

BACnet France



Numéro 19

Novembre 2026

Journal



Dossier Cybersécurité

Une GTB
« cybersécurisée » pour
un opérateur d'importance
vitale

Initiation des futurs
techniciens à la sécurisation
des communications
numériques

Gestion intelligente des
bâtiments pour les PME :
comment les petits et
moyens projets immobiliers
bénéficient de solutions de
GTB rentables

5

18

22

26

**ENER
MEETING**
2027

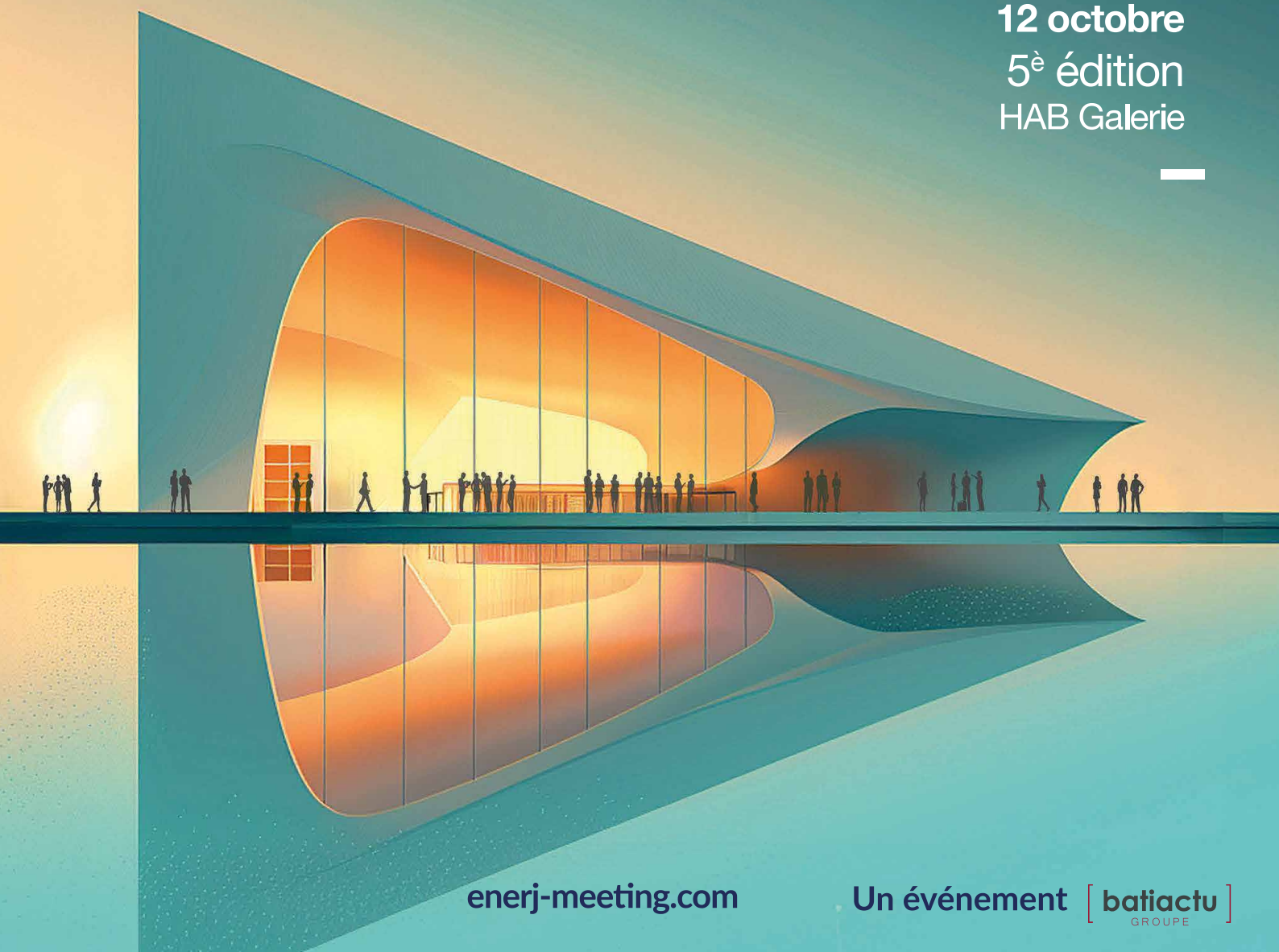
LA JOURNÉE DE
LA PERFORMANCE
ENVIRONNEMENTALE
DU BÂTIMENT

Paris
23 février
11^e édition
Carrousel du Louvre

BÂTIR 2050 MAINTENANT

Marseille
1^{er} juin
1^{ère} édition
Palais de la Bourse

Nantes
12 octobre
5^e édition
HAB Galerie



enerj-meeting.com

Un événement [**batiactu**]
GROUPE



Avancements de la Cybersécurité pour la Convergence IT/OT avec BACnet/SC

De nos jours, les bâtiments connaissent un rôle de plus en plus important dans notre vie, où nous passons plus de la moitié de notre existence. Le changement climatique devenant de plus en plus perceptible et mesurable, s'ajoute à la complexité du sujet dans un pays dans lequel le bâti est considéré comme une œuvre pour les architectes. Le bâtiment est aussi un héritage, un patrimoine et une vitrine connue et reconnue pour les Français et les visiteurs de plus en plus nombreux.

Les contraintes des bâtiments neufs et existants sont multiples et elles deviennent les leviers d'actions pour leur amélioration et leur évolution. La réglementation est une imposition qui va dans ce sens.

Les principaux leviers restent les mêmes depuis des décennies et se complètent, en ordre chronologique :

- L'efficacité énergétique (l'énergie consommée doit être minime)
- Réduction de l'empreinte carbone (minime pour lutter contre le réchauffement climatique)
- Économie circulaire pour réduire l'impact écologique du bâtiment
- CYBERSÉCURITÉ

La dernière contrainte devient une condition sine qua non pour assurer les trois précédentes. Les trois premières sont très impactantes pour l'enveloppe, les équipements et leurs usages. L'utilisation des équipements par contre concerne la cybersécurité, les BACS qui assurent les usages et les moyens de communication

