantage ou d'espionnage augmente lorsque le protocole Internet (IP) devient un élément déterminant dans le réseau du bâtiment. Les attaques sur le réseau IP menacent les fonctions de sécurisation de l'automatisation des bâtiments.

Il est donc temps d'accorder à l'infrastructure IT de l'automatisation des bâtiments l'attention qu'elle mérite et de projeter et réaliser de nouvelles installations sûres.

1.2 Objectif du document

Le présent guide présente aux bureaux d'études, intégrateur-rice-s systèmes et informaticien-ne-s du bâtiment comment est mis en place, structuré et exploité un réseau de bâtiment sûr. Il informe également sur les responsabilités des spécialistes IT de la maîtrise d'ouvrage, du bureau d'études, des intégrateur-rice-s et des exploitant-e-s. Enfin, il fournit des conseils et astuces sur la mise en œuvre d'un projet KNX Secure.

Ce guide contient des informations d'ordre général. Toute mesure doit être ajustée aux conditions locales.

2 Smart buildings : les éléments moteurs en Suisse

La numérisation du parc immobilier suisse vient à peine de commencer. Mais la tendance est à la conception de bâtiments intelligents dès le départ et à l'équipement des ouvrages existants. L'Internet of Things (IoT) et d'autres éléments moteurs viennent renforcer cette évolution :

- **Pression au niveau des coûts :** la présence d'un seul réseau dans un bâtiment simplifie la maintenance et abaisse les coûts.
- **Autarcie énergétique :** dans le meilleur des cas, les bâtiments intelligents produisent et consomment leur propre énergie. Pour ce faire, il doit y avoir un échange intelligent de données entre les appareils, aussi bien entre les différents corps d'état qu'entre les bâtiments (couplage sectoriel).
- **Industrie 4.0 :** les usines intelligentes doivent également être accessibles à distance. Les technologies IT et OT (Operational Technology) grandissent ensemble.
- **Smart city :** des approches Smart City se développent dans différentes villes et quartiers. La mise en réseau et les nouvelles technologies ont pour vocation de renforcer l'efficacité, la durabilité et la cohabitation des êtres humains.
- **Évolution des technologies :** le (multi-) cloud hybride devient le concept déterminant des architectures IT. Grâce à l'intelligence artificielle, aux logiciels d'automatisation, aux nouvelles approches de sécurisation des réseaux de type Zero Trust, à l'augmentation de la densité des capteurs, aux accès sans fil rapides (5G, Wi-Fi 6) et aux architectures IT intelligentes, il est possible d'intégrer les bâtiments à des structures de réseau plus importantes sur la base de normes ouvertes.

Un seul réseau pour tous les services et installations dans le bâtiment, au lieu de plusieurs normes différentes implémentées en parallèle : cette évolution obéit, d'une part, à une logique des coûts, et, d'autre part, elle simplifie la maintenance et la surveillance de la consommation énergétique dans l'ouvrage.

Tous les services nécessaires utilisent ainsi la même infrastructure IP et doivent être conformes aux prescriptions de cybersécurité de votre réseau. Cela permet d'administrer le réseau à long terme à une seule adresse (service informatique) et d'obtenir les certificats de cybersécurité.

Ethernet Norme de transfert câblé des données. Inventé pour les réseaux LAN (Local Area Networks), il est aujourd'hui également utilisé sur les Wide Area Networks (WAN).

Les applications les plus exigeantes en matière de fiabilité utilisent l'Ethernet temps réel. Actuellement, la bande passante disponible atteint 400 Gb/s. Et elle est en progression constante. Très bientôt, nous aurons 800 Gb/s, et des taux de transfert atteignant 1,6 terabit/s sont en développement.

2.1 Des règles du jeu fondamentales

Le service informatique se voit confier de nouvelles tâches : il ne s'occupe plus seulement des flux de données et des réseaux, mais également des réseaux de l'automatisation des bâtiments. Il n'assure pas seulement des accès sécurisés depuis l'extérieur (Remote), mais également des connexions et structures réseau dans l'ensemble de l'ouvrage. Le tout en veillant à combiner intelligemment et en toute sécurité les normes **Ethernet** (câble), Wi-Fi 6 et 5G.

Et lorsqu'un bâtiment fait partie de ce que l'on appelle une « infrastructure critique », les exigences en matière de cybersécurité sont plus sévères. Les directives en matière d'informatique, mais également de périphériques, deviennent plus strictes.

3 L’informatique des bâtiments intelligents

3.1 Mise en place d’une infrastructure IP sécurisée

Les technologies de l’information sont basées sur l’échange de données – et aujourd’hui sur le protocole Internet. Ce dernier est partout, sur les réseaux locaux (LAN), sur les réseaux longue distance (WAN) et sur l’Internet public.

Les périphériques, supports de données ou données isolés localement sont de plus en plus rares. L’informatique évolue vers une architecture cloud regroupant plusieurs prestataires, ainsi que des clouds publics et privés (multicloud). S’y ajoutent des structures informatiques locales et des données qui ne peuvent être sur le cloud pour des raisons légales. Il y a également des infrastructures « edge », situées en périphérie de réseau. Dans celles-ci, le traitement des données est décentralisé là où les données sont nécessaires. Une **latence** courte est importante

Latence Le délai de transit ou retard est un critère de qualité essentiel d’une infrastructure informatique, et selon l’application, la latence joue un rôle plus ou moins important : plus elle est faible, meilleure est l’expérience utilisateur.

L’informatique des bâtiments intelligents doit donc réunir certaines conditions préalables. Elle est étroitement liée à la technique des bâtiments et est équipée d’interfaces vers les appareils KNX.

Configuration minimale requise pour la sécurité technique :

- Connexion Internet avec adresse IP statique
- Routeur du fournisseur d’accès en mode bridge avec pare-feu
  - > DHCP limité, réseau local avec adresse IP fixe
  - > Accès restreints depuis le WAN
  - > Services ouverts (ports) seulement sur les périphériques vraiment nécessaires à l’exploitation
  - > Accès à distance seulement via VPN (Virtual Private Network)
  - > Seuls les mots de passe sûrs sont autorisés. Encore mieux : authentification multifacteur en standard ou **Zero Trust**
  - > Restreindre les points d’accès Wi-Fi publics et l’accès à TechNet/pare-feu

Zero Trust La sécurité réseau classique est basée sur le fait que chaque client obtient l’accès au réseau après son authentification et peut y évoluer librement. L’architecture Zero Trust est radicalement différente : elle ne fait confiance à aucun client et à aucun utilisateur. Cette approche éminemment personnalisée directement au niveau des données permet un contrôle permanent des flux de données.

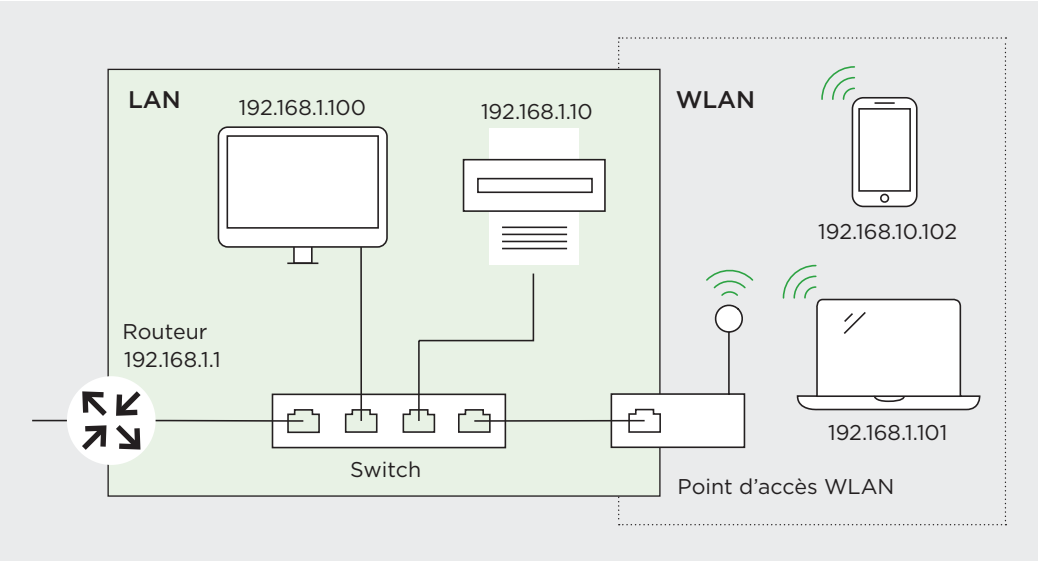


Fig. 3.1-1 Mise en place d’un réseau simple

3.2 Mise en place d'un réseau sécurisé

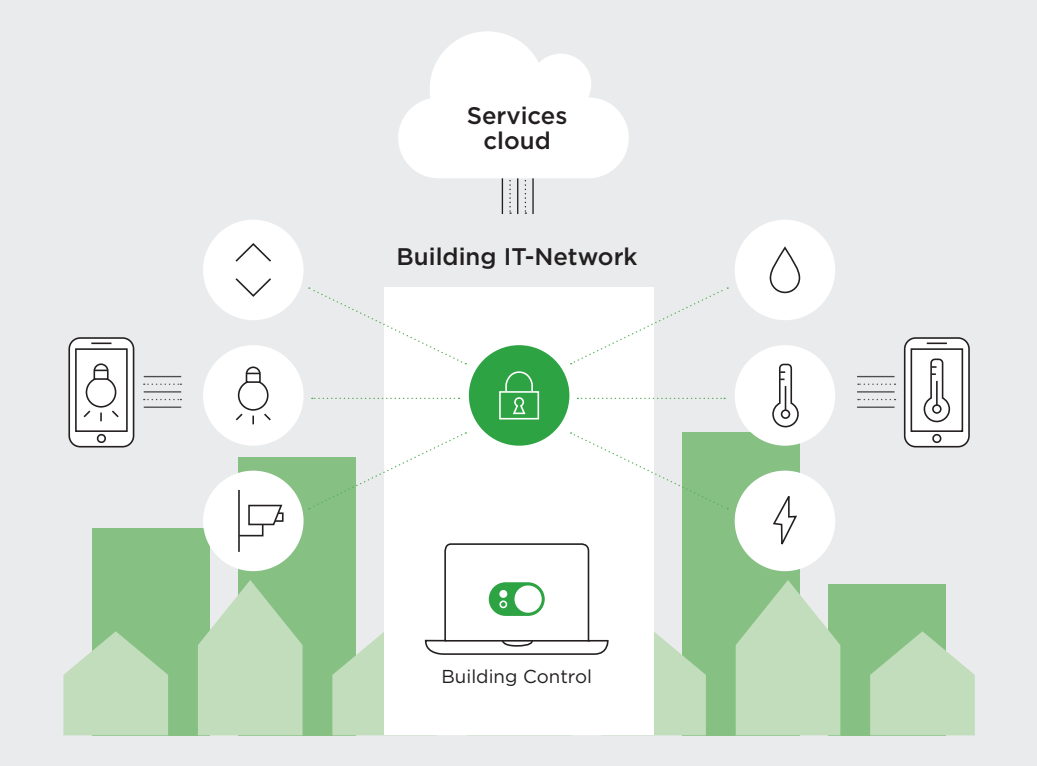
La complexité d'un réseau ne saurait être sous-estimée. Pour le mettre en place, il faut donc avoir de l'expérience en architectures réseau. Dans le cas contraire, l'aide d'un expert en réseaux est indispensable. Nous recommandons de coopérer étroitement avec le service informatique, d'autant plus qu'il s'agit de mettre en place un cloud privé.

Le cloud privé offre des services IT sur Internet ou sur un réseau privé réservé à un cercle d'utilisateurs restreint. Le smart building est un élément isolé d'un réseau plus étendu, composé d'autres clouds publics ou privés.

Au sein du smart building, les différentes installations / éléments d'installation doivent pouvoir communiquer sur un réseau commun sécurisé, protégé contre tout accès non autorisé.

Pour le bâtiment intelligent, cela signifie que les «silos de réseaux», tels qu'ils avaient été créés par le passé, ne répondent pas au niveau actuel de la technique. Ces derniers offrent beaucoup trop de vulnérabilités et, de plus, leur sécurité est assurée différemment selon le type d'installation. Raison pour laquelle, dans le cadre de la convergence entre la gestion technique des bâtiments et l'informatique, le groupe d'intérêt du marché **IP-BLiS** recommande l'emploi harmonisé du protocole Internet (IP) sur l'ensemble du réseau. IP-BLiS n'est pas une nouvelle organisation, mais une initiative regroupant des organisations existantes.

IP-BLis Plusieurs acteurs de l'automatisation des bâtiments coopèrent au sein de l'organisation pour promouvoir les réseaux IP sécurisés dans les bâtiments.



Source : ip-blis.org BuildingTrend.png

Fig. 3.2-1 IP-BLiS favorise les solutions basées sur IP sécurisées, harmonisées et valides pour toutes les normes dans le smart building.

