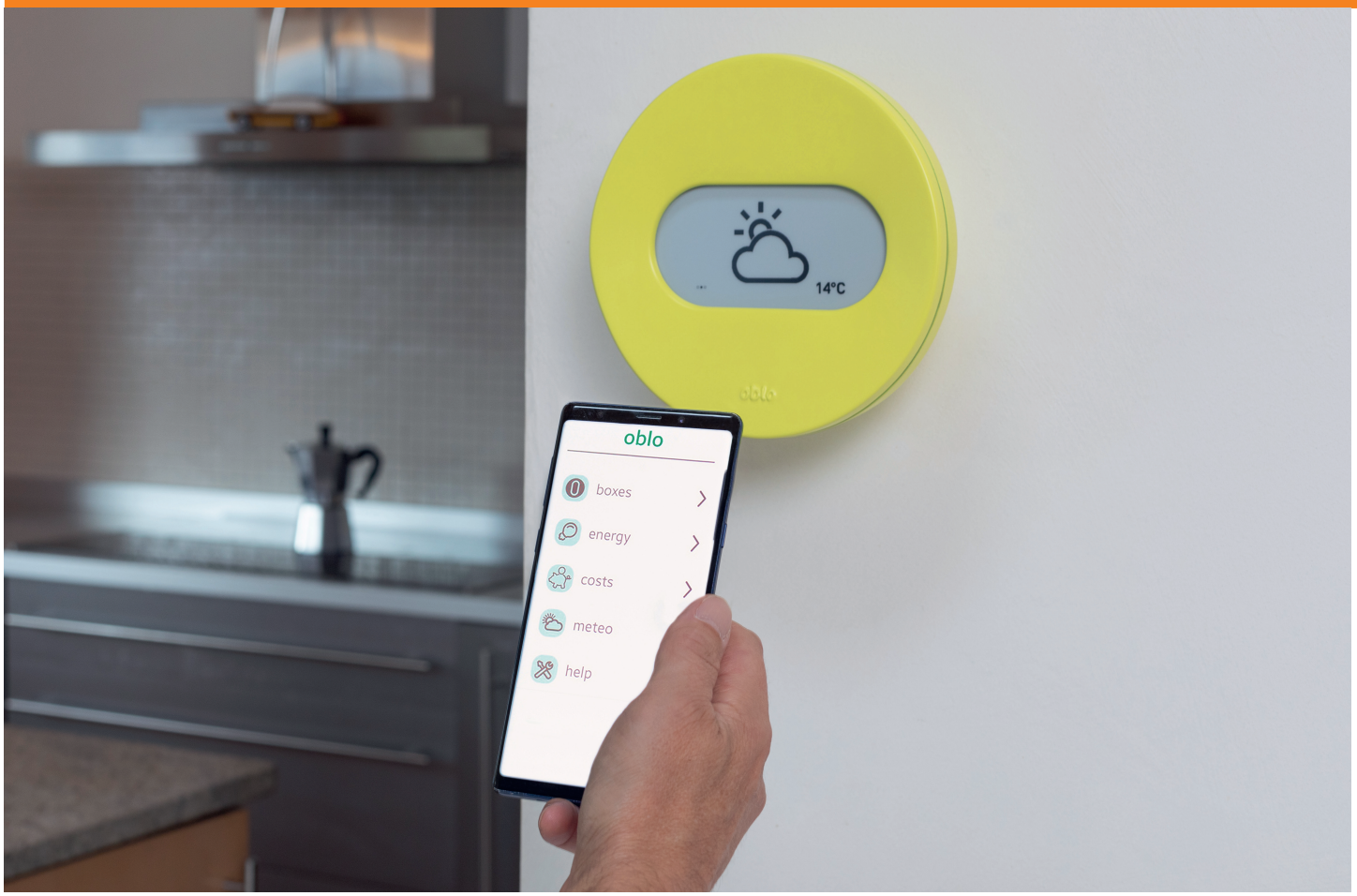

Objets intelligents ? Attention à la sécurité !

Cybersécurité de l'immotique et de l'IoT | Ces dernières années, diverses solutions ont été développées pour assurer la sécurité des communications dans les domaines de l'automatisation des bâtiments et de l'Internet des objets. Cet article propose notamment de faire le point sur le fonctionnement et les avantages de ces solutions, ainsi que sur certains éléments à considérer lors de leur mise en œuvre.

