UNE MEILLEURE PROTECTION POUR L'AUTOMATISATION DU BÂTIMENT

BACnet Secure Connect

siemens.ch/comfort/fr

SIEMENS

Sommaire

Pourquoi les systèmes de gestion technique du bâtiment doivent-ils être mieux protégés ?

Les systèmes de gestion technique du bâtiment (GTB) ont connu des évolutions technologiques ces dernières années. Avec le développement de la mise en réseau dans les bâtiments, la technologie opérationnelle (Operational Technology ou OT) et les systèmes informatiques se rapprochent de plus en plus. Il est donc d'autant plus important de protéger intégralement les deux réseaux contre d'éventuelles cyber-attaques. BACnet Secure Connect (BACnet/SC) constitue un élément important de la réponse aux exigences de sécurité croissantes.

Depuis longtemps déjà, les cybermenaces concernent bien plus que les systèmes informatiques. Les systèmes OT, tels que le chauffage, la ventilation et la climatisation (CVC), l'éclairage, les compteurs d'énergie, les technologies de sécurité ou le contrôle d'accès, sont également de plus en plus menacés en raison de la connectivité croissante et des possibilités d'attaque plus nombreuses qui en découlent. Pour limiter le risque d'attaque contre ces appareils physiques, souvent négligés jusqu'à présent, il faut renforcer leur protection. Les systèmes OT ont besoin de fonctions de sécurité intégrées et d'un trafic de données inviolable afin de répondre à l'objectif de protection principal: la disponibilité des installations. Une étape importante a été franchie avec la poursuite du développement du protocole réseau BACnet (Building Automation and Control Network), standardisé au niveau mondial, en BACnet/SC. BACnet/SC contient une couche réseau supplémentaire pour garantir la sécurité du protocole de communication des données pour les réseaux d'automatisation et de régulation des bâtiments.

BACnet/SC repose sur des protocoles d'application IP reconnus et établis, ainsi que sur des techniques standard utilisées dans le secteur informatique. Ce système intègre la sécurité au niveau des appareils directement dans le protocole de communication et chiffre toutes les données échangées entre les appareils. La même technologie de chiffrement est déjà utilisée pour sécuriser le trafic de données dans les services bancaires en ligne et d'autres applications critiques.

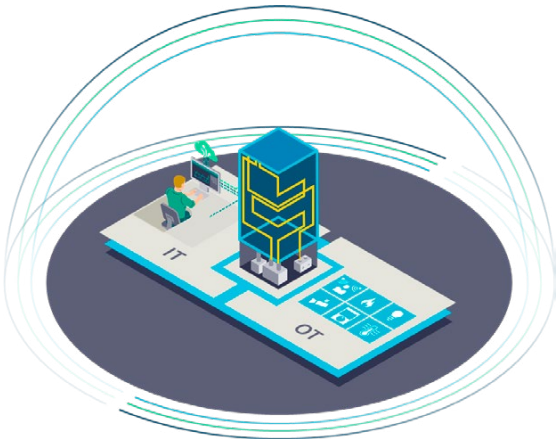
Si la sécurité des systèmes OT est prise en compte dans une approche de sécurité globale avec des mécanismes de défense à plusieurs niveaux, il est possible non seulement de protéger les infrastructures opérationnelles, mais aussi de fermer les vecteurs d'attaque et de réduire les risques de cybermenaces contre les systèmes OT.

Si les systèmes en réseau ne sont pas correctement protégés, la domotique et les processus opérationnels de votre bâtiment peuvent être perturbés, ou les données de contrôle de votre entreprise manipulées.

Plus de sécurité et une meilleure connectivité IT pour les systèmes OT

BACnet/SC constitue une étape essentielle sur la voie d'un système GTB intégré, protégé de manière optimale et adapté aux exigences de la numérisation croissante dans le secteur du bâtiment.

La nouvelle option de liaison de données BACnet/SC représente un complément important à la norme BACnet et améliore la cybersécurité et la connectivité informatique des systèmes BACnet. Avec les systèmes BACnet/SC, vous n'investissez pas seulement dans la cybersécurité : vous préparez également votre système GTB aux exigences futures et assurez sa compatibilité avec les innovations à venir dans le domaine des bâtiments intelligents.