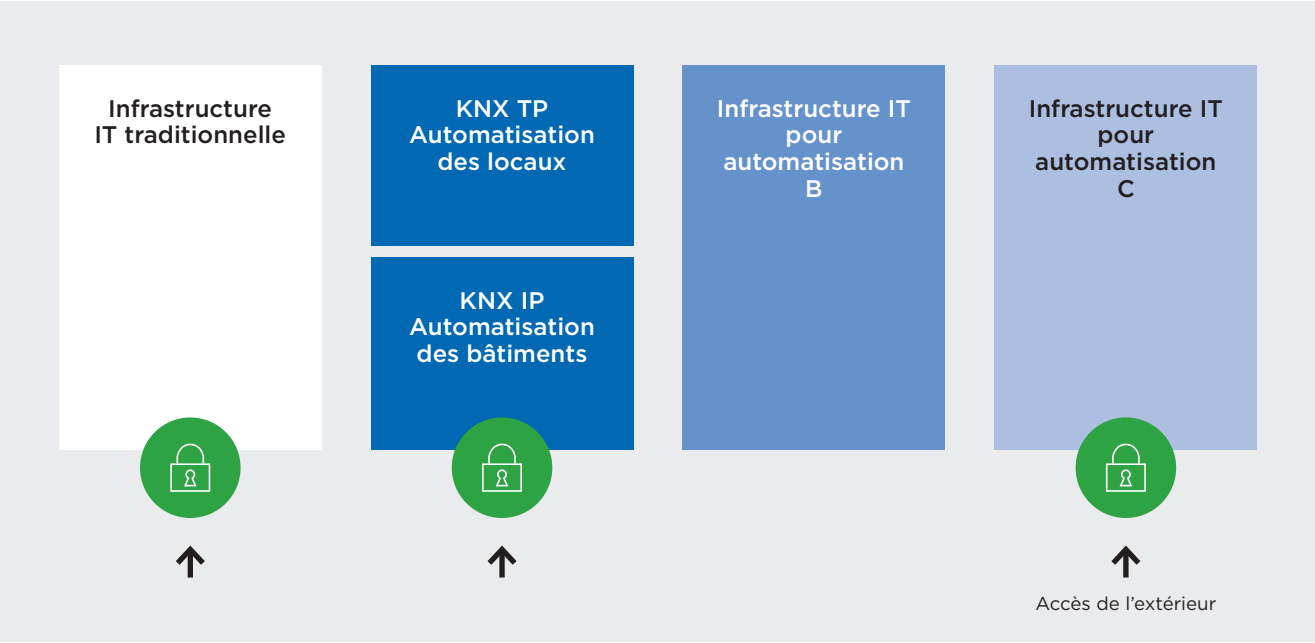


Fig. 3.2-2 À éviter dans les bâtiments : une infrastructure brouillonne et différents concepts de sécurité.

Comme mentionné en introduction, selon le niveau actuel de la technique, les différents réseaux sont regroupés dans un réseau harmonisé. Cela impose, par nature, l'effort de coordination correspondant de la part de toutes les parties prenantes. Un administrateur réseau peut ou doit prévoir la mise en place d'un tel réseau dès la phase de l'étude.

Comment mettre en place des réseaux IP sécurisés dans les bâtiments ?
Chaque bâtiment exige une structure réseau personnalisée. De manière générale, les réseaux doivent être segmentés, c'est-à-dire divisés en plusieurs petits sous-réseaux. Chaque sous-réseau peut recevoir ses propres dispositifs de protection et fonctions de contrôle. Tout accès se fait donc d'abord par un sous-réseau.

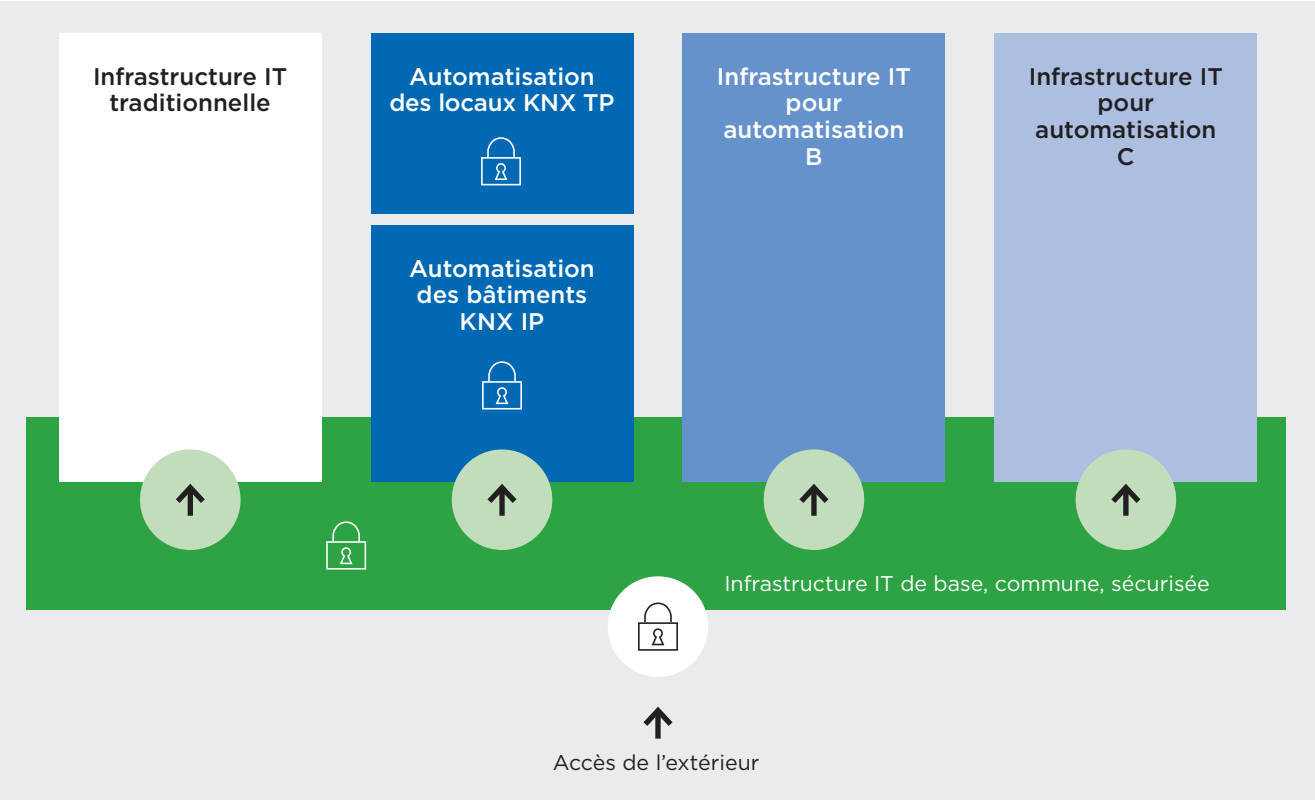


Fig. 3.2-3 Il faut créer une infrastructure informatique de base sûre et, avant tout, coordonnée.

La **virtualisation du réseau** constitue la prochaine étape. Un réseau défini par logiciel (SDN) permet de confier le contrôle à un logiciel via le réseau. Celui-ci gère tous les périphériques du réseau d'une manière centralisée. La fonction des différents routeurs et switches se limite au transport et ces derniers n'ont plus besoin d'être programmés individuellement. Les réseaux peuvent également être établis comme un service sur le cloud et être gérés de manière centralisée. Le **Network as a Service (NasS)** fournit tous les services informatiques nécessaires pour centraliser sur le cloud la gestion du trafic de données au sein du bâtiment et avec d'autres sites.

Moyennant des concepts de réseau de type **Zero Trust,** les équipes informatiques protègent des bâtiments de tout accès non autorisé. Selon cette approche, aucune confiance n'est faite aux périphériques, de sorte que le trafic de données est contrôlé à chaque instant. Ce concept exempt de mot de passe doit être intégré à la planification du réseau dès le départ. L'accès doit aussi être soumis à une **authentification multifacteur,** c'est-à-dire à des approbations via un deuxième, voire un troisième canal (p. ex. SMS).

Comment coopérons-nous avec le service informatique ?
Il doit être impliqué de manière précoce et réaliser une analyse du réseau, qui déterminera la suite de la procédure. On examine alors qui doit pouvoir accéder à quelles fonctions et données dans le cadre de quel rôle. La logique veut que le service informatique se charge également du monitoring de l'automatisation du bâtiment respectivement du réseau auquel elle est liée. Cela permet d'identifier automatiquement les intrus sur la base des anomalies constatées dans le trafic réseau.

Quels sont les autres aspects à prendre en compte ?
Le périmètre d'un bâtiment est aujourd'hui très flou. Il n'y a plus de véritable intérieur ni extérieur. Parfois, les facility managers accèdent également au bâtiment depuis

l'extérieur sur certains réseaux – rendant les exigences posées à la sécurité du réseau plus pointues. Le SDN offre la base de l'intégration d'autres sites comme par exemple d'autres bâtiments ou sites de télétravail sur un réseau commun.

Les appareils Ethernet tels que les switches et les routeurs doivent répondre aux plus hautes exigences et être compatibles SDN. L'industrie propose des matériels spécifiques sécurisés pour les infrastructures critiques.

L'Ethernet est la technique sur laquelle sont basés les réseaux câblés et les protocoles réseau tels que **IP (Internet Protocol).** Le réseau Ethernet transporte aussi du courant, par exemple pour alimenter des capteurs. Ces appareils doivent être protégés contre la surtension (SP, Surge Protection). Dans les applications d'automatisation, on utilise l'Ethernet temps réel. Grâce à des adaptations techniques, ces réseaux remplissent les exigences de fiabilité les plus élevées dans la communication.

Protocole Internet
Le protocole Internet (IP) est à la base de l'Internet et aujourd'hui de la plupart des réseaux de données. Il permet de traiter des paquets de données indépendamment d'une connexion. Les réseaux IP sont dynamiques et hétérogènes, et donc relativement insensibles aux pannes. Les protocoles utilisés actuellement sont IPv4 et IPv6.

Dans **l'edge computing,** les données sont traitées sur place et non pas dans un centre de calcul – par exemple dans un bâtiment neuf équipé en informatique. Cela réduit les temps de latence par exemple pour les robots tributaires de données en temps réel. Des temps de latence élevés augmenteraient les risques auxquels sont exposées les données dans l'automatisation.

Les switches modernes permettent de mieux faire converger les systèmes industriels et OT (Operational Technology) vers les réseaux informatiques classiques, et d'introduire les techniques de réseau industrielles également dans les bâtiments.

Il est également envisagé et prévu d'intégrer les réseaux sans fil (WLAN basé sur le standard Wi-Fi et la téléphonie mobile 5G) à l'automatisation des bâtiments. Cette étape exige d'effectuer des mesures dans le bâtiment et de répartir soigneusement les points d'accès en fonction de leur portée (« couverture »).

4 Structure sécurisée de l'automatisation des bâtiments (KNX Secure)

4.1 KNX Secure

KNX Secure fournit des technologies d'exploitation sécurisée de systèmes KNX et d'optimisation réseau avec les réseaux IP. Ces technologies permettent de réaliser des installations KNX sûres dans l'automatisation des locaux et des bâtiments – intégrales ou axées sur des applications spécifiques.

Pour les intégrateur-rice-s systèmes KNX, KNX Secure n'a en fait rien de très nouveau. KNX Secure comprend :

- **KNX IP Secure :** le flux de données KNX est protégé par un chiffrement intégral sur le réseau IP.
- **KNX Data Secure :** le flux de données KNX est protégé par chiffrement et authentification sur le câble de données KNX à deux conducteurs ou par radio.

Les deux technologies peuvent être combinées ou utilisées en parallèle.

Les appareils KNX Secure sont identifiés par la lettre « X », un cadenas ou une plaquette signalétique. Ils autorisent un fonctionnement sécurisé ou non sécurisé. En cas de modification ou d'extension, l'installation KNX reste donc flexible. L'exploitation mixte est également possible et la mutation peut s'effectuer progressivement dès lors que les appareils KNX sont compatibles avec la norme KNX Secure.

> À l'achat de nouveaux appareils, KNX Secure doit devenir la norme, notamment si la topologie est basée sur IP.

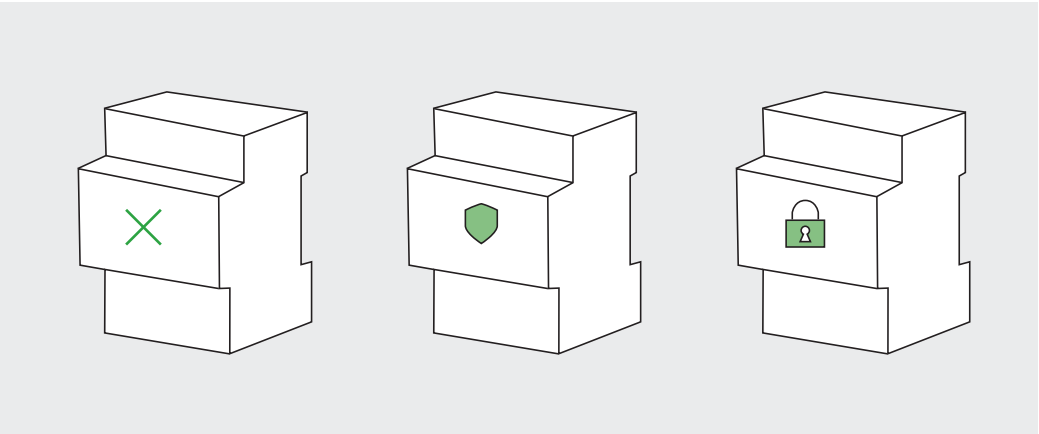


Fig. 4.1-1 Les appareils KNX sont identifiés de plusieurs manières.

Le format des télégrammes étant plus long, les composants systèmes utilisés (p. ex. coupleurs de zones / lignes) et les interfaces de données locales d'ETS (p. ex. USB) doivent prendre en charge les Extended Frames.

4.1.1 Certificats des appareils

Les appareils KNX Secure possèdent un certificat qui est apposé sur le boîtier sous la forme d'un code QR.

Fig. 4.1-2 Exemple de certificat sur un coupleur de ligne. Le certificat ❶ est apposé de manière permanente, le deuxième ❷ peut être retiré pendant l'étude, avant la pose dans un répartiteur.

Le certificat de l'appareil contient la «clé de configuration d'appareil départ usine» (Factory Default Setup Key, FDSK, longueur de la clé 128 bits) ainsi que le numéro de série de l'appareil.

Fig. 4.1-3 Le certificat est apposé sur chaque appareil Secure sous la forme d'un code QR et/ou d'une séquence alphanumérique. Il contient la «clé de configuration d'appareil départ usine» (Factory Default Setup Key, FDSK) ainsi que le numéro de série de l'appareil.