XAVIER AYMON

Dans un monde où les bâtiments intelligents jouent un rôle essentiel dans la gestion des infrastructures, la sécurité des systèmes de communication internes devient primordiale. Les bus de communication, qui assurent l'échange d'informations entre les différents systèmes d'un bâtiment – tels que le chauffage, la ventilation, la climatisation et l'éclairage –, sont en effet particulièrement vulnérables aux cyberattaques. Pour faire face à ces menaces croissantes, des protocoles de communication sécurisés ont été développés. Parmi eux, KNX Secure et BACnet Secure Connect se distinguent par leur capacité à garantir l'intégrité, la confidentialité et l'authentification des données échangées, offrant ainsi une protection robuste contre les intrusions malveillantes.

De plus, l'émergence de la technologie Matter pour l'Internet des objets (Internet of Things, IoT) et de systèmes novateurs qui s'appuient sur un hébergement cloud sécurisé pour le stockage et le traitement des données illustre la manière dont l'IoT et les solutions intelligentes redéfinissent la sécurité et l'efficacité dans les bâtiments modernes.

Cet article propose d'explorer ces technologies en examinant leur fonctionnement, leurs avantages ainsi que les défis qu'elles posent en termes de mise en œuvre et de gestion au quotidien.

KNX Secure : chiffrement des télégrammes et des adresses

Avec l'augmentation des cyberattaques ciblant les infrastructures critiques, la sécurité des systèmes KNX est devenue

Figure : Antonin Maudry

une préoccupation majeure. KNX Secure **(figure 1)** est une extension du protocole KNX, conçue pour garantir la sécurité des communications à travers un chiffrement robuste des données échangées.

Le logiciel ETS 6 joue un rôle central dans la mise en place du chiffrement des télégrammes KNX sur la couche TP (Twisted Pair). Grâce à cet outil, il est possible de configurer les dispositifs KNX Secure de telle sorte que chaque télégramme, c'est-à-dire chaque message envoyé entre les appareils du réseau, soit chiffré. Chaque dispositif KNX équipé de KNX Secure dispose d'une unité de contrôle de bus (Bus Control Unit, BCU) qui gère les clefs de chiffrement. Ces clefs sont nécessaires non seulement pour sécuriser les télégrammes, mais aussi les adresses de groupes. Ces dernières sont utilisées pour la communication entre différents appareils d'un même groupe fonctionnel. Le chiffrement des adresses de groupes garantit que seules les parties autorisées peuvent accéder aux informations échangées au sein de ce groupe, renforçant ainsi la sécurité globale du réseau.

L'un des effets directs du chiffrement KNX Secure est l'impossibilité de surveiller les données en clair sur le réseau. Cela signifie que les outils de diagnostic traditionnels, qui permettaient de lire les télégrammes pour analyser le bon fonctionnement du système, ne peuvent plus être utilisés de manière simple. Cela renforce la sécurité en empêchant toute tentative d'espionnage, mais complique également les tâches de maintenance et de dépannage. Il est toutefois également possible de mettre en place une installation mixte, où certaines communications sont sécurisées tandis que d'autres ne le sont pas. Par exemple, un ordre envoyé à un actionneur peut être sécurisé, tandis que le retour d'information sur l'état de cet actionneur, visible par le superviseur, peut ne pas être chiffré. Cette flexibilité permet de choisir le niveau de sécurité nécessaire en fonction des besoins spécifiques de chaque projet.

En offrant des outils puissants pour protéger les communications internes contre les menaces potentielles, KNX Secure représente une avancée significative dans la sécurisation des systèmes de gestion des bâtiments.