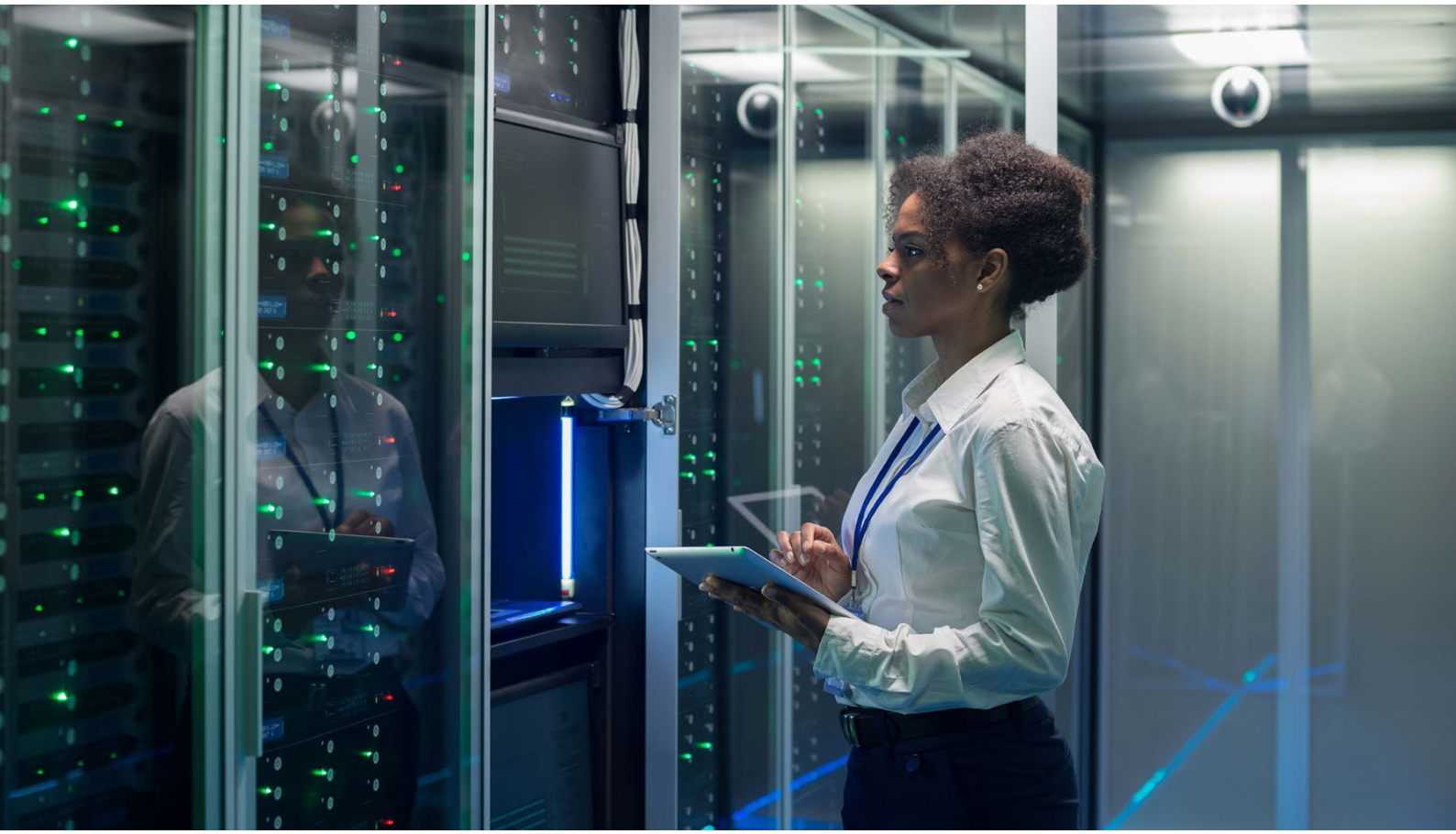
BACnet/SC en bref	Vorteile von BACnet/SC
BACnet/SC complète BACnet avec une autre **option de connexion de données sécurisée**	**Protection des investissements:** compatibilité avec les réseaux BACnet actuels et futurs, et possibilité d'extension/de mise à niveau progressive
Chiffrement du trafic de données BACnet pour protéger la communication GTB contre les manipulations	**Protection des données:** communication sécurisée de bout en bout même dans des environnements réseau non sécurisés
Mécanisme d'authentification pour limiter l'accès à un projet	**Protection:** exclusion des appareils non autorisés sur le réseau et des attaques de type «homme du milieu»
Connexion informatique améliorée our une communication sécurisée dans l'automatisation du bâtiment	**Pratique et économique:** s'intègre parfaitement dans l'environnement informatique existant

Déploiement et détection d’appareils faciles

BACnet/SC offre un chiffrement supplémentaire pour la communication BACnet et impose une authentification des appareils au moyen de certificats. Les réseaux OT sont ainsi moins vulnérables aux cyber-attaques.

Des technologies standardisées et éprouvées sont utilisées, comme le protocole WebSocket via HTTPS, sécurisé par TLS v1.3 (authentification mutuelle) et des certificats X.509, que les experts en informatique connaissent déjà. Le protocole UDP de BACnet/IP a été remplacé par le protocole TCP. BACnet/SC fonctionne sans problème avec les pare-feux IP et la traduction d’adresses réseau (NAT). De plus, il n’y a plus de broadcasts sur le réseau IP.

Le protocole éprouvé WebSocket via HTTPS remplace UDP par TCP.



Caractéristiques de BACnet/IP et BACnet/SC

	BACnet/IP	BACnet/SC
Modèle de communication standardisé	●	●
Interopérabilité entre les fournisseurs listés par le BACnet Testing Laboratory (BTL) et les BACnet Interoparability Building Blocks (BIBBs) correspondants dans le Protocol Implementation Conformance Statement (PICS)	●	●
Compatibilité avec les versions existantes et futures de BACnet	●	●
Routage BACnet entre différentes connexions de données BACnet (BACnet/IP, BACnet/SC)	●	●
Numéros d'instance d'appareil et numéros d'instance d'objet pour identifier les appareils/objets	●	●
Évolutivité et flexibilité du système	●	●
Protocole UDP sans connexion	●	
Protocole TCP orienté connexion		●
Trafic de données avec chiffrement de bout en bout WebSocket sécurisé par TLS v1.3		●
Tous les appareils sont authentifiés avec des certificats X.509 avant de rejoindre le réseau		●
Ne nécessite pas de Broadcast Management Device BACnet (BBMD) pour accéder aux sous-réseaux IP		●
Fonctionne bien avec les pare-feux IP ou la traduction d'adresses réseau (NAT)		●
Aucune adresse IP statique requise		●

Comme BACnet/SC ne constitue qu'une option de liaison de données supplémentaire, il peut accéder aux liaisons de données BACnet existantes, comme BACnet/IP, via le routage BACnet. BACnet/SC utilise toujours la même méthode d'identification des appareils/objets (numéros d'instance d'appareil et d'objet).