Nous recommandons de retirer le certificat de l'appareil après qu'il a été scanné sur ETS, et ensuite de le conserver dans un endroit sûr (p. ex. avec la documentation relative à l'installation).

4.1.2 Gestion sur ETS

ETS ETS est l'outil de configuration harmonisé permettant de paramétrer les appareils de plus de 500 fabricants dans le monde et de réaliser les projets KNX.

Les certificats des appareils apposés sur les appareils Secure doivent être saisis dans le projet ETS correspondant pendant la phase de l'étude. Cette opération peut se faire à l'aide d'un scanner, de la webcam de l'ordinateur portable ou de son clavier ou encore sur une application spécifique. Dans le projet ETS, en présence d'appareils KNX Secure, la fonction Secure est activée automatiquement. ETS assure en arrière-plan, l'ensemble de la gestion des certificats des appareils du projet en question.

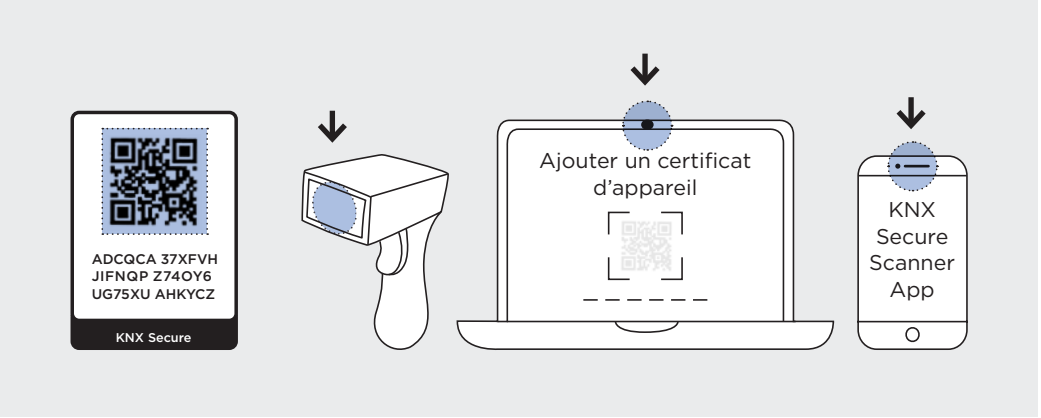


Fig. 4.1-4 Les certificats des appareils peuvent être saisis à l'aide d'un scanner, de la webcam de l'ordinateur portable, d'une application spécifique ou d'un clavier.

FDSK «Clé de configuration d'appareil départ usine» (Factory Default Setup Key, FDSK).
Cette clé de configuration paramétrée à l'avance est unique pour chaque appareil et ne peut être ni effacée ni modifiée.

Lors du chargement des adresses physiques des appareils KNX, le logiciel ETS reconnaît quelle FDSK lue correspond à l'appareil en question à partir de son numéro de série. À partir de la FDSK, le logiciel génère en arrière-plan dans le projet une clé individuelle du périphérique (Toolkey) qui est transmise à l'appareil KNX Secure lors de la mise en service initiale. Cette opération est chiffrée et se produit au premier téléchargement à l'aide de la FDSK. Ensuite, il n'est possible d'apporter des modifications sur un appareil KNX Secure que sous ce projet ETS. Par la suite, la FDSK ne sera plus nécessaire, à moins que l'appareil ne soit réinitialisé à son réglage d'usine (moyennant un processus propre au fabricant). Dans ce cas, toutes les données de sécurité paramétrées seront effacées.

Pour toute adresse de groupe sécurisée liée à un appareil KNX Secure et créée au stade de l'étude, ETS génère une clé d'exécution secrète. Toutes les clés d'exécution sont enregistrées dans le projet et visibles dans le rapport «Sécurité du projet» (voir point 4.1.4).

Cela fonctionne pour tous les appareils câblés (TP), basés sur le sans-fil (RF) et sur le réseau (IP).

4.1.3 Représentation de KNX Secure sur ETS

Dans la représentation de la topologie, les appareils KNX Secure sont signalés par le symbole d'un bouclier permettant de les distinguer facilement des appareils KNX non sécurisés. Le même symbole du bouclier identifie les objets de groupes ou adresses de groupes reliés par une attribution sécurisée.

4.1.4 Mot de passe du projet

Dès qu'un appareil KNX Secure est ajouté à un projet KNX sous ETS, le logiciel exige la configuration d'un mot de passe. Celui-ci doit être noté et ne doit **pas** être perdu, car à défaut il ne sera plus possible d'accéder au projet.

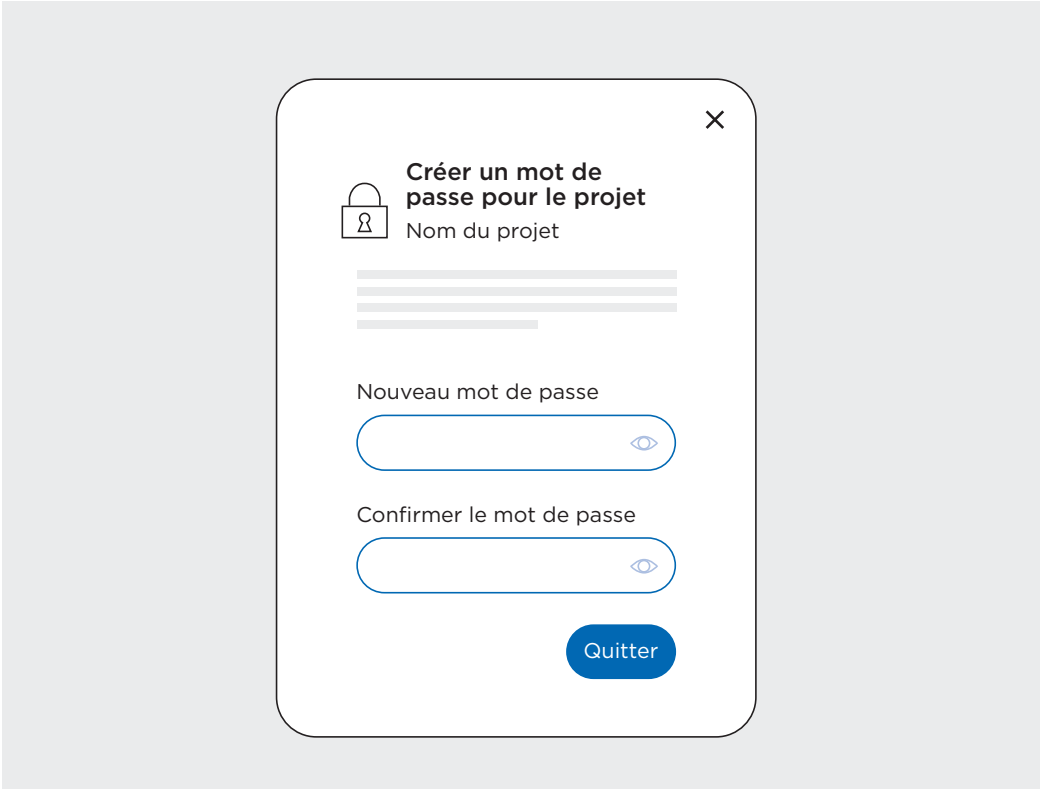


Fig. 4.1-5 Le mot de passe du projet sur ETS doit être conservé dans un endroit sûr, car il est impossible d'accéder à nouveau au projet sans celui-ci.

4.1.5 Rapport Secure sur ETS

Via l'option « Rapports » du logiciel ETS et la rubrique « Sécurité du projet », il est possible d'imprimer tous les détails relatifs à la sécurité du projet ETS en question. Dans le rapport « Sécurité du projet » figurent la clé backbone et toutes les clés des appareils, ainsi que les codes d'authentification des interfaces. Ce rapport contient donc toutes les données relatives à la sécurité, d'où l'importance de le conserver en lieu sûr. En cas de perte du projet ETS, ces informations resteront au moins disponibles. Elles sont nécessaires pour remettre en service les appareils après une réinitialisation à leur réglage d'usine. Le rapport « Sécurité du projet » doit être transmis à l'exploitant du bâtiment (donneur d'ordre), accompagné des autres données relatives au projet.

4.1.6 Spécification normalisée

ISO-Standards
iso.org

Les mécanismes de protection spécifiques de KNX Secure sont basés sur des algorithmes de sécurisation normalisés sur le plan international selon **ISO** 18033-3 et s'appuient sur le chiffrement reconnu suivant la norme AES 128 CCM.

KNX
knx.org

En outre, **KNX** Secure est standardisé en Europe (en tant qu'élément de la série EN 50090, parties 3-4) et dans le monde entier (en tant que norme EN ISO 22510). KNX est donc le premier système de bus de terrain au monde à offrir un concept de sécurisation multifabricants pour les applications de la maison et du bâtiment intelligents. De quoi assurer une protection maximale des données par l'authentification et le chiffrement de la communication de données.

KNX Data Secure utilise le mode CCM avec chiffrement AES 128 bits (chiffrement des données « Counter-Mode » avec contrôle d'intégrité « CBC-MAC-Mode ») et clés symétriques. Par clé symétrique on entend qu'aussi bien l'émetteur, pour le chiffrement des messages sortants (authentification et contrôle d'intégrité), que les récepteurs, pour la vérification et le déchiffrement des messages entrants, utilisent la même clé.

4.2 KNX Data Secure

KNX Data Secure chiffre et authentifie les télégrammes entre deux terminaux via les voies de transmission KNX telles que Twisted Pair et radio. Pour cela, tous les participants et composants à protéger doivent être des appareils KNX Data Secure, qu'ils soient connectés au système de bus KNX via Twisted Pair ou par radio.

Le logiciel ETS assure que les adresses de groupes sécurisées ne soient reliées qu'à des objets de communication (appareils) compatibles KNX Data Secure. Outre la sécurisation intégrale de zones et lignes KNX entières, KNX Data Secure permet également de sécuriser certaines applications KNX exposées à des risques.

Dans la même topologie, les fonctions sécurisées et non sécurisées peuvent cohabiter – y compris au sein d'un appareil KNX Data Secure. Cela signifie qu'un appareil KNX Data Secure peut avoir aussi bien des objets de groupes connectés à des adresses de groupes sécurisées que des objets de groupes connectés à des adresses de groupes non sécurisées.

Dans le système KNX Data Secure, il ne faut pas oublier que les télégrammes transmis sur la ligne de bus sont plus longs que les télégrammes standard en raison de la clé de sécurité. Raison pour laquelle il faut veiller, dès le stade de l'étude, à répartir intelligemment la topologie, notamment le nombre d'appareils sécurisés par ligne. Depuis la version ETS 6, les coupleurs de segments sont utilisables avec des tables de filtrage qui, grâce à l'activation de ces dernières, sont capables de segmenter le trafic de bus.

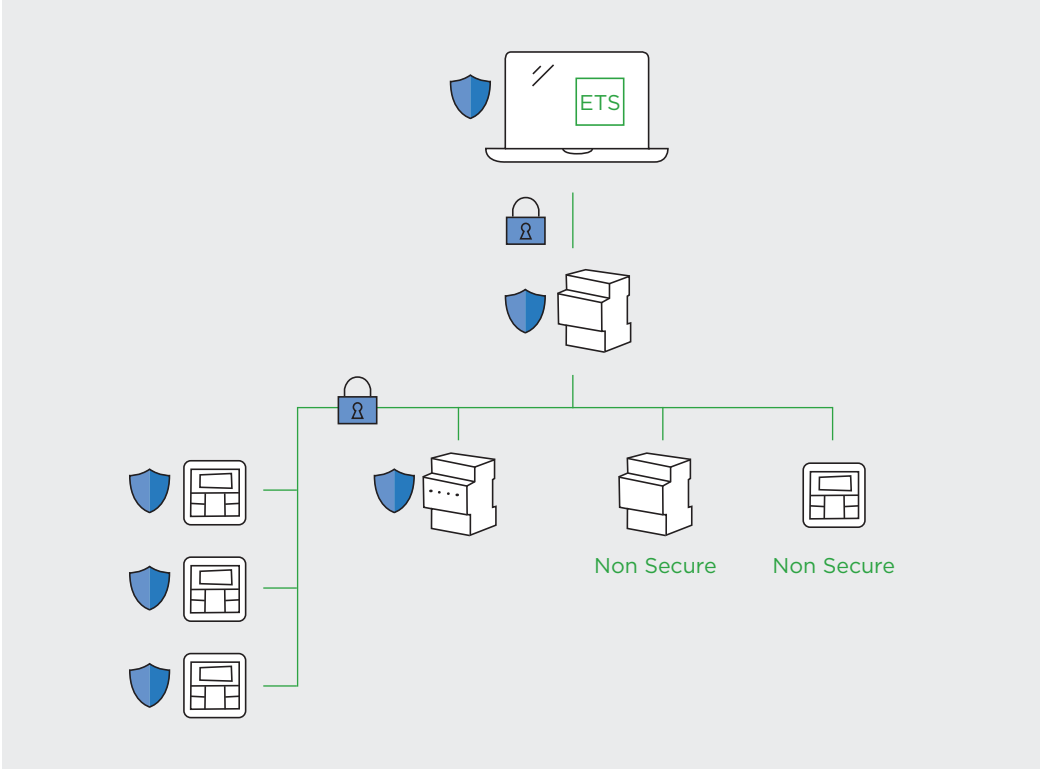


Fig. 4.2-1 KNX Data Secure: les télégrammes et appareils KNX sur le réseau KNX sont chiffrés et protégés. Ils ne sont pas accessibles, manipulables ou modifiables par des tiers non autorisés sur le réseau.

4.3 KNX IP Secure

Avec KNX IP Secure, tous les télégrammes KNX échangés entre eux par les routeurs KNX IP (ou appareils KNX IP) dans un projet sont transmis chiffrés et sécurisés. Les messages de tunnelage ou de routage KNX sur IP ne sont donc pas accessibles et manipulables par des tiers (voir également fig. 6.2-1 « Principe de mise en place d'un réseau de technique des bâtiments sécurisé »). Aux fins du chiffrement, **ETS** prépare la communication IP des routeurs KNX IP en conséquence en arrière-plan.