Figure : Siemens

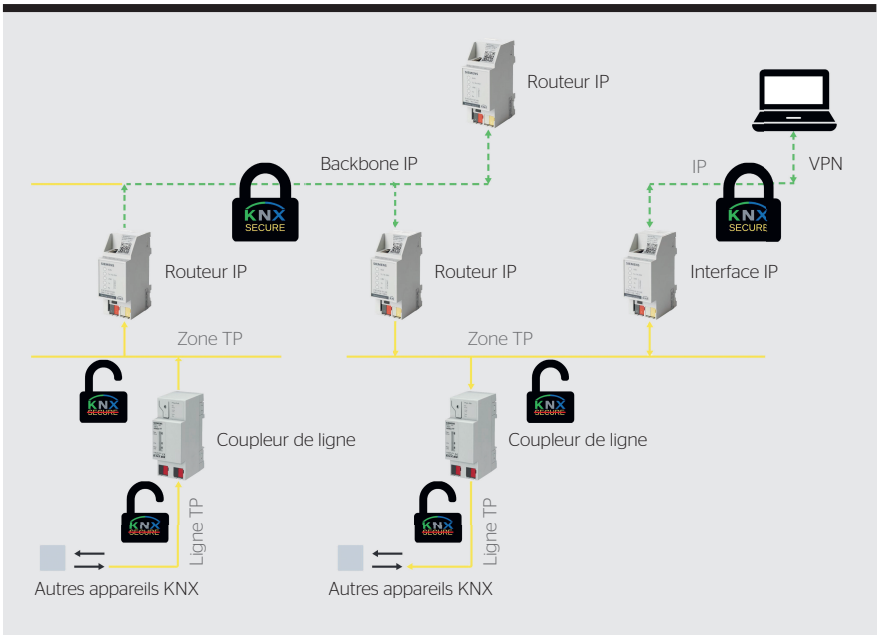

Figure 1 KNX IP Secure permet de sécuriser la communication KNX via IP.

BACnet Secure Connect: chiffrement et certificats

Le protocole BACnet/IP est largement utilisé dans le domaine de l'automatisation des bâtiments, notamment pour la remontée des points de données vers le système de gestion de bâtiment (Building Management System, BMS). Son adoption massive s'explique par les nombreux avantages qu'il offre, notamment sa flexibilité, son interopérabilité avec divers équipements et systèmes, ainsi que sa capacité à gérer un grand nombre de points de données en temps réel. Malgré ses nombreux atouts, BACnet/IP présente une faiblesse majeure: son absence de sécurité intrinsèque. Dans sa version standard, ce protocole ne chiffre pas les données échangées, ce qui signifie que toutes les communications sur le réseau sont exposées. Toute personne ayant accès au réseau, même avec des privilèges limités, peut scanner les communications, visualiser les informations échangées, et potentiellement prendre le contrôle du système entier.

Pour répondre à ces défis de sécurité, une nouvelle extension du protocole a été développée: BACnet Secure Connect (BACnet/SC) introduit des mécanismes de chiffrement et d'authentification, rendant ainsi les communications BACnet/IP sécurisées **(figure 2)**. Cette extension repose sur l'utilisation de certificats numériques pour authentifier les appareils et les utilisateurs, garantissant que seules les entités autorisées peuvent participer aux échanges de données. De plus, les communications entre les dispositifs sont chiffrées, empêchant ainsi toute interception ou altération des messages échangés.

La technologie BACnet Secure Connect repose sur un contrôle rigoureux des certificats qui autorisent la communication cryptée entre les participants. Chaque appareil ou utilisateur participant au réseau sécurisé doit posséder un certificat valide. Ces certificats sont vérifiés par un composant central, le hub, qui joue un rôle clé dans l'infrastructure BACnet/SC. Celui-ci est chargé de valider la conformité des certificats, s'assurant ainsi que seules les entités autorisées peuvent échanger des informations sur le réseau. Ce processus de vérification garantit que toutes les communications restent confidentielles et à l'abri des accès non autorisés.

L'implémentation de BACnet Secure Connect dans un bâtiment nécessite plusieurs éléments cruciaux:

- Compatibilité des produits: les équipements doivent être compatibles avec la norme BACnet Secure Connect. Cela peut nécessiter une mise à niveau ou le remplacement des dispositifs existants pour assurer une communication sécurisée.
- Gestion des certificats: la gestion des certificats numériques est essentielle