afférents sont concernés. De ce point de vue, la cybersécurité est la nouvelle colonne vertébrale de nos bâtiments intelligents.

Pendant longtemps, la sécurité d'un bâtiment se mesurait à ses accès physiques, ses alarmes incendie, ses contrôles d'intrusion. Aujourd'hui, elle se mesure aussi – et de plus en plus – à la robustesse de son réseau de supervision. Un automate de CVC compromis, une passerelle BACnet exposée sans protection, un firmware jamais mis à jour : autant de portes dérobées vers des infrastructures qui, hier encore, semblaient à l'abri du monde numérique. Ce temps est révolu.

Le protocole BACnet a été pensé, à l'origine, pour l'interopérabilité – pas pour résister à un environnement hostile. C'est précisément pour combler cet écart que BACnet/SC (Secure Connect) a été développé : chiffrement des échanges, authentification mutuelle par certificats, intégrité des communications de bout en bout. Ce n'est plus une option réservée aux projets sensibles, c'est en train de devenir le socle attendu de toute nouvelle installation de gestion technique de bâtiment.

Notre rôle, en tant qu'association, n'est pas seulement de suivre cette évolution mais de l'accompagner activement auprès de nos membres et partenaires économiques du bâtiment : intégrateurs, fabricants, bureaux d'études, exploitants, architectes, consultants, ... Cela signifie informer et former aux nouvelles pratiques de déploiement de certificats, sensibiliser les maîtres d'ouvrage aux risques

d'un parc d'automates hérité et non sécurisé, et pousser les fabricants à intégrer BACnet/SC nativement plutôt qu'en option coûteuse et tardive. La cybersécurité d'un bâtiment ne se rattrape pas après coup – elle se conçoit dès l'architecture réseau, dès le cahier des charges.

Les chiffres qui circulent sur les cyberattaques visant les systèmes industriels et tertiaires ne sont plus des abstractions lointaines : ils concernent directement les infrastructures que nos membres conçoivent, installent et exploitent chaque jour. Un hôpital, un data center, un immeuble de bureaux tertiaires – tous partagent désormais la même exigence : la disponibilité et l'intégrité de leur supervision technique sont aussi critiques que leur alimentation électrique.