ETS Le logiciel Engineering Tool Software (ETS) permet de configurer les appareils KNX. Il est compatible multifabricants.

À l'activation de « la mise en service sécurisée » du routeur KNX IP, ETS génère une « clé backbone » en arrière-plan. Si nécessaire, cette clé peut être consultée à tout moment sur ETS via l'option « Rapports » > « Sécurité du projet ». Les composants tiers, à savoir les appareils, systèmes et passerelles qui n'ont pas été configurés dans le projet ETS, peuvent participer à la communication sécurisée à l'aide de cette « clé backbone ».

Lorsque le réglage « Mise en service sécurisée » est désactivé après une activation puis réactivé par la suite, ETS génère une nouvelle clé backbone à chaque activation. Celle-ci doit alors être modifiée sur tous les appareils communiquant avec le backbone KNX IP.

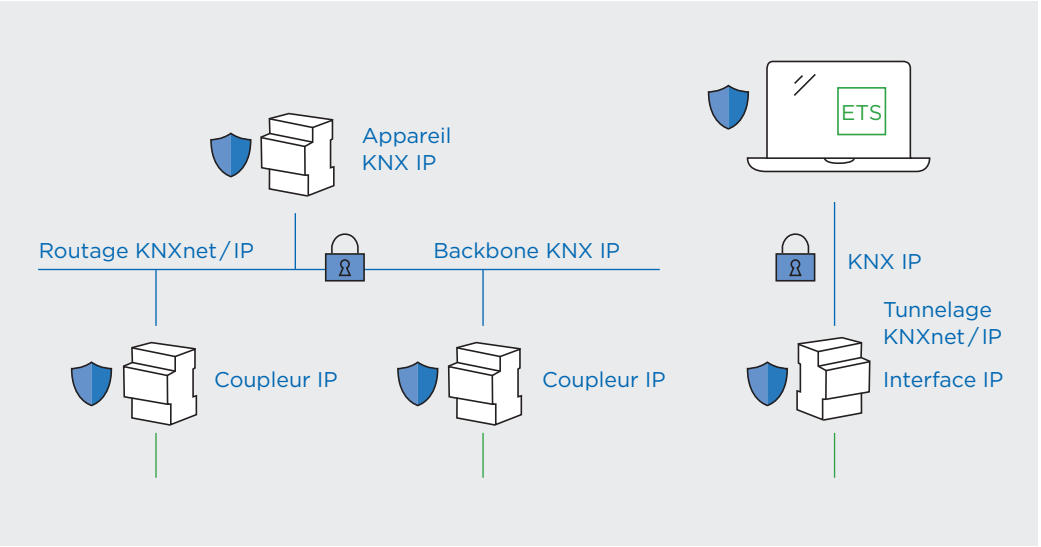


Fig. 4.3-1 KNX IP Secure : sur le réseau IP (routage KNXnet/IP et tunnelage KNXnet/IP), les télégrammes KNX sont chiffrés et protégés. Ils ne sont pas accessibles ni manipulables par des tiers non autorisés sur le réseau.

4.3.1 Routeur KNX IP

Un routeur KNX IP (voir fig. 4.3-2) se compose d'une connexion vers KNX TP menant aux composants KNX TP via les bornes rouge et noire, et d'une connexion vers la ligne de niveau supérieur, réalisée via IP (connecteur RJ-45).

Au niveau IP, le routeur KNX IP possède une fonction de routage basée sur le routage KNXnet / IP et plusieurs interfaces basées sur le tunnelage KNXnet / IP. Pour être bien protégé, KNX Secure doit obligatoirement être activé sur le routeur et sur toutes les interfaces.

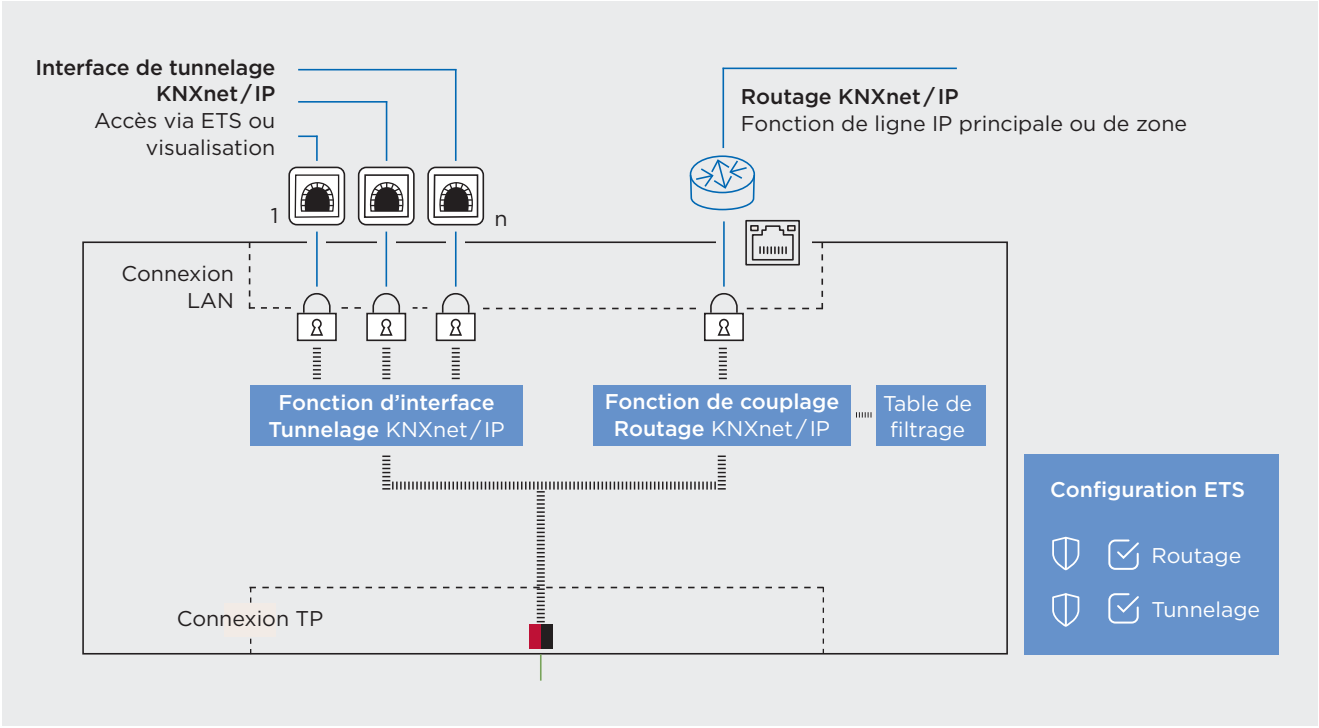


Fig. 4.3-2 Structure d'un routeur KNX IP avec ses trois interfaces : tunnelage KNXnet / IP, routage KNXnet / IP et KNX Twisted Pair (TP).

Secure pour la fonction de routage (routage KNXnet / IP)
Les télégrammes de routage KNX IP sont chiffrés, et ils ne peuvent être lus que par des appareils soit équipés de la clé backbone d'ETS, soit configurés avec ou sous le même projet ETS. ETS permet également d'accéder aux installations KNX via le routage KNXnet / IP. Si Secure est activé, l'accès n'est possible que via le projet ETS dans lequel le routeur a été configuré.

Secure pour la fonction des interfaces IP (tunnelage KNXnet / IP)
Selon le fabricant, les routeurs KNX IP peuvent avoir plusieurs interfaces de tunnelage KNXnet / IP pouvant être utilisées pour les visualisations ou la communication avec d'autres installations. Ce n'est que si ces interfaces de tunneling KNXnet/IP sont également configurées sur KNX Secure dans ETS que la communication IP est entièrement sécurisée. L'accès au système n'est alors possible que dans le projet ETS correspondant.

4.3.2 Interfaces KNX IP

Les interfaces KNX IP sont utilisées pour les visualisations ou la communication avec d'autres installations. Elles servent également d'interfaces avec ETS.

Secure pour interfaces KNX IP
Les interfaces de tunnelage KNXnet/IP doivent être activées sur KNX Secure dans ETS. L'accès via IP au système KNX n'est alors possible que via le projet ETS ou un appareil (visualisation, etc.) connaissant le code d'authentification de l'interface correspondante.

4.4 Topologies KNX Secure

4.4.1 KNX Data Secure dans l'ensemble du projet

Bien entendu, grâce à la technologie KNX Secure mise en place de bout en bout, les installations KNX Secure peuvent aussi être réalisées sur des installations KNX TP complètes avec plusieurs zones et lignes. Ici également, il est possible de gérer des appareils sécurisés et non sécurisés dans la même topologie KNX.

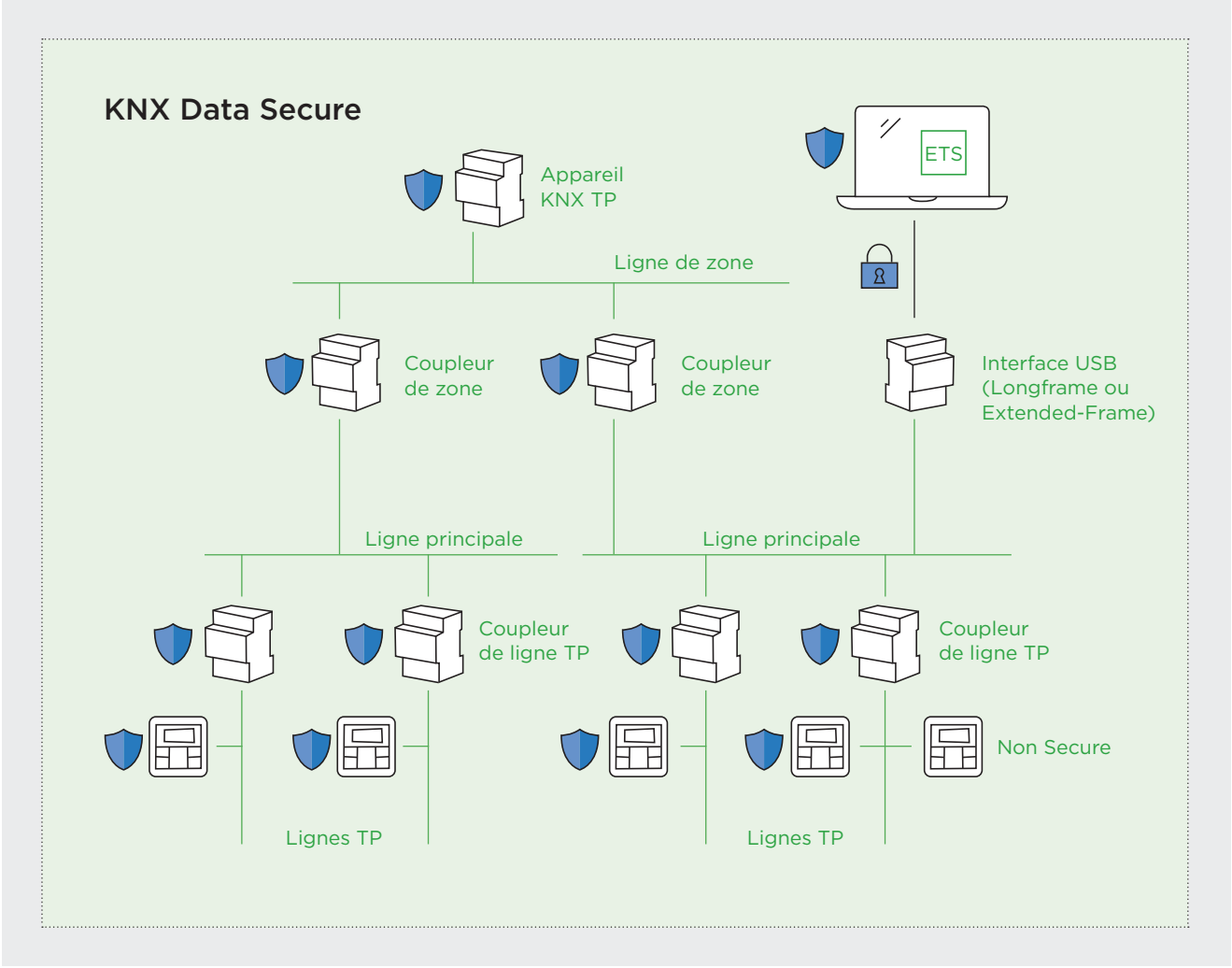


Fig. 4.4-1 Projet KNX Data Secure sur plusieurs lignes et zones

4.4.2 Combinaison KNX Data Secure - KNX IP Secure

Cette application est appelée à devenir rapidement la norme, notamment dans les grands projets. KNX Data Secure et KNX IP Secure peuvent être utilisés ensemble dans des topologies IP / TP mixtes. Grâce à cette possibilité, les zones critiques ou les applications d'automatisation des bâtiments peuvent être très bien protégées, qu'elles soient intégrées via IP, Twisted Pair ou KNX radio.