Les appareils BACnet de dernière génération prennent en charge à la fois BACnet/IP et BACnet/SC. Cependant, de nombreux appareils compatibles BACnet/SC fonctionneront plus ou moins transitoirement avec BACnet/IP. Lors du changement de configuration réseau de BACnet/IP à BACnet/SC ou du routage de connexions de données existantes vers BACnet/SC, il n'est pas nécessaire de procéder à une nouvelle détection des appareils et des objets ou de recréer des tendances, des calendriers et des graphiques. Cela permet de gagner beaucoup de temps lors des projets de mise à niveau. En outre, BACnet/SC offre toujours les caractéristiques de performance BACnet éprouvées, telles que:

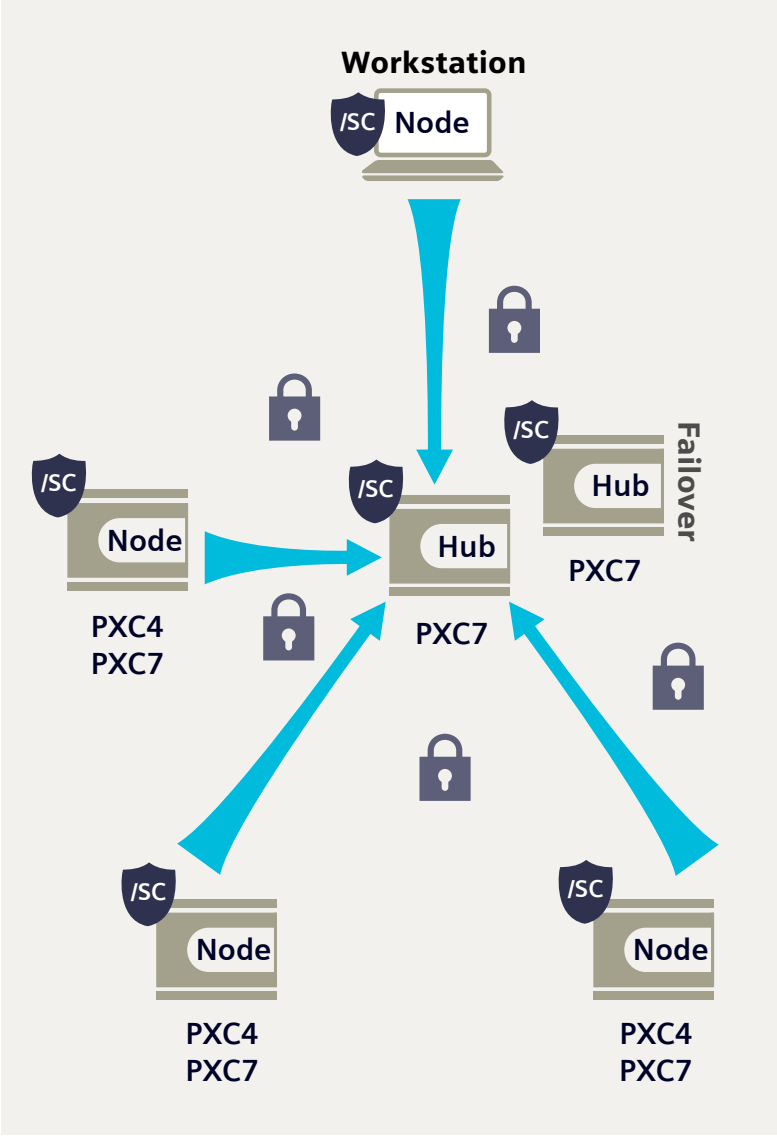
- Évolutivité et flexibilité du système
- Interopérabilité entre différents fournisseurs conformes à BACnet avec les listings BTL et les BIBB correspondants dans la PICS des appareils qui composent le système.

Architecture de réseau logique de BACnet/SC

«hub» et «nœud» sont des fonctions logiques dans le Firmware des appareils BACnet/SC. L'architecture hub et nœud de BACnet/SC nécessite au moins un hub BACnet/SC sur le réseau.

Le hub est le point central de l'authentification des appareils. Tous les autres appareils du réseau BACnet/SC comportent des nœuds. Les nœuds s'authentifient auprès du hub. Tout le trafic des nœuds doit passer par le hub.

- La fonction hub est exécutée par les contrôleurs système. Ils sont suffisamment fiables et puissants pour prendre en charge de nombreuses connexions de nœuds simultanées ainsi que le routage BACnet entre différentes connexions de données, tout en assurant leurs fonctions de contrôle.
- Comme le hub représente un point de défaillance unique (SPOF), un deuxième hub (un hub de basculement) est fortement recommandé pour la sécurité du réseau en cas de panne. Il peut s'agir d'un autre contrôleur système du réseau doté de la fonctionnalité hub BACnet/SC.
- Si le hub principal tombe en panne, les nœuds sont configurés pour rechercher le hub de basculement. La communication se poursuit sans interruption. Chaque appareil doté de la fonctionnalité hub est également un nœud par défaut et peut être utilisé dans le projet selon les besoins.