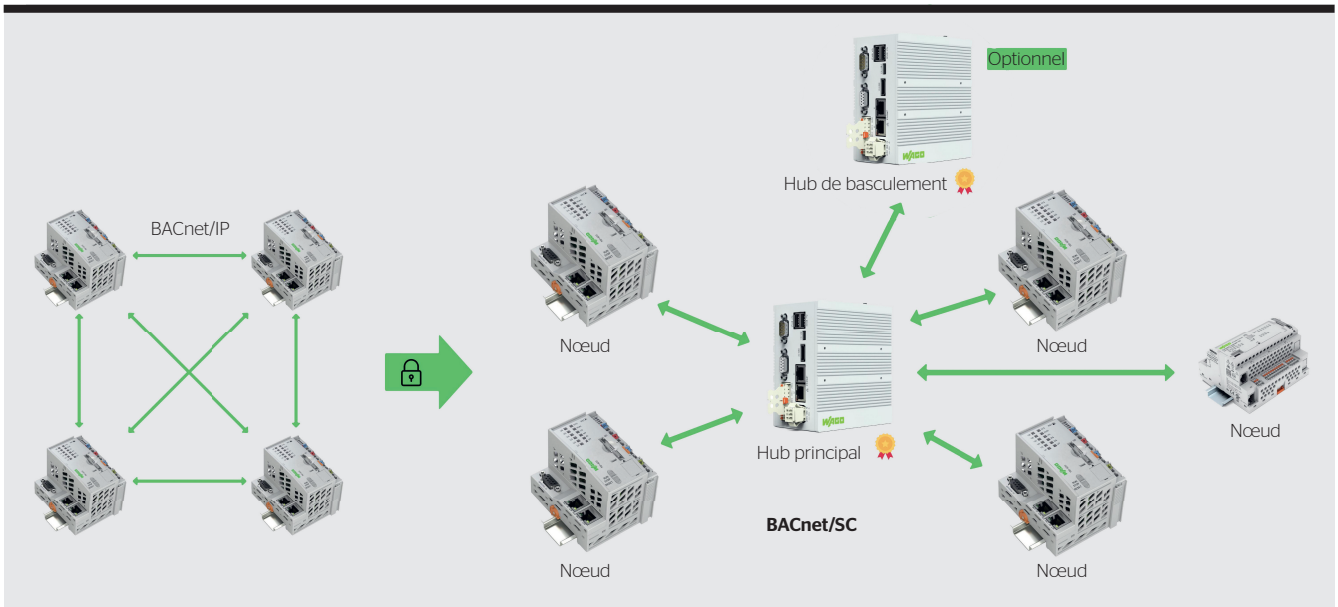

Figure 2 Comparaison des architectures BACnet/IP et BACnet/SC.

pour le fonctionnement continu du système. Cela inclut la création, la distribution, la mise à jour et la révocation des certificats via des outils dédiés. De plus, la durée de vie des certificats doit être gérée de manière proactive pour éviter des interruptions de service.

- Redondance des hubs : afin d'assurer une continuité de service en cas de défaillance du hub principal, une redondance des hubs peut être mise en place. Cette configuration permet de maintenir les communications même si l'un d'eux tombe en panne.

BACnet Secure Connect représente donc une avancée importante pour la sécurisation des réseaux de gestion des bâtiments. Bien que son implémentation nécessite des ressources supplémentaires, les avantages en termes de sécurité et de confidentialité en font une solution incontournable pour les infrastructures critiques.

La technologie Matter pour l'Internet des objets

La technologie Matter émerge comme une norme révolutionnaire pour l'IoT, visant à fournir une connectivité fiable, sécurisée et interopérable entre les dispositifs de diverses marques. Cette technologie utilise la topologie de réseau maillé via le protocole Thread, favorisant un réseau décentralisé où chaque appareil peut relayer des données, améliorant ainsi la portée et la fiabilité. Ce système est idéal pour les grandes surfaces et les bâtiments complexes.

Matter renforce la sécurité en utilisant des techniques de cryptage modernes pour protéger les communications entre les appareils. Chaque dispositif dispose de certificats numériques ainsi que de mécanismes d'authentification robustes. Cette technologie se distingue par sa compatibilité avec divers protocoles réseau tels que le Wi-Fi, Ethernet et Thread, ce qui lui permet de s'adapter à divers scénarios d'utilisation sans compromettre la performance des appareils.

L'interopérabilité est l'un des atouts majeurs de Matter, facilitant l'intégration d'appareils de différentes marques dans un écosystème unifié. Cela simplifie l'expérience utilisateur – une application mobile intuitive permet aux utilisateurs d'ajouter facilement de nouveaux appareils à leur réseau –, et stimule l'innovation et la concurrence parmi les fabricants. Autre avantage notable : la possibilité de réaliser des

IN KÜRZE

Bei intelligenten Objekten auf die Sicherheit achten

Cybersicherheit in der Gebäudeautomation und im IoT

In einer Welt, in der smarte Gebäude und das Internet der Dinge eine immer grössere Rolle bei der Verwaltung von Infrastrukturen spielen, ist die Cybersicherheit der in diesen Bereichen verwendeten Kommunikationssysteme zentral. Deshalb wurden in den letzten Jahren verschiedene Lösungen entwickelt, um Hackerangriffe zu verhindern, die mitunter schwerwiegende Folgen haben können.