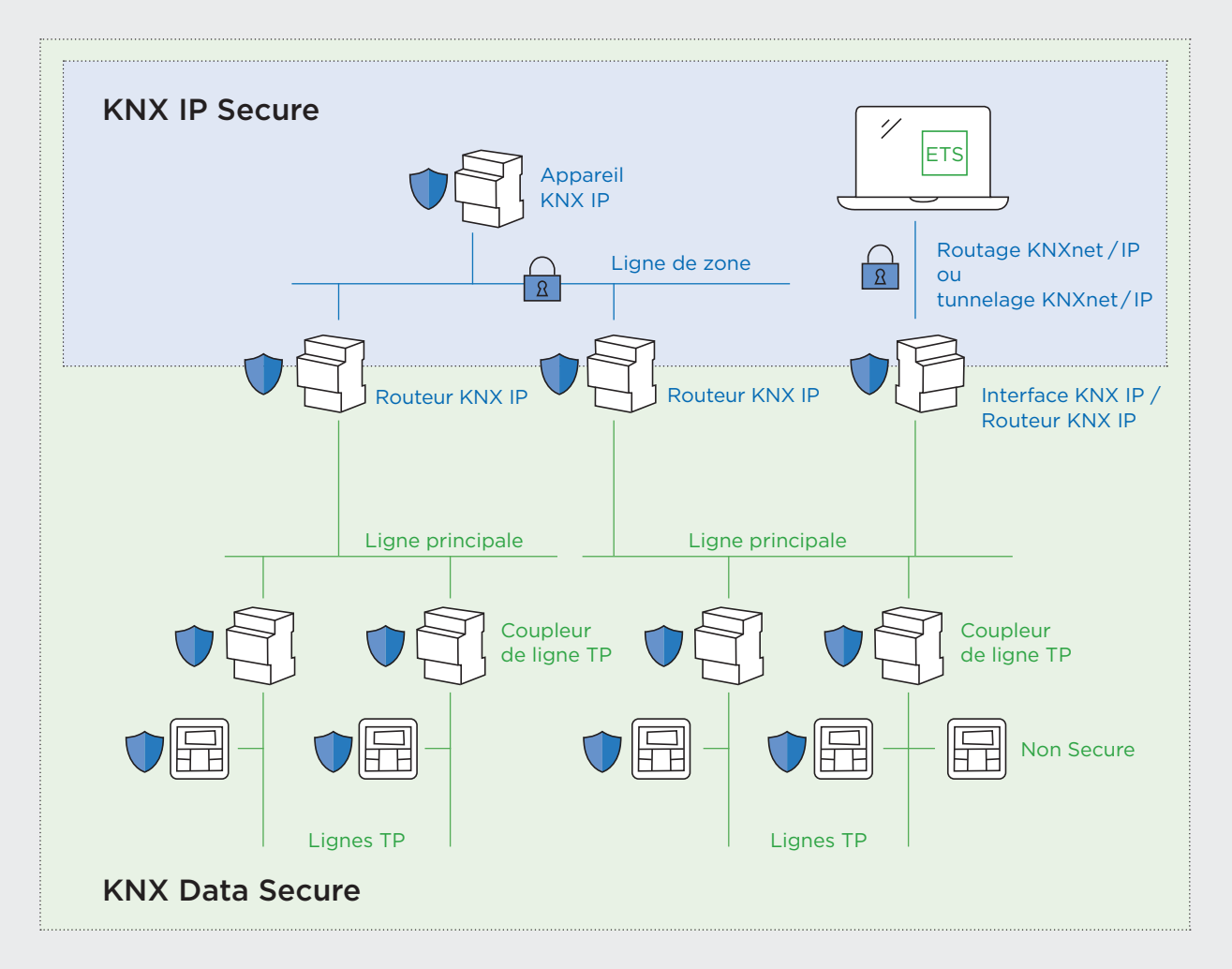


Fig. 4.4-2 KNX Data Secure et KNX IP Secure dans un projet

4.5 Termes essentiels et leur définition

Termes importants dans l'environnement KNX Data Secure et leur signification

Mot de passe de projet
Afin de pouvoir programmer un appareil Secure en mode Secure activé (ou d'activer ou de désactiver le mode Secure sur l'appareil Secure), la « Mise en service sécurisée » doit être activée dans le projet ETS. Cela n'est possible que si un mot de passe de projet a été attribué au projet ETS au préalable.

Certificat de l'appareil
Code QR figurant sur l'appareil Secure. Contient la « clé de configuration d'appareil départ usine » (Factory Default Setup Key, FDSK) ainsi que le numéro de série de l'appareil.

Factory Default Setup Key (FDSK)
La Factory Default Setup Key (FDSK) de chaque appareil compatible KNX Data Secure est unique au monde et est utilisée pour sa mise en service initiale. Sa longueur est de 128 bits et elle s'entend comme la clé de configuration d'appareil départ usine d'un appareil compatible KNX Data Secure. La FDSK figure sur le certificat de l'appareil.

Numéro de série
Le numéro de série est le numéro d'identification du fabricant dont la longueur est de 6 octets. Il sert à identifier les appareils KNX de manière univoque. Il est défini individuellement en cours de production (une fois dans le monde pour chaque fabricant) et il est programmé sur l'appareil sans être modifiable.

Clé du périphérique, Toolkey
La Toolkey est utilisée exclusivement par ETS pour programmer un appareil compatible KNX Data Secure. Sa longueur est également de 128 bits, elle est unique par appareil dans un projet et elle remplace la FDSK dès la mise en service initiale. Ensuite, ETS utilise la Toolkey pour tout processus de programmation en mode sécurisé.

Clé de groupe / Clé d'exécution
Afin de sécuriser l'exécution via les adresses de groupes par Data Secure, des clés de groupes (Group Keys) sont utilisées pour le chiffrement et le déchiffrement des télégrammes de groupes. Chaque adresse de groupe possède sa propre clé d'exécution (clé AES) de 128 bits dans un projet ETS dès lors que l'adresse de communication sécurisée est utilisée entre les appareils KNX Data Secure. Un code d'autorisation intégré aux télégrammes assure que seuls les appareils du groupe configurés en conséquence puissent échanger des données.

Clé backbone
Une fois que l'IP du média backbone d'un projet ETS a été définie et la sécurité du backbone IP activée, ETS génère la clé backbone du projet. ETS charge ensuite cette clé sur le coupleur KNX IP Secure et les interfaces KNX IP Secure du projet (si celles-ci s'appuient sur une communication sécurisée ou que la mise en service sécurisée y est activée). La backbone key et le statut d'activation de la sécurisation des appareils Secure et des canaux de tunnelage peuvent être consultés dans le rapport « Sécurité du projet ».

Master Reset
Fonction de réinitialisation d'un appareil compatible KNX Secure dans un état fonctionnel défini par le fabricant. La réalisation d'un Master Reset entraîne l'effacement de tous les paramètres utilisateur et la réactivation de la clé initiale (FDSK).

4.6 Synthèse KNX Secure

Pour les intégrateur-rice-s de système KNX, KNX Secure n'a en fait rien de très nouveau, mais est une extension de la technologie KNX existante. KNX Secure inclut des technologies de gestion sécurisée de systèmes KNX via Twisted Pair (câble à 2 conducteurs), radio ou réseaux IP. Ces technologies sécurisent l'automatisation des locaux et des bâtiments contre les cyberattaques – soit toute l'installation ou uniquement certaines applications spécifiques.

Dans un système KNX (projet), des appareils KNX Secure et des appareils KNX non Secure peuvent fonctionner en parallèle. À leur tour, les adresses de groupes par lesquelles les appareils communiquent ensemble dans une installation peuvent également être Secure ou non Secure. À partir des caractéristiques du projet et en accord avec la maîtrise d'ouvrage, les intégrateurs (planificateurs) définissent les groupes d'adresses KNX et appareils KNX devant être Secure et ceux devant demeurer conventionnels (non Secure).

KNX Secure empêche :

- que les paramètres et réglages des appareils configurés KNX Secure (capteurs, actionneurs, etc.) soient modifiés à l'aide d'un logiciel ETS « externe au projet ». L'accès à ces appareils n'est possible qu'avec le projet ETS « d'origine » dans lequel sont enregistrées les clés des périphériques (Toolkeys) générées par ETS à partir de la clé FDSK.
- que les télégrammes KNX sécurisés via KNX Secure puissent être lus ou envoyés sur le bus manuellement ou par des tiers. Les adresses de groupes non sécurisées d'un système KNX peuvent être enregistrées et manipulées même si certaines parties du système sont Secure (à l'exception de KNX IP Secure).
- qu'avec KNX IP Secure, les télégrammes KNX IP sans backbone ni clé de projet ne soient interceptés ou manipulés. L'ensemble de la communication KNX via IP est chiffrée AES-128 et horodatée.

Les coupleurs de segments peuvent aider les intégrateurs à structurer la topologie d'un projet en fonction de KNX Secure. Ils peuvent s'avérer très utiles pour subdiviser le trafic de télégrammes en plusieurs zones.

Conseils

Dans une installation KNX, il est possible d'utiliser KNX IP Secure et KNX Data Secure en parallèle.

Dans une installation KNX, les applications sécurisées et non sécurisées peuvent être utilisées en parallèle. Tous les appareils ne doivent pas forcément être sécurisés.

Lorsqu'une installation compte plusieurs routeurs IP et que l'un d'entre eux est commutés sur KNX IP Secure, tous les autres doivent également être commutés sur IP Secure.

Un objet de communication d'un appareil qui est déjà connecté à une adresse de groupe sécurisée ne peut pas être connecté à une autre adresse de groupe non sécurisée. En l'absence de proxys de sécurité sur l'installation, cette règle s'applique à l'ensemble de l'installation. En présence d'un proxy de sécurité, cette règle s'applique aux domaines de sécurité pertinents.

Au sein des mêmes domaines de sécurité, une adresse de groupe doit être soit simple, soit sécurisée pour tous les objets de groupe connectés. Lorsqu'un appareil est non Secure, mais que la sécurisation est incontournable, cet appareil KNX non sécurisé doit être remplacé par un appareil KNX Secure.

Les nouvelles fonctions de sécurisation peuvent être intégrées sans problème même aux installations existantes. KNX Secure est une extension ayant une compatibilité ascendante : les appareils existants ignorent les messages KNX Secure.

4.7 Perspectives KNX IoT

KNX IoT est utilisé exclusivement via des réseaux IP et emploie le protocole TLS (Transport Layer Security) pour sécuriser le flux de données. Selon l'API utilisée, l'Ethernet, le WLAN ou le Thread sont les possibilités à disposition. Elles permettent un chiffrement de bout en bout de la communication entre un capteur et le cloud.

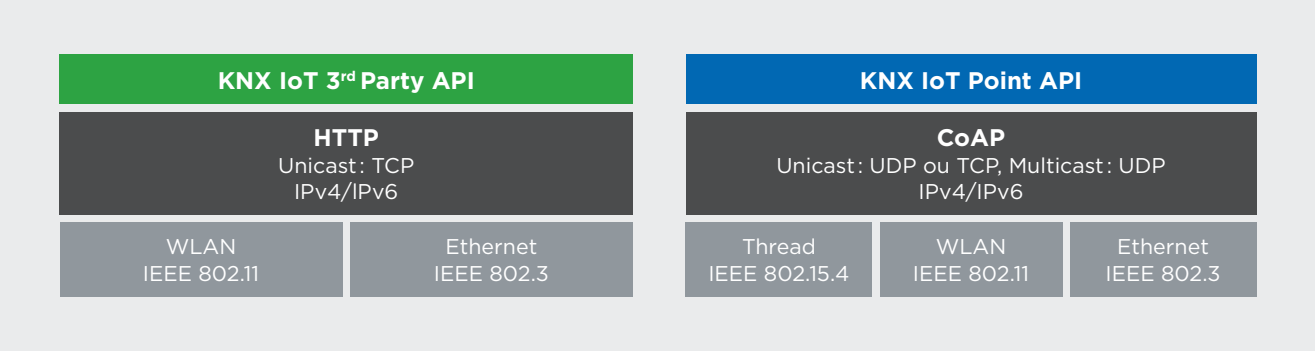


Fig. 4.7-1 Les deux variantes de KNX IoT (3rd Party API et Point API) s'appuient exclusivement sur des réseaux IP standard dans le respect des normes IEEE et IETF. De quoi exclure pratiquement tous les problèmes avec les services informatiques des clients.

Conseils

Une attention particulière doit être accordée aux installations dans les espaces publics, c'est-à-dire où les personnes peuvent se déplacer sans surveillance. À ces endroits, il est également possible d'attaquer les systèmes KNX câblés.

Si les installations KNX communiquent sans fil, nous recommandons l'emploi de KNX Secure.

Si une installation est connectée à Internet, l'utilisation d'un tunnel VPN pour y accéder via Internet est OBLIGATOIRE. En présence d'une interface de tunnelage KNX Secure, il faut veiller à utiliser des mots de passe forts comme recommandés par ETS et à ne pas les remplacer par des mots de passe personnels faibles.

En présence d'un backbone KNX IP et d'autres réseaux IP, il faut utiliser une séparation du réseau VLAN. Le réseau KNX IP et les autres réseaux ne peuvent communiquer entre eux que via un pare-feu adapté.

Les appareils de l'automatisation des bâtiments doivent être «IT-friendly», et par exemple prendre en charge l'attribution d'adresses IP (DHCP) dynamiques et fixes et la résolution de noms (DNS). Les broadcasts pour la communication sont interdits.

5 La cybersécurité dans les bâtiments et la technique des bâtiments

5.1 Fondements de la cybersécurité

L'Internet mis en place dans les années 60 était certes insensible aux pannes, mais on ne s'est jamais soucié de la sécurité des serveurs et des réseaux. Une aubaine pour la cybercriminalité. Elle est ensuite devenue un commerce juteux qui, sur le plan économique, n'est guère différent de l'économie légale : avec des fournisseurs, des intermédiaires et un « service clientèle » opérationnel. Aujourd'hui, il n'est pas nécessaire d'être un hacker pour lancer une attaque sur une entreprise ou un smart building. Les bons contacts et une bonne dose d'énergie criminelle suffisent. Comme le prouve d'ailleurs le nombre croissant des brèches de sécurité. La question n'est plus de savoir si l'on va en être victime, mais quand cela va se produire et avec quelles conséquences. Raison pour laquelle ces attaques, qui se produiront inévitablement, doivent être identifiées le plus rapidement possible et contrecarrées par des mesures.