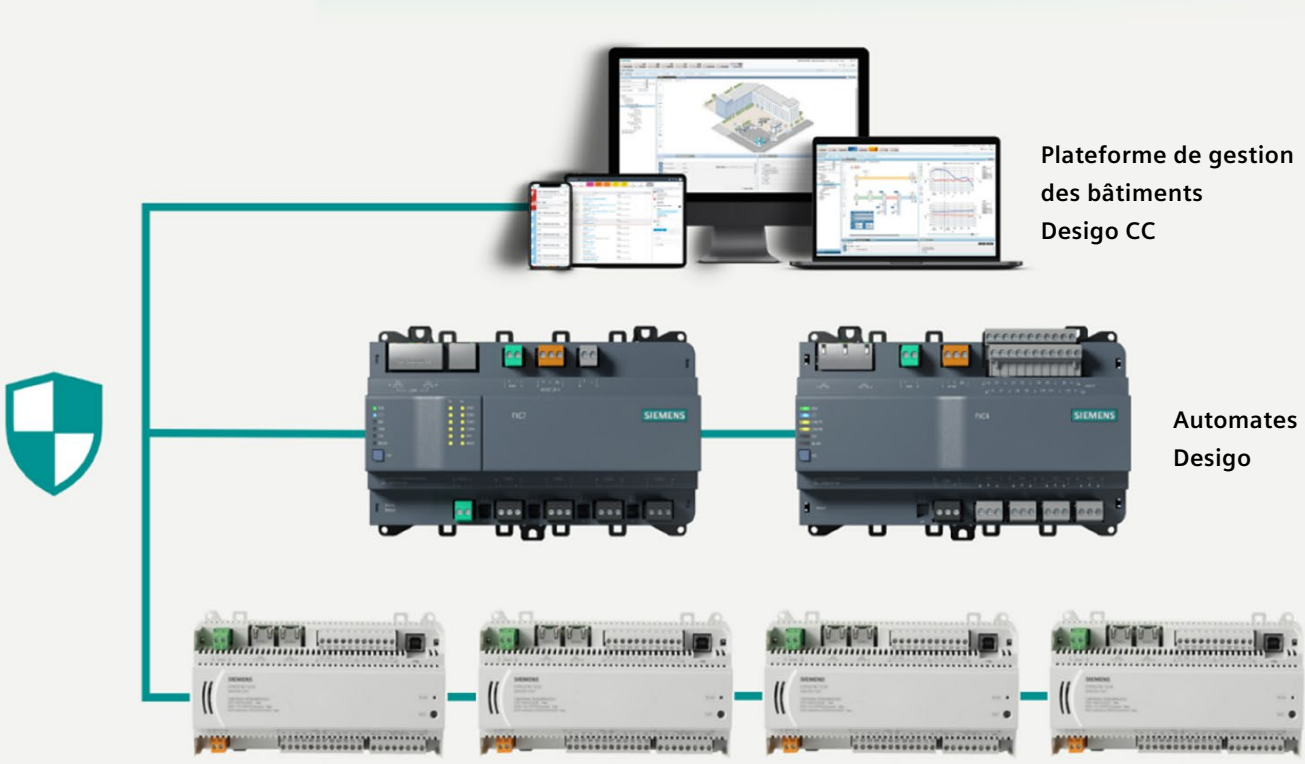


Le système BACnet/SC de Siemens

Avec les nouveaux automates Desigo de la série PXC4..7 et la plateforme de gestion Desigo CC-, Siemens propose une solution complète et certifiée BTL avec les appareils des profils B-BC et B-XAWS avec BACnet/SC. Des outils de gestion des certificats avec communication BACnet/SC complètent le système BACnet/SC de Siemens.

L'automate Desigo PXC7 est un nœud qui peut, si nécessaire, assumer la fonction de hub BACnet/SC ou de hub de basculement ainsi que de routeur BACnet/SC. Grâce à ses quatre ports EIA-485, le modèle Desigo PXC7 peut transmettre des données entre les réseaux BACnet/SC et BACnet/IP. L'automate Desigo PXC4 et la plateforme de gestion Desigo CC fonctionnent comme des nœuds BACnet/SC. Les automates de pièce PXC3 et DXR.E sont des appareils compatibles BACnet/SC qui peuvent être activés via une mise à jour du Firmware. Ces produits vous accompagnent dans la mise en œuvre d'une infrastructure GTB plus sécurisée, à commencer par les principaux composants système.

Une solution complète de bout en bout qui allie automatisation du bâtiment et cybersécurité.

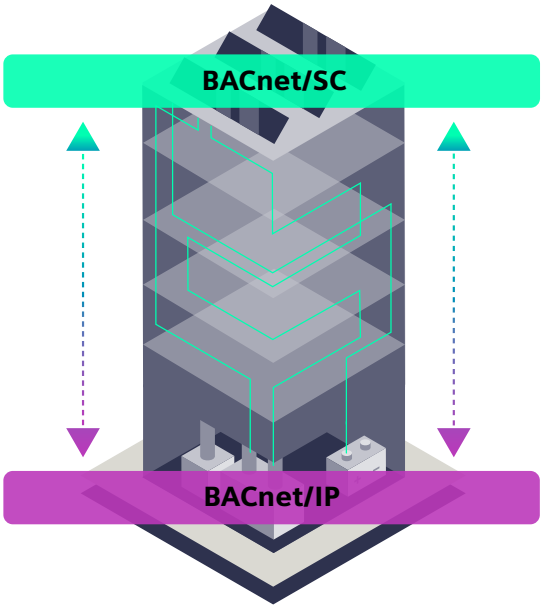


Un aperçu du système et les descriptions correspondantes sont disponibles ici:
https://www.siemens.com/fr/fr/produits/buildingtechnologies/automatisation/desigo.html

BACnet/SC pour les nouvelles constructions ou la modernisation des systèmes BACnet existants

Pour une infrastructure de bâtiment sécurisée, il vaut la peine d'utiliser des produits proposant la fonction BACnet/SC. Pour les nouveaux projets de construction, les systèmes BACnet devraient être planifiés avec des produits BACnet/SC natifs déjà disponibles ou des produits suffisamment performants pour prendre en charge les futures mises à niveau du Firmware vers BACnet/SC.