Dieser Artikel gibt einen Überblick über Funktion und Vorteile von KNX Secure und BACnet/SC (BACnet Secure Connect) sowie über Aspekte, die bei der Implementierung in der Gebäudeautomation beachtet werden müssen. Zudem wird das Funktionsprinzip der Matter-Technologie beschrieben, die im IoT Interoperabilität, Sicherheit, Benutzerfreundlichkeit und Flexibilität vereint und den Aufbau robuster und skalierbarer IoT-Netzwerke ermöglicht. Schliesslich wird mit Oblo – einem vorausschauenden Heizungsregelungssystem – ein Beispiel für ein IoT vorgestellt, dessen Cybersicherheit auf einem sicheren Cloud-Hosting beruht.

Figure: Wago

mises à jour « over the air (OTA) ». Les fabricants peuvent en effet déployer des mises à jour de sécurité et de fonctionnalités directement sur les appareils, maintenant ainsi leur efficacité et leur sécurité à long terme.

Matter représente une avancée majeure dans le domaine de l'IoT, offrant une solution qui allie interopérabilité, sécurité, facilité d'utilisation et flexibilité. Sa topologie de réseau maillé et sa compatibilité avec plusieurs protocoles facilitent la création de réseaux IoT robustes et évolutifs.

Un exemple d'IoT prometteur et sécurisé

Oblo est un système de régulation de chauffage innovant et anticipatif, conçu pour améliorer l'efficacité énergétique dans divers types d'espaces, qu'ils soient résidentiels, commerciaux ou industriels. En se basant sur les prévisions météorologiques, ce système anticipe les besoins en chaleur, permettant ainsi de mieux gérer l'inertie thermique des bâtiments et d'optimiser la distribution de chaleur. Compatible avec tous les types de chauffage, il permet d'atteindre environ 15 à 20 % d'économie d'énergie.

Cet exemple d'IoT s'appuie sur un hébergement cloud sécurisé pour stocker et traiter en temps réel les données nécessaires à l'anticipation des besoins énergétiques. Grâce à cette infrastructure, les données sensibles relatives aux bâtiments et à la gestion thermique sont protégées tout en offrant des capacités d'analyse avancée et une haute disponibilité.

Conclusion

À mesure que l'Internet des objets prend de l'ampleur et connecte un nombre croissant de dispositifs intelligents, il devient de plus en plus crucial d'assurer la sécurité des communications nécessaires à son bon fonctionnement. Les objets connectés collectent et échangent d'énormes volumes de données, souvent sensibles, qu'il s'agisse d'informations personnelles, d'usages énergétiques ou de contrôle de systèmes critiques. Une protection robuste contre les cyberattaques et les intrusions malveillantes est essentielle pour garantir la confidentialité, l'intégrité et la disponibilité de ces systèmes. Sans une sécurité adéquate, les infrastructures IoT sont vulnérables à des risques majeurs qui peuvent compromettre non seulement les utilisateurs individuels, mais aussi des réseaux entiers, avec des conséquences potentiellement graves. La sécurité dans l'IoT n'est plus une option, mais une nécessité pour assurer la confiance et la durabilité de ces technologies dans un monde de plus en plus interconnecté.

L'adoption de technologies avancées telles que KNX Secure, BACnet/SC, Matter, ou encore l'hébergement des données dans un cloud sécurisé, constitue un tournant décisif dans la gestion des bâtiments et de l'IoT. Ces solutions non seulement renforcent la sécurité des systèmes de communication, mais augmentent également l'efficacité énergétique, tout en offrant des avantages substantiels en termes de flexibilité et de durabilité environnementale. Ces avancées technologiques répondent de manière adéquate aux exigences actuelles et préparent le terrain pour une future intégration encore plus poussée des bâtiments intelligents dans notre quotidien.

Auteur
Xavier Aymon est administrateur de l'Atelier R2D2.
→ Atelier R2D2 Sàrl, 1966 Ayent
→ hello@atelier-r2d2.ch