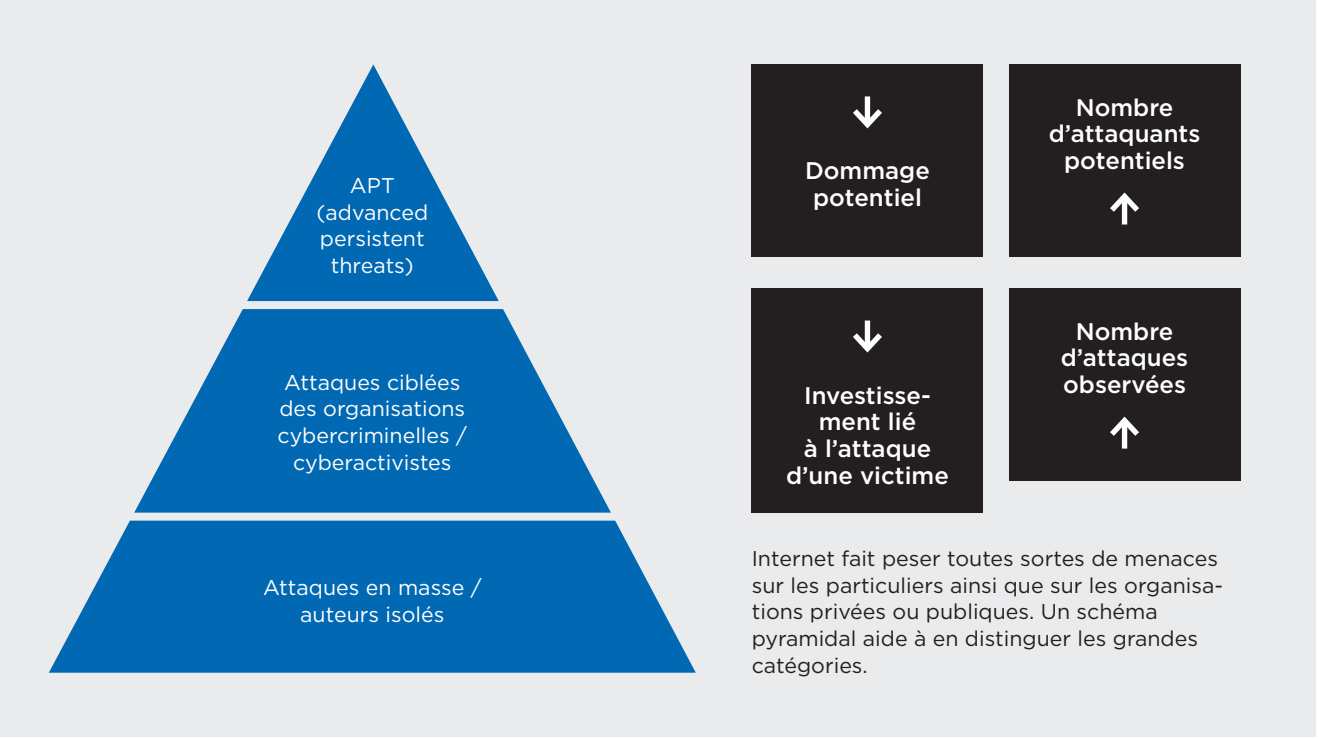
La cybersécurité, en tant que discipline de l'informatique, couvre tous les volets de la sécurité et des risques liés aux processus numériques. Les mesures, concepts et directives sont développés et mis en œuvre pour que les appareils et réseaux connectés à Internet soient protégés contre tout accès non autorisé, vol de données et manipulations de tout type.

Une cyberattaque est une attaque hostile menée sur un réseau IP tiers et les périphériques qui y sont connectés. Sa finalité est différente selon les cas – de plus en plus, il s'agit d'attaques par ransomware, où les données sont chiffrées par le pirate et ne sont libérées qu'en échange d'une rançon. Il existe également des attaques motivées par des raisons politiques, liées au vol de données ou à la manipulation de terminaux. Très souvent, les hackers s'installent sur le réseau pendant des semaines sans se faire détecter pour ne pas révéler leurs intentions..

Les smart buildings sont bien entendu attrayants, car on peut y attaquer plusieurs entreprises à la fois, optimisant la rentabilité d'une attaque. Les installations OT sont également souvent visées, par exemple pour neutraliser un réseau électrique ou une ligne de production.

5.1.1 Formes de menaces

Les attaques sont menées via des points vulnérables sur le réseau, les applications ou les terminaux. Une méthode bien plus simple consiste néanmoins à dissimuler des logiciels malveillants dans des e-mails frauduleux ou des liens alléchants, sur lesquels on cliquera volontiers, autorisant l'accès des hackers à notre système. Ladite ingénierie sociale fonctionne même par téléphone, par exemple lorsque le pirate manipule le personnel pour qu'il lui révèle son mot de passe.



Internet fait peser toutes sortes de menaces sur les particuliers ainsi que sur les organisations privées ou publiques. Un schéma pyramidal aide à en distinguer les grandes catégories.

Fig. 5.1-1 Représentation simplifiée de la pyramide des menaces selon SANS, RecordedFuture

Les frontières entre les catégories d'attaque sont perméables.

- **APT :** attaques pouvant occasionner des dommages élevés, souvent préparées de longue date par des acteur étatiques. Elles requièrent d'énormes ressources en arrière-plan.
- **Attaques ciblées :** les mobiles des cybercriminels sont avant tout financiers, et ils attaquent des cibles rentables. Ils usent souvent de moyens tels que le chantage et le vol de données..
- **Auteurs isolés :** il n'y a pas besoin d'être un hacker pour mener une attaque. Les attaques en masse sont lancées à l'aide d'une prestation « Crimeware as a Service » moyennant un hackerware en modèle de location. Ensuite, les agresseurs et les fournisseurs d'accès se partagent les rançons. Les attaques peuvent également être motivées par des raisons politiques (activistes) ou être des tests pour prouver son courage

5.2 Nouveaux concepts de sécurité

Depuis les débuts des réseaux IP, il est recommandé de s'équiper de pare-feu (appareils opérant un blocage ciblé du trafic réseau entrant) et de logiciels antivirus. Cela ne suffit plus : dans l'univers IP complexe d'aujourd'hui, les clouds privés et publics forment un multicloud et le personnel travaille de plus en plus souvent en dehors du réseau de l'entreprise, par exemple en télétravail, ce qui étend considérablement le périmètre du réseau et le soumet à des modifications constantes.

L'approche doit donc être celle de la « Security by Design » dans tous les domaines des technologies de l'information, du développement des logiciels à l'architecture IT.
Les données (informations) doivent être protégées de sorte que seules des personnes, ordinateurs ou machines autorisés puissent y avoir accès. L'identification, l'autorisation et le chiffrement du transfert de données sont décisifs. Pour résumer : celui qui communique doit toujours être sûr de l'authenticité de son correspondant.

Le modèle de sécurité Zero Trust est une approche de ce type. Plus besoin de mot de passe, car désormais le système ne fait confiance à aucun terminal ni utilisateur. Chaque connexion de données est analysée et approuvée. Une approche de cybersécurité efficace et globale crée des liens entre les êtres humains, processus, réseaux informatiques et autres technologies.

Conseils généraux de sécurité

Veillez à ce que vos logiciels soient toujours à jour. Y compris les systèmes d'exploitation de vos terminaux..

Si vous utilisez des mots de passe : utilisez des mots de passe longs contenant des caractères spéciaux et des chiffres. Pour cela, prenez les caractères d'une phrase mnémotechnique répondant à une certaine séquence. Si possible, activez l'authentification multifacteur. Utilisez un gestionnaire de mots de passe (p. ex. celui du navigateur) et n'utilisez jamais le même mot de passe pour différents services informatiques.

Sur l'ordinateur, ne travaillez jamais en mode administrateur.

Ne faites confiance à aucun message inattendu vous parvenant par tel ou tel canal. Vérifiez les liens, n'ouvrez les pièces jointes que si vous êtes sûrs de leur authenticité ou après les avoir analysées avec un antivirus.

Pour obtenir des logiciels, ne faites confiance qu'aux sources officielles.

Sur chaque nouvel appareil connecté au réseau, modifiez le mot de passe par défaut du fabricant.

5.2.1 Informations plus détaillées et liens

- **Centre national pour la cybersécurité :** www.ncsc.admin.ch
- **Swiss Cyberdefense DNA :** www.scd-dna.ch
- **MITRE ATT&CK :** tactiques, techniques et procédures employées dans les cyberattaques www.attack.mitre.org
- **Base de données de logiciels malveillants :** www.attack.mitre.org/software
- **Cisco Cybersecurity :** www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- **Cybersecurity Framework (NIST) :** www.nist.gov/cyberframework
- **Cisco Talos Intelligence Group :** www.talosintelligence.com
- **Site web de recherche des entrées ouvertes :** www.shodan.io

5.3 Le smart building en tant que cloud privé

La technique des bâtiments devient compatible IP et est désormais connectée aux réseaux, y compris à Internet. Ce qui l'expose à de nouvelles problématiques de sécurité dans les bâtiments intelligents. Un nouvel acteur entre en jeu : les professionnels de l'informatique connaissent les dangers au niveau des applications et des réseaux.

Les maisons d'habitation, les ouvrages professionnels et industriels sont rendus intelligents grâce à l'automatisation, à des capteurs et à l'intelligence artificielle. Pour ainsi dire, Industrie 4.0 signifie commander des lignes de production entières sur un smartphone. À travers les données, l'Internet of Things (IoT) génère des valeurs ajoutées et des gains de performance dans l'économie. Autrement dit, l'expansion des approches réseau propriétaires et des technologies basées sur des réseaux IP va de pair avec celle d'Internet.

Soudain, les maisons deviennent vulnérables. Les cambrioleurs n'ont plus besoin de briser une vitre, il leur suffit de localiser les points faibles du réseau et de les exploiter. Lorsque soudain le régulateur du chauffage s'ouvre à fond, que le téléviseur vous espionne en secret ou que le lave-linge se met en marche, cela peut a priori paraître anodin. Mais si en réalité l'objectif du hacker était différent ? Comme par exemple de contrôler les domaines et données les plus sensibles ? On peut ainsi imaginer que le méfait soit commis via Alexa & Cie., par exemple pour ouvrir la serrure intelligente d'une porte et faciliter l'entrée des cambrioleurs dans le bâtiment.

5.3.1 Le danger venant de l'environnement IP est réel

D'après les études de Cisco, 75 milliards d'appareils Internet of Things seront installés d'ici 2025, souvent sans approche axée sur la sécurité. Le degré d'intelligence des maisons, bureaux et appartements étant en augmentation, de plus en plus d'appareils communiquent sur le réseau via IP et via le cloud. Les compteurs d'eau, de gaz et d'électricité, les luminaires, les centrales photovoltaïques, les ventilateurs, les ascenseurs, les contrôles d'accès, etc. Progressivement, on assiste également à l'expansion des systèmes de sécurité, qui analysent par exemple le taux d'exploitation des locaux et les distances via la technologie collaborative. Ils génèrent des données extrêmement précieuses permettant aux criminels de mettre à exécution leurs plans les plus funestes.

Souvent, les bâtiments ont plusieurs dizaines d'années et ont été équipés au fur et à mesure, créant un mix de technologies anciennes et nouvelles, souvent sans planification de la sécurité de bout en bout. Les services informatiques, qui pourraient apporter leurs connaissances sur les flux de données et les risques de cybersécurité, sont rarement impliqués. Les questions suivantes se posent alors : qui contrôle les installations, qui installe les dernières mises à jour sur les appareils et sur les éléments de commande, si tant est que des patches soient disponibles ? Il suffit d'un seul maillon faible dans la chaîne, un capteur qui n'est plus fabriqué et ne reçoit pas de mises à jour, pour que le hacker ait un pied dans le bâtiment.

Un ouvrage équipé de composants d'automatisation est un système hétérogène complexe basé sur des standards, des technologies et des processus différents impliquant de nombreuses dépendances. Les éléments de l'automatisation des bâtiments sont extrêmement intéressants pour les agresseurs. La moindre faille peut entraîner une catastrophe – car aucun chef d'entreprise n'est à l'abri d'un chantage derrière une passoire numérique.

L'automatisation des bâtiments doit donc être considérée comme un élément « vital » d'un ouvrage et être protégée en tant que telle. Pour compliquer le tout, la conception de chaque bâtiment est unique sur les plans architectural et technique. Les composants

informatiques essentiels sont souvent installés dans un placard à balais ou sous un bureau – ce qui n'a rien à voir avec un centre de calculs équipé des mesures de sécurité les plus sévères visant à protéger physiquement l'infrastructure.

5.3.2 Réflexions fondamentales sous l'angle de l'informatique

La mise en place du service d'automatisation est décisive, tout comme l'évaluation de la sécurité technique de l'installation. Comme pratiquement partout, la question est de savoir si les processus informatiques ne se déroulent que dans le bâtiment ou si l'on a recours à des ressources sur un ou plusieurs clouds. Le problème se pose souvent à ce niveau : les intégrateurs et les fabricants ne se soucient guère de cette question, car un bâtiment automatisé peut en principe fonctionner sans service informatique. La sécurité informatique de l'automatisation des bâtiments est donc reléguée au second plan.

Mais lorsque les bâtiments deviennent plus qu'intelligents, l'informatique et l'intelligence artificielle du cloud sont effectivement là : conçus intelligemment, les réseaux s'auto-surveillent et identifient les anomalies. De plus, la visibilité sur le réseau est un facteur de sécurité : les bâtiments automatisés et leurs protocoles non informatiques sont intégrés au cloud hybride des entreprises en tant que cloud privé, surveillés à l'aide d'outils visant une transparence totale du réseau. Lorsque l'on aborde l'étude d'un bâtiment intelligent, ici un nouveau centre de calcul, il faut être conscient du fait que la mise en place d'un cloud privé s'avère incontournable.