Le système de gestion et les automates dans les réseaux connectés au cloud ou dans les réseaux informatiques d'entreprise sont les composants les plus importants pour démarrer avec BACnet/SC. Ils sont généralement directement accessibles, ce qui les rend très vulnérables. Il est moins nécessaire de sécuriser les réseaux profondément à l'intérieur des bâtiments. Une autre raison justifie de démarrer avec des systèmes BACnet/SC dans les automates : ils offrent la puissance nécessaire pour prendre en charge la fonctionnalité hub BACnet/SC et le routage BACnet entre différentes connexions de données BACnet. Grâce au routage BACnet, les produits BACnet/IP existants qui ne prennent pas en charge BACnet/SC peuvent également être utilisés dans des projets si leurs fonctionnalités spécifiques sont nécessaires.



Pour les systèmes BACnet existants, il est recommandé de procéder par étapes pour la mise à niveau ou l'extension. Cela garantit une transition en douceur et préserve les investissements déjà réalisés par les propriétaires de bâtiments dans les systèmes d'automatisation et de sécurité.

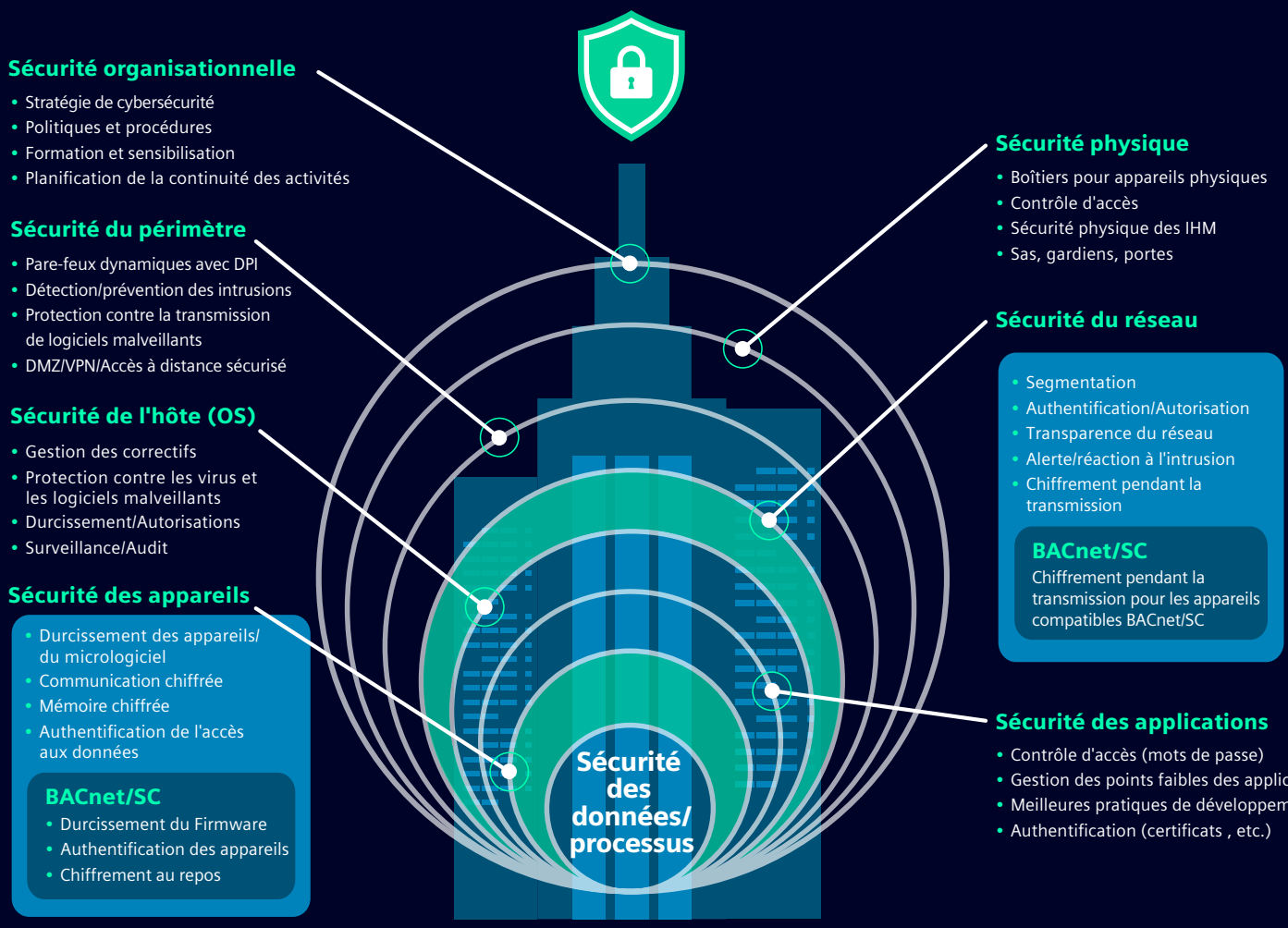
- BACnet/SC peut être connecté aux réseaux/systèmes BACnet/IP existants via le routage BACnet
- (disponible dans Desigo PXC7). Les systèmes existants peuvent être mis à niveau de manière progressive et flexible si nécessaire.
- Pour effectuer des mises à niveau, les réseaux/systèmes BACnet peuvent être divisés en réseaux logiques BACnet individuels avec différents types de connexion de données et les îlots logiques du réseau BACnet/SC peuvent être connectés via le routage BACnet.
- Les réseaux non sécurisés restants peuvent être mis à niveau à mesure que les appareils sur ces réseaux deviennent obsolètes et que des appareils de remplacement sont disponibles.
- Étant donné que les communications BACnet/SC sont sécurisées uniquement entre le hub BACnet/SC et les nœuds (le réseau logique BACnet/SC), les segments de réseau non BACnet/SC doivent être protégés de manière adéquate en tenant compte de la sécurité globale du système.