Et qu'il ne s'agit pas d'une mesure accessoire. Cela passe par une nouvelle approche de l'étude et de nouvelles normes de sécurité au niveau de la technologie, de l'organisation et des process. L'évolution de la sécurité technique dans les bâtiments emboîte le pas aux développements IT et OT (technologie d'exploitation). Dans les deux domaines, nous faisons aujourd'hui appel aux normes de sécurité les plus élevées et à des systèmes automatisés de contrôle des accès et des flux de données. À présent, l'heure est venue d'intégrer les bâtiments intelligents, de créer des systèmes convergents protégés en toute transparence et d'une manière centralisée, en l'occurrence par des technologies développées et appliquées par des professionnels qualifiés. De quoi donner un sens à l'économie numérisée, dans laquelle les personnes doivent être protégées quel que soit leur lieu de travail physique. D'ailleurs, dans les environnements de travail hybrides du « new normal », les bâtiments devraient veiller par nature à la protection des personnes dans les processus d'information et de travail.

5.4 Actions recommandées

La sécurisation des bâtiments intelligents contre les risques liés à l'environnement IP exige une étroite collaboration entre les professionnels de l'automatisation des bâtiments et de l'informatique. Ensemble, ils créent un cloud privé et un réseau accessible dans des conditions très strictes, composé de plusieurs réseaux partiels. Ils doivent contrôler les flux de données, analyser les anomalies et appliquer en continu les mises à jour et les correctifs.

La coopération entre fabricants, intégrateur-rice-s et exploitants est requise. Celle-ci doit commencer par une évaluation complète, suivie d'une analyse des données et des risques.

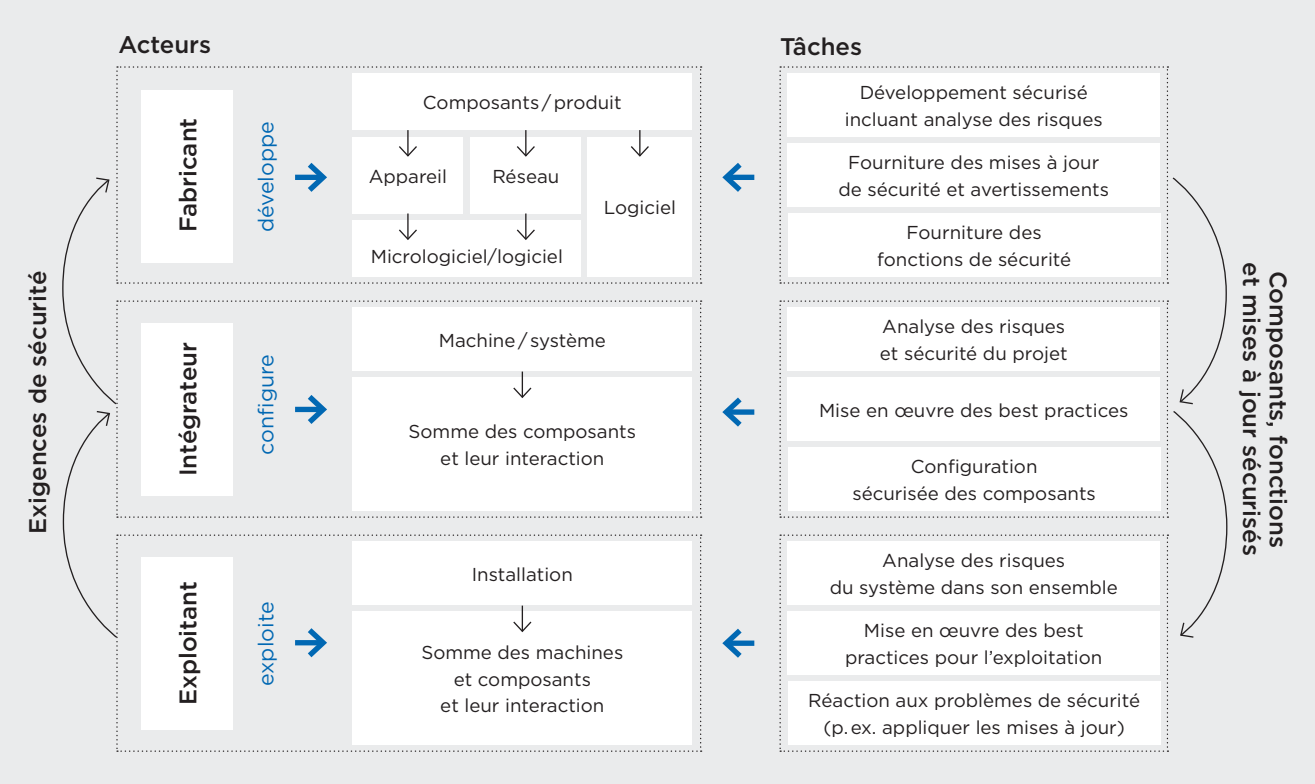


Fig. 5.4-1 Les exigences de sécurité au sein du bâtiment doivent être remplies par trois acteurs qui travaillent main dans la main et partagent leur savoir-faire.

5.4.1 Soutien apporté au service informatique

Seul-e-s les expert-e-s en informatique possèdent le savoir-faire et l'expérience de l'exploitation sécurisée de réseaux IP et de la gestion d'infrastructures multicloud complexes, c'est-à-dire de clouds interconnectés ayant un accès public ou privé. Les environnements informatiques modernes sont basés sur le cloud; les frontières entre le stockage local et le stockage sur le cloud s'estompent. Une évaluation exhaustive révèle les propriétés d'un bâtiment, ainsi que celles de ses processus et fonctions intelligentes. Elle permet d'en dériver les mesures adéquates pour une exploitation sûre.

Enfin, les services informatiques doivent considérer l'automatisation des bâtiments au cœur de leur mission originelle. L'automatisation doit être axée sur des normes.

5.4.2 Réseaux sécurisés et flexibles

Les réseaux modernes sont gérés par des logiciels et ils sont segmentés. Ils incluent des sites internes, mais également externes. Ils peuvent être basés sur le Wi-Fi, la 5G et l'Ethernet, en local, sur le campus ou dans les réseaux étendus.

Un contrôleur commande toutes les fonctions et régule le flux de données sur tous les segments du réseau. Ces réseaux partiels forment des zones protégées et bloquent les agresseurs assez longtemps pour qu'ils soient découverts à temps. Les actifs, terminaux et flux de communication doivent être identifiés et classés, et le réseau segmenté en conséquence. À titre d'exemple, les appareils d'automatisation ne doivent autoriser aucun accès aux serveurs internes.

Tous les accès doivent être surveillés en temps réel. Avec l'approche Zero Trust, on sait toujours clairement qui a accès à quoi sur quel terminal du bâtiment. L'intelligence artificielle sur le réseau reconnaît les modifications dans le trafic ou dans les patterns et tire la sonnette d'alarme.

5.4.3 Concept de cybersécurité

Toute installation future doit être examinée avec un expert en cybersécurité. Une infrastructure standardisée et largement automatisée facilite grandement la surveillance, permettant au service informatique de se concentrer sur son cœur de métier, d'identifier par exemple les threads et de les éliminer à temps avant qu'ils ne provoquent des dommages.

Les principes de l'informatique sont valables dans le smart building : les passerelles réseau doivent être sécurisées, les patches et les terminaux gérés. Un concept opérationnel ne va pas non plus sans gestion intelligente des données, dans laquelle les données productives et donc critiques sont stockées ailleurs (backup) en temps réel et peuvent être récupérées rapidement en cas d'urgence.

5.4.4 Former les personnes aux bâtiments intelligents

L'informatique va de pair avec le principe d'une culture de la sécurité vécue, car plus de 80 % de toutes les brèches de sécurité ont une origine humaine. On révèle son mot de passe, on clique sur n'importe quel lien ou on ouvre les pièces jointes – une aubaine pour les cybercriminels, qui accèdent au réseau par des e-mails contenant des logiciels malveillants. Par conséquent, les personnes occupant un smart building doivent prendre conscience du fait qu'elles évoluent dans un environnement sensible en matière de sécurité. Comme dans les exercices de lutte contre l'incendie, elles doivent connaître les risques actuels et le niveau de menace en général.

5.4.5 Les normes en tant que fondement

Pour que l'informatique soit sécurisée dans le bâtiment, les normes en vigueur doivent servir de base au développement de concepts de protection. L'ISO / IEC Joint Technical Committee (JTC1) développe la famille de normes ISO / IEC 27000 pour les systèmes informatiques. L'IEC Technical Committee 65 (TC 65) publie la norme IEC 62443 pour les systèmes OT.

Ces deux normes, associées aux certifications de conformité et tests de vérification, constituent les piliers essentiels d'un programme de cybersécurité réussi et complet pour les bâtiments intelligents.

5.5 Normes

Certaines normes et guides sont essentiels dans la sécurité dans les smart buildings. Ils sont à la base de concepts de sécurité personnalisés.

- **Guide de vérification de la cybersécurité OT :** www.isaca.de
- **La sécurité informatique dans l'automatisation des bâtiments (VDMA 24774) :** www.vdma.org

Normes de référence

- **IEC 62443 Security Levels :** les tâches relatives à la sécurité portent sur tout le cycle de vie d'une installation. La série internationale de normes sur les « Réseaux de communication industriels – Sécurité informatique des réseaux et des systèmes » décrit les aspects techniques et les aspects liés aux processus de la sécurité informatique industrielle.
- **ISO / IEC 27001 :** système de management de la sécurité de l'information avec une personne responsable chargée de la mise en œuvre des processus internes à l'entreprise.
- **Série ISO / IEC 2700x :** les normes 0 à 5 décrivent tous les éléments de la sécurité de l'information.
- **ISO / IEC 15408 :** évaluation et certification des produits IT.
- **Norme ETSI EN 303645 :** la nouvelle norme de la sécurité IoT définit la cybersécurité sur l'Internet des Objets (p. ex. capteurs).

5.6 Types de chiffrement

Le chiffrement protège la confidentialité, l'authenticité et l'intégrité des données. Le chiffrement est basé sur une méthode de conversion d'un texte en clair en un texte incompréhensible dépendant d'une clé. Ce texte ne sera lisible que si la clé secrète est utilisée. Pour cela, il faudra utiliser un logiciel ou encore un matériel spécifique. Il existe plusieurs types de chiffrement : symétrique, asymétrique ou hybride.

Les procédés de chiffrement symétriques sont efficaces et rapides. La même clé est utilisée pour le chiffrement et le déchiffrement. Les procédés asymétriques emploient des paires de clés composées d'une Public Key (publique) et d'une Private Key. Les deux clés sont mathématiquement liées. Les messages chiffrés avec la clé publique ne peuvent être déchiffrés qu'avec la clé privée du destinataire. Les procédés hybrides associent les deux méthodes. Le premier chiffrage s'effectue avec une clé choisie au hasard et valable une seule fois.

Les objectifs de protection courants sont les suivants.
Lors de l'envoi d'un message, il faut s'assurer :

- qu'il ne puisse être lu que par une personne en particulier
- qu'il provienne effectivement du prétendu expéditeur
- et qu'il ne soit pas modifié au cours du transport.

Le chiffrement est donc un facteur important d'un concept intégral de sécurité dans les technologies de l'information et les réseaux : le transport des données est chiffré, tout comme l'authentification entre les « interlocuteurs » (homme, logiciel, machine, terminal).

Le chiffrement de bout en bout est le chiffrement complet du flux de données passant par plusieurs stations intermédiaires et réseaux d'un terminal à l'autre. Il s'agit du cas idéal d'un service informatique sûr.

Les réseaux IP sont protégés par les mécanismes de sécurité suivants :

- **AES (Advanced Encryption Standard) :** utilisant des clés de 128, 192 ou 256 bits de longueur, la méthode AES est considérée comme très sûre et très performante. Avec une longueur de 256 bits, elle est pratiquement inviolable.
- **TLS (Transport Layer Security) :** navigation sûre via https:// et e-mails sécurisés via smtps. Ce protocole utilise le chiffrement asymétrique avec AES.
- **WPA 2/3 :** sécurisation des réseaux mobiles via Wi-Fi 5 ou 6 basée sur la méthode AES.
- **SHA :** famille d'algorithmes utilisée pour prouver l'authenticité des appareils (sécurité des certificats).
- **VPN (Virtual Private Network) :** les connexions réseau privées chiffrées peuvent être mises en place de plusieurs manières. Elles forment un tunnel de données virtuel à travers plusieurs réseaux. Le plus souvent, elles utilisent le protocole IPsec, voire le protocole TLS.
- **IPsec (Internet Protocol Security) :** suite de protocoles de communication sécurisée sur des réseaux IP non sécurisés. Elle est basée sur différents procédés de chiffrement et algorithmes.

6 Informations sur la planification de projets d'automatisation des bâtiments sécurisés

6.1 Connaissances techniques sur l'IP et coopération

L'optimisation du niveau de sécurité dans un bâtiment intelligent exige une approche globale et coordonnée. Ce document décrit les principaux points à prendre en considération.

La sécurité KNX inclut également la sécurité IP, à savoir la sécurisation du flux de données venant de l'extérieur du bâtiment et à l'intérieur de celui-ci. En d'autres termes : le smart building n'est pas une île KNX dans un vaste océan de données. Il est exposé aux mêmes intempéries et tempêtes que tout système ou organisation sur Internet.

Techniquement parlant : on a un cloud privé qui peut même devenir partie intégrante d'un multicloud plus grand.

Pour les installateur-rice-s, la mise en place de la sécurité dans le bâtiment intelligent exige d'acquérir un nouveau savoir-faire IP ou de faire appel aux professionnels qualifiés correspondants. Et si les services informatiques des entreprises sont impliqués, on doit faire appel à eux de manière précoce.

6.2 Tâches lors de la planification de la technique des bâtiments

6.2.1 Définir les conditions cadres

Lorsqu'il commence son étude, le projeteur (en technique des bâtiments) doit rencontrer la maîtrise d'ouvrage et son service informatique pour définir les conditions cadres : concept d'adresses IP, règles de sélection du matériel, des routeurs et des mots de passe, y compris leur administration, etc. Et il faut définir KNX IP Secure comme la nouvelle norme en matière de transfert d'informations KNX aux infrastructures IP. Voir l'exemple mentionné au chapitre 6.3.