Une approche globale de la sécurité des bâtiments

Un système de défense efficace comporte plusieurs niveaux. Le principe Defense-in-Depth (défense en profondeur) est simple: Aucun mécanisme de sécurité ne peut à lui seul protéger contre d'éventuels assaillants. Toutefois, s'il existe plusieurs mécanismes de défense indépendants, il est beaucoup plus difficile de pénétrer dans le système. Les attaques sont tellement ralenties qu'elles ne sont souvent plus rentables pour l'assaillant.

BACnet/SC offre aux experts informatiques des méthodes établies pour intégrer les systèmes OT dans un concept de sécurité global et ainsi garantir la sécurité de l'entreprise. Un réseau OT soigneusement conçu et correctement configuré avec BACnet/SC soutient une approche proactive et multicouche de «défense en profondeur» et peut constituer la dernière ligne de défense d'un bâtiment intelligent en cas de cyberattaque.

BACnet/SC relève du concept de «défense en profondeur»

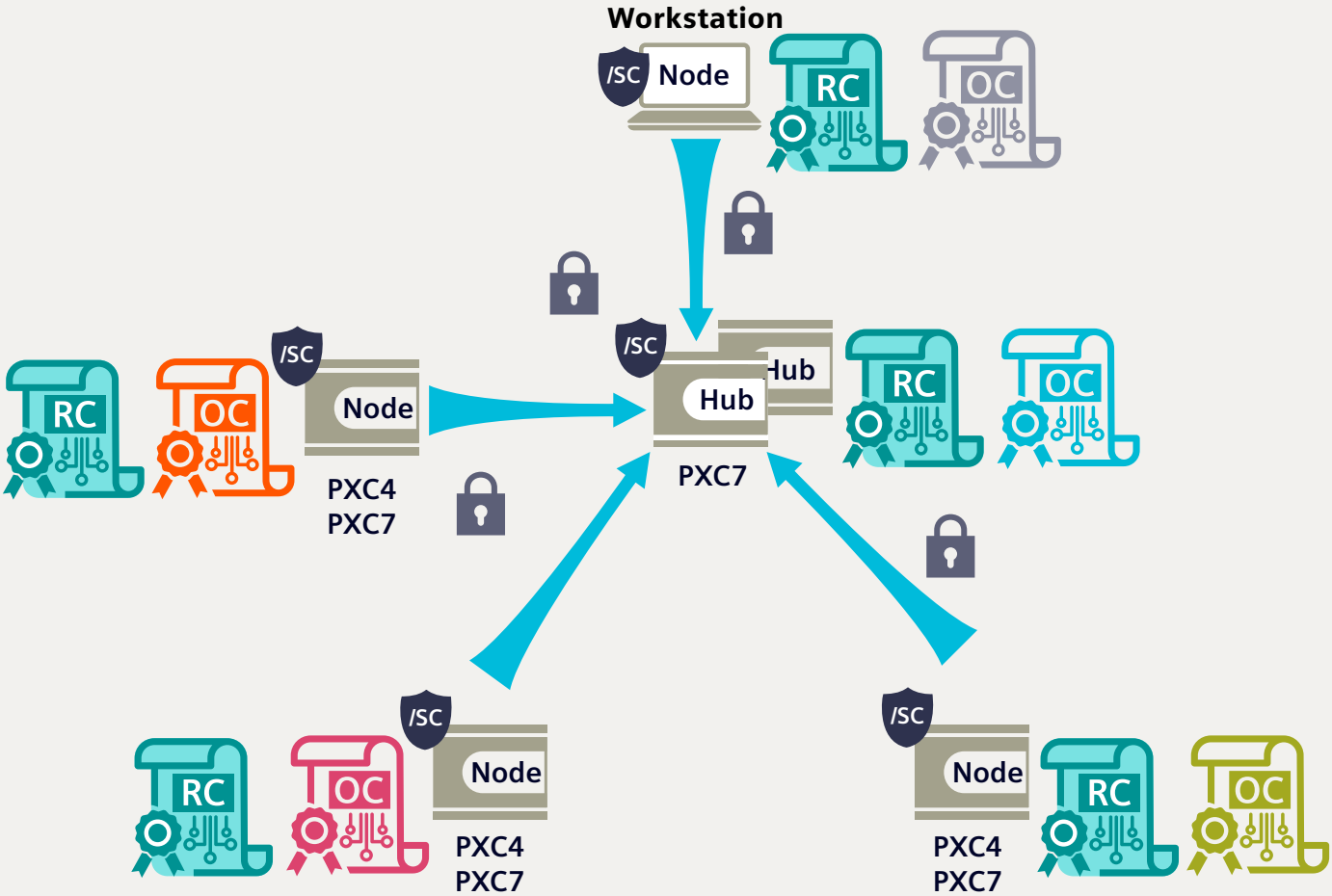


Gestion et outils des certificats BACnet/SC

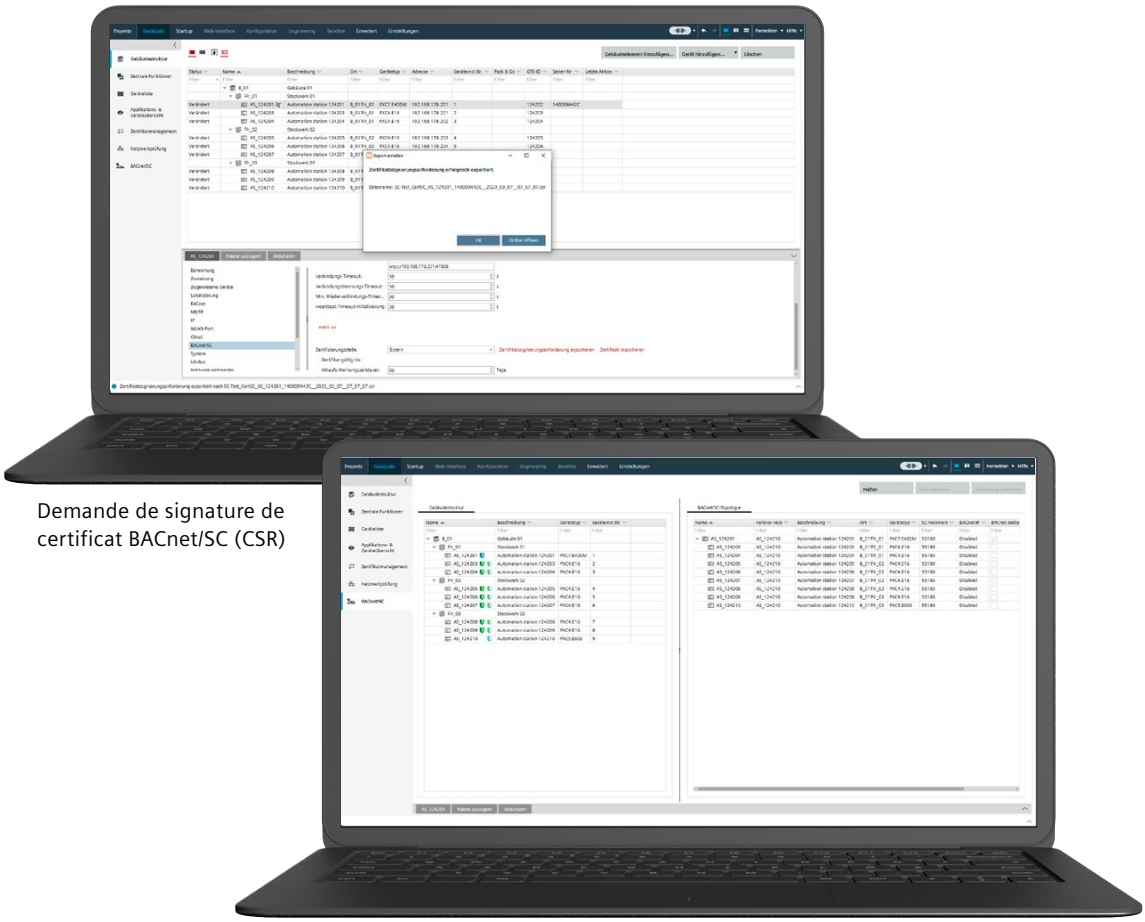
Avec BACnet/SC, l'authentification des appareils dépend de l'utilisation des certificats corrects. Chaque appareil a besoin de deux certificats pour participer au réseau BACnet/SC.

Le premier certificat est un certificat racine commun, identique sur tous les appareils d'un projet, quel que soit le fabricant de l'appareil. Il existe en outre les certificats d'exploitation individuels, uniques pour chaque appareil et utilisés pour authentifier les appareils et pour chiffrer et déchiffrer le trafic de données. BACnet/SC exige qu'une seule autorité de certification (CA) signe les certificats pour tous les appareils du projet.

Siemens vous propose l'application gratuite ABT Site, dont les flux de travail simples et intuitifs répondent à toutes les exigences de la gestion de réseau BACnet/SC. ABT Site comprend toutes les fonctions nécessaires pour générer, signer ou fournir des certificats sur des appareils Siemens, entre autres. De plus, il est possible d'importer et d'exporter des certificats BACnet/SC au niveau du fichier afin qu'ils soient interopérables avec les outils d'autres fournisseurs ou qu'ils servent d'intermédiaire avec une autorité de certification de votre choix.



Gestion simple des certificats avec ABT Site



Demande de signature de certificat BACnet/SC (CSR)

Example d’aperçu du réseau BACnet/SC

Procédure d’utilisation d’ABT Site en tant qu’autorité de certification

Pour de nombreuses entreprises, il peut être plus simple d’utiliser l’application ABT Site de Siemens en tant qu’autorité de certification. Dans ce cas, ABT Site est utilisé de manière totalement autonome pour créer, signer, fournir et renouveler des certificats. Vous bénéficiez ainsi d’une communication chiffrée et d’une authentification des appareils sans la complexité d’une autorité de certification externe.