6.2.2 Identités et gestion des autorisations

Qui accède ou a besoin d'accéder à quel moment ou à quel endroit et de quelle manière aux installations, et qui administre ces accès ? Les planificateur-rice-s doivent le définir de manière précoce. Le VPN peut être une solution pour l'accès externe, car les ports ouverts n'existeront certainement plus ! En outre, le concept doit également tenir compte des phases du projet que sont la construction, l'exploitation et la maintenance.

6.2.3 Une structure de projet claire

Face à la démocratisation de la mise en réseau et des smart buildings, il est de plus en plus important d'avoir une structure claire au niveau du projet, des adresses et de l'environnement IP. Les responsables de la planification et de la mise en œuvre coordonnées sont des planificateurs en génie électrique, en génie du bâtiment et en génie informatique.

Leurs tâches, entre autres :

- la distribution logique et la structuration de l'installation (topologie, zones et lignes) compte tenu du trafic de télégrammes,
- l'élaboration d'un schéma de principe documentant avec précision les topologies KNX et IP.
- Raison pour laquelle le schéma IP et le concept IP et tous les segments de réseaux, numéros IP et interfaces doivent être consignés dans la documentation.
- En complément, la gestion des mots de passe et leur divulgation doivent être documentées.
- Et, très important, chaque projet doit faire l'objet d'un concept d'adressage, comme indiqué dans les Ditectives Projets de KNX Swiss.

Une fois ces bases de planification jetées, la topologie et la sécurité d'une installation de technique des bâtiments intégrant des composants KNX et IP peut être planifiée et menée de manière optimale

6.2.4 Notions de base de sécurité

La sécurité d'une installation KNX ou IT doit être considérée dans toutes les phases du projet. La brochure KNX Secure de la KNX Association fournit des précisions importantes à ce sujet sur knx.org.

En guise de synthèse, voici les points à prendre en compte :

- Les automatisations fonctionnent toujours via des réseaux dédiés (VLAN) avec leur propre matériel (routeurs, switches, etc.).
- Une segmentation du réseau interdit tout mouvement latéral des éventuels agresseurs sur le réseau.
- Toutes les propriétés de sécurité des réseaux IP doivent être exploitées : filtrage MAC, chiffrement, mots de passe forts ou authentification multifacteur, réseaux Wi-Fi 6 avec chiffrement WPA3 et nom SSID ne permettant pas d'identifier le matériel.
- KNX IP Multicast utilisé avec une adresse autre que l'adresse standard.
- Pas de ports ouverts vers Internet sur les appareils KNX.
- Si possible, blocage de tout accès externe (Default-Gateway « 0 »).
- Accès externe à KNX seulement via VPN ou un autre accès sécurisé en fonction de l'extension du standard KNX.
- Éviter tout trafic inutile : les routeurs doivent bloquer les adresses sources correspondantes et ne doivent pas autoriser la diffusion broadcast et les liaisons point à point.
- Paramétrer la sécurité d'ETS et l'utiliser de manière sûre.

6.2.5 Ébauche de modèle de concept d'automatisation sécurisée des bâtiments

Comme signalé à titre introductif, le réseau d'un smart building est utilisé par de nombreuses « parties prenantes ». Sous la perspective de l'automatisation des bâtiments, il faut également s'assurer que toutes les zones, y compris les zones de réseau en amont, soient protégées contre tout accès non autorisé.

L'exemple suivant montre comment un tel réseau pourrait être configuré. Cette illustration ne prétend aucunement être exhaustive, elle a seulement pour vocation d'aider à élaborer des concepts grossiers dans la technique et l'informatique des bâtiments pour un projet..

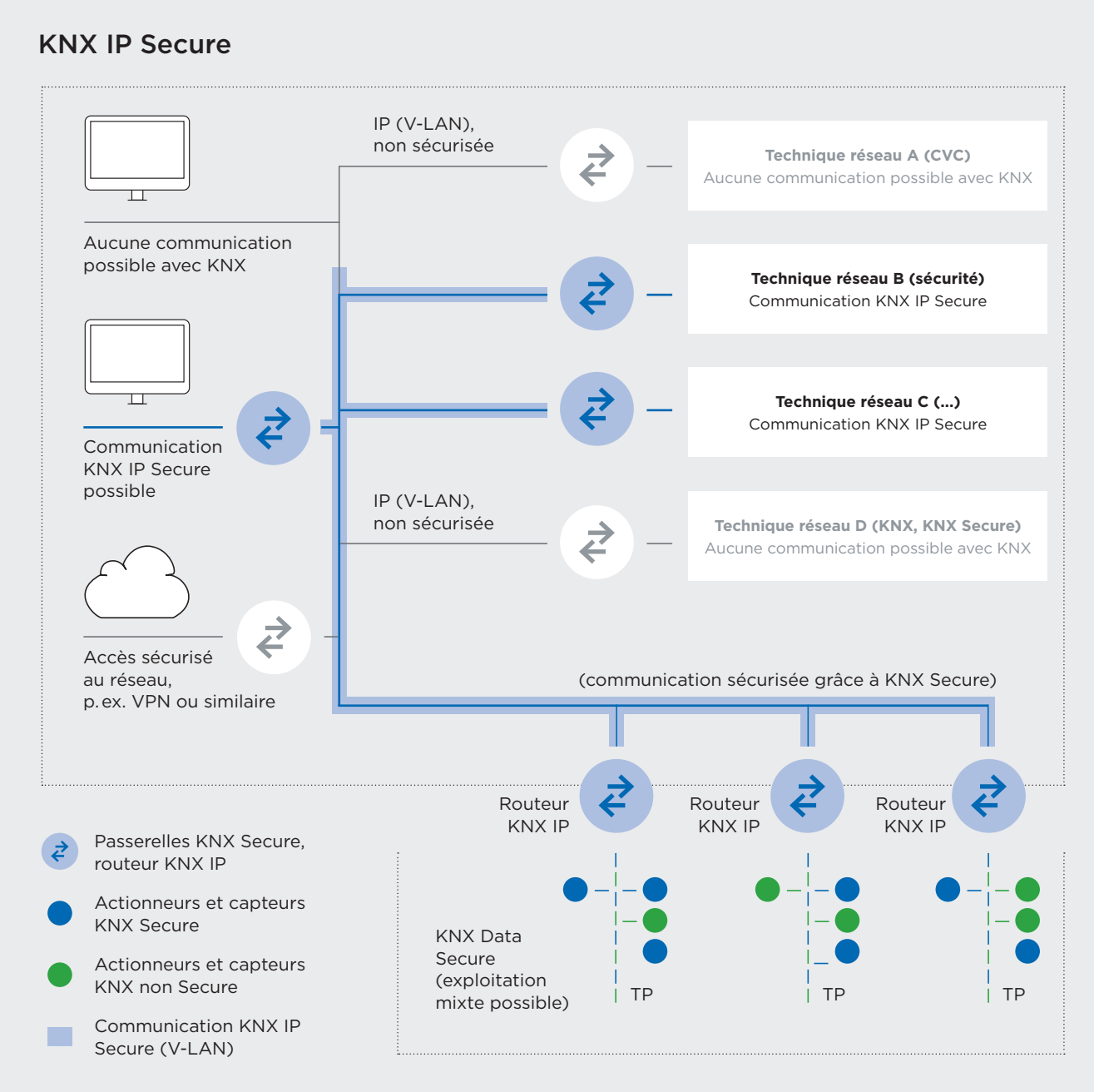


Fig. 6.2-1 Schéma de principe d'un réseau de technique des bâtiments sécurisé

6.3 Déroulement d'un projet KNX Secure

Le graphique ci-après présente d'une manière schématique comment mettre en œuvre avec succès un projet KNX Secure. Il décrit grossièrement ce qui doit être prévu dans chaque phase SIA et quand il est plus favorable d'activer le chiffrement dans l'ensemble du projet ETS. Avec l'Aide à la planification KNX Swiss et les Directives Projet de KNX Swiss, les intégrateur-rice-s systèmes KNX, ainsi que les planificateurs en génie électrique et les planificateur-rice-s en génie informatique des bâtiments, disposent d'outils de qualité pour une réalisation réussie de leurs projets.

Conseil

Conclusion : dès lors que tous les partenaires du projet communiquent avec les mêmes normes que KNX, rien ne s'oppose à la réussite de leur projet KNX Secure ou à la sécurisation du réseau de l'informatique des bâtiments.

Aperçu du déroulement d'un projet KNX Secure

Préparation KNX
Phases SIA 1 + 2

Étude KNX
Phase SIA 3

Offre KNX
Phase SIA 4

Réalisation KNX
Phase SIA 5

Exploitation KNX
Phase SIA 6

Activation de KNX Secure

Démarrage du projet / préparation
Décision d'employer KNX Secure dans le projet
- Définir les fondements et responsabilités dans l'élaboration du concept de cybersécurité/sécurité

Étude
Élaborer le concept de cybersécurité/sécurité KNX/IT
- Définir ce qui doit être exécuté avec KNX Secure et sans KNX Secure (non Secure)
- Définir la gestion des certificats des appareils («collecter» les codes QR (certificats des appareils), classement, procédure de sélection pour chargement sur ETS, flux documentaire, etc.)
- Préparer la documentation KNX Secure Tenir compte de la saturation du bus, définir la topologie

Soumission
- Intégration du concept de cybersécurité / sécurité KNX et de l'informatique dans l'appel d'offres
- Définir les positions d'honoraires de la cybersécurité (KNX et informatique) et les prestations nécessaires Préparer la documentation KNX Secure

Création du projet ETS
- Préparer le projet KNX Secure
- Définir le mot de passe du projet ETS et le documenter
- Saisir la clé KNX Secure des appareils de manière structurée suivant le concept (scanner, webcam de l'ordinateur portable, application, etc.) Important : coordination en cas de présence de plusieurs équipes dans un projet ETS (externe, freelance, etc.)
- Tenir compte de la saturation du bus

Mise en service du projet
- KNX Secure est prêt (tous les certificats des appareils sont chargés), mais pas activé
- Vérifier l'intégralité des documents KNX Secure
- Tenir compte de la saturation du bus, activer impérativement les tables de filtrage

Élaboration du projet de base

↓ *Période d'adaptation ou de modification*

Mise en service du projet, info aux clients finaux

Date de révision et d'adaptation
Adaptations ou compléments à la demande du client

Activation de KNX Secure dans le projet ETS
Le mode KNX Secure (mot de passe défini à l'avance et documenté) est activé sur ETS. ATTENTION, en cas de perte, le mot de passe ne peut pas être réinitialisé !
- L'application de tous les routeurs IP doit être redémarrée.
- Les applications de tous les appareils KNX Secure TP en mode Secure doivent également être redémarrées (voir classeur dynamique «Appareils modifiés» sur ETS).

Remise du projet définitif
Remise de la documentation KNX Secure au client final, y compris toutes les informations Secure telles que les mots de passe, etc. (voir également cahier technique Fichier de configuration ETS)
- Faire un backup du fichier du projet, y compris stockage sécurisé, avec mot de passe du projet

Créer le document

6.4 Aides à l'accompagnement de projets

L'association KNX Swiss élabore différentes documentations techniques (cahiers techniques, guides et aides à la planification) en étroite collaboration avec des acteurs KNX experts, afin d'assurer la planification, la structuration et l'exploitation correctes des projets KNX. Celles-ci sont toujours axées sur l'optimisation des projets KNX présents et futurs, du stade de l'étude à celui de l'exploitation en passant par la réalisation.

6.4.1 Directives Projet KNX Swiss

Les Directives projet KNX Swiss constituent un précieux outil pour l'assurance qualité dans les projets KNX. Elles contiennent des notions et propositions essentielles pour réussir la conception d'un projet et permettent de structurer correctement une installation KNX, facteur incontournable pour le parfait fonctionnement d'un smart home ou d'un smart building. Ces directives aident également les intégrateurs systèmes à structurer clairement les informations sous ETS et à harmoniser l'identification des composants.

Fig. 6.3-1 Directive Projets KNX Swiss: Mise en œuvre structurée de projets KNX

6.4.2 Aide à la planification KNX Swiss

En Suisse, la gestion d'un projet de construction se subdivise suivant les phases et les phases partielles du modèle de prestations de la Société suisse des ingénieurs et des architectes (SIA). L'aide à la planification KNX Swiss fournit des listes de contrôle complètes pour chacune de ces phases, permettant de définir à quel moment exécuter quels travaux et de répondre aux questions qui se posent. Les listes de contrôle portent également sur KNX Secure ou l'informatique des bâtiments sécurisée. Les contenus de l'Aide à la planification sont essentiellement basés sur l'expérience de longue date des partenaires KNX, des intégrateur-rice-s systèmes KNX et des projeteurs électricité réalisant pour leur clientèle des installations optimisées, sans erreurs et efficaces sur le plan énergétique.

Fig. 6.3-2 Aide à la planification projet KNX Swiss: Planification et mise en œuvre structurées de projets KNX

www.knx.ch

Groupe de project et auteurs

KNX Secure continue à évoluer, c'est pourquoi vos apports et compléments sont toujours les bienvenus. Veuillez nous aider à maintenir ce guide à jour. Nous serions très heureux de lire les commentaires de l'ensemble du secteur d'activité..

www.knx.ch/secure
knx@knx.ch

Auteurs

- Bruno Habegger, com:agentur
- René Senn, raum consulting

Coopération

- Beat Bebi, Feller AG
- Thomas Roth, Maneth Stiefel AG
- Stefan Balsiger, Siemens Suisse SA
- Klaus Wächter, Siemens SA
- Christoph Koch, Cisco Suisse

KNX NATIONAL SWISS

Bureau KNX Swiss
Bahnhofstrasse 88
8197 Rafz