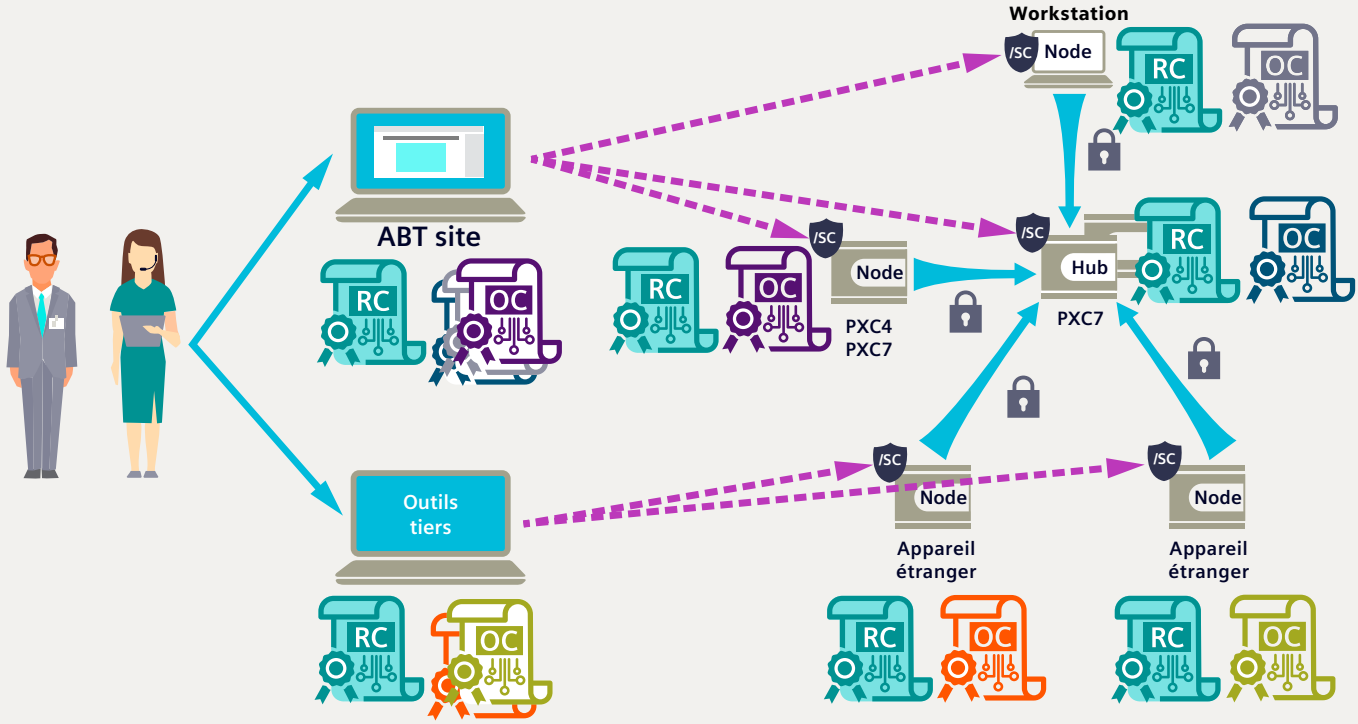
Procédure d’utilisation d’une autorité de certification spécifique au client

Si vous préférez utiliser votre propre autorité de certification de confiance, des étapes supplémentaires sont nécessaires pour l’échange de certificats. Dans ce cas, une demande de signature de certificat (CSR) est exportée depuis ABT Site et les certificats sont signés par l’autorité de certification choisie. Une fois les certificats signés par l’autorité de certification de confiance, ils sont réimportés dans ABT Site et mis à disposition sur les appareils Siemens.

Une coordination étroite entre l’IT et l’OT est requise

Dans les deux cas, l’équipe informatique ou d’exploitation du bâtiment chargée de la gestion des certificats doit définir les cas d’utilisation et les procédures nécessaires pour sécuriser efficacement le réseau. Des réseaux correctement sécurisés nécessitent une culture organisationnelle soucieuse de la sécurité et un personnel dédié chargé de surveiller les équipements, de renouveler les certificats et de coordonner les fournisseurs OT respectifs sur le site. Ce rôle implique un niveau de responsabilité plus élevé, car l’équipe responsable détient la clé de ce réseau OT sécurisé. Les experts IT et OT doivent donc travailler en étroite collaboration pour garantir que le le réseau OT est correctement surveillé et géré.

Diagramme de flux de travail de la gestion des certificats



En raison de la numérisation et de la mise en réseau croissantes de l'automatisation du bâtiment, le risque de cyber-attaques augmente. Cela concerne aussi de plus en plus le domaine OT. La cybersécurité des systèmes OT n'est donc plus une option, mais une nécessité absolue.

BACnet/SC permet une communication et une authentification sécurisées entre les appareils AB afin d'assurer la cybersécurité et une meilleure connectivité informatique dans les réseaux OT.

BACnet/SC est compatible avec n'importe quel système BACnet et offre flexibilité, évolutivité et interopérabilité.

Les produits et services Siemens répondent aux normes de sécurité les plus élevées afin de protéger au mieux l'infrastructure des bâtiments contre d'éventuelles cyberattaques. Nous travaillons constamment à la mise sur le marché d'autres produits BACnet/SC répondant à différentes exigences en matière d'automatisation du bâtiment. En tant que partenaire de confiance en matière de cybersécurité, nous prenons les cybermenaces au sérieux. Notre approche globale de la cybersécurité vous aide à relever les défis d'un monde de plus en plus numérisé.

Pour en savoir plus sur les solutions d'automatisation du bâtiment de Siemens, cliquez ici.

Nous proposons une gamme de produits et services qui renforcent la cybersécurité sur plusieurs systèmes:

- Services de cybersécurité pour évaluer la situation actuelle et élaborer un plan visant à combler les failles de cybersécurité tout en protégeant les investissements réalisés
- Produits et systèmes conçus dès le départ pour garantir la cybersécurité, faisant appel aux technologies les plus récentes et vérifiés par d'exigeants tests de pénétration
- Transparence des informations concernant les vulnérabilités et les incidents avec des mises à jour en temps réel sur les mesures prises
- Expertise en automatisation, en numérisation et en cybersécurité conforme aux normes internationales et offrant une protection à long terme même si les technologies, les produits et les systèmes évoluent

L’intégration des systèmes énergétiques, de l’immobilier et de l’industrie permet à Smart Infrastructure de réunir le monde réel et le monde numérique pour gagner en efficacité et en durabilité et améliorer nos modes de vie et de travail.

Avec nos clients et partenaires, nous créons un écosystème qui répond de façon intuitive aux besoins des usagers et aide les clients à optimiser l’utilisation des ressources.

Un écosystème qui aide nos clients à évoluer, encourage les progrès des communautés et favorise un développement durable.

siemens.ch/smartinfrastructure

Editeur
Siemens Suisse SA
Smart Infrastructure
Freilagerstrasse 40
8047 Zurich
Suisse
Tél. + 41 585 578 700

N° de commande SI-11001F/CH