Ce numéro du journal consacre plusieurs articles et une large place à ces enjeux, avec des retours d'expérience concrets sur les migrations vers BACnet/SC et les bonnes pratiques de durcissement des réseaux de terrain. Des documents ANSSI à jour sont explicités avec les conséquences pour BACnet/SC. Je vous invite à les lire avec l'idée que la sécurité n'est pas un frein à l'innovation, mais sa condition de pérennité. Un bâtiment intelligent qui ne protège pas ses communications n'est, in fine, qu'un bâtiment vulnérable et connecté.

Rejoignez-nous dans cette action, en devenant membres de BACnet France. Contactez donc notre Délégué Général, Mr Florent Trochu, en écrivant à florent.trochu@acr-regulation.com. À suivre aussi l'espace BACnet/SC sur notre site web www.bacnetfrance.org

Jean Daniel Napar
Président BACnet France



Édito

Avancements de la Cybersécurité pour la Convergence IT/OT avec BACnet/SC

3

Dossier Cybersécurité

La réglementation française de la cybersécurité : où en est-on en août 2026 ?

5

Sécuriser BACnet n'est plus une option, c'est une obligation d'ingénierie

Migration vers BACnet/SC : méthode et retours de terrain

7

Référentiels ANSSI – Décryptage et liaison avec BACnet/SC

9

BACnet/SC pour les nuls

11

Tendances et évolutions technologiques

Poursuivre le déploiement massif de BACS performants, pérennes, réglementaires et cyber-sécurisés avec BACnet !

12

Performance énergétique et cybersécurité : comment concilier les deux enjeux majeurs du bâtiment moderne ?

14

Données BACnet et IA : détecter l'anormal avant l'incident

16

Une GTB « cybersécurisée » pour un opérateur d'importance vitale

18

L'humain, facteur clé de succès pour l'intégration d'une GTB

20

Références

Initiation des futurs techniciens à la sécurisation des communications numériques

22

Gestion intelligente des bâtiments pour les PME : comment les petits et moyens projets immobiliers bénéficient de solutions de GTB rentables

7

26

Rénovation GTB-CFA du site CARAT 1 (A & B) – Projet livré en 2025 à Châtillon (92)

9

27

REIWA : BACnet au cœur d'une architecture ouverte au service de la performance énergétique

11

28

Produits

ecos : des automates polyvalents et intelligents pour l'automatisation de locaux

12

30

BACnet News

De la formation à l'intégration GTB : préparer les futurs experts des bâtiments communicants

16

32

Notes de la rédaction

34



Dix-neuvième édition | Octobre 2026

Photo de couverture
Campus de Beaulieu - Bâtiment de l'ISTIC
© Université de Rennes

A télécharger sur
www.bacnetfrance.org
www.bacnetjournal.org

La réglementation française de la cybersécurité : où en est-on en août 2026 ?

Un cadre encore en gestation, mais déjà opérant dans les faits

La réglementation française en matière de cybersécurité suit les Directives européennes NIS2 (sécurité réseaux et des systèmes d'information) et CRA (réglementation sur la cyber-résilience). La transposition réglementaire peut avoir des spécificités françaises.

À la rentrée 2026, la France reste l'un des quatre États membres de l'Union Européenne à ne pas avoir formellement transposé la directive NIS2, aux côtés de l'Irlande, de l'Espagne et des Pays-Bas. Le texte porteur de cette transposition, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité – dit « loi Résilience » –, a été adopté par le Sénat dès mars 2025, mais son examen par l'Assemblée nationale a de nouveau glissé, reporté au mieux à la rentrée parlementaire de septembre 2026. La Commission européenne a saisi la Cour de justice de l'Union européenne à l'encontre des États retardataires, avec, à la clé, des astreintes financières potentielles.

Ce retard législatif ne doit toutefois pas donner l'illusion d'un vide juridique confortable. D'une part, la directive NIS2 elle-même s'applique déjà au niveau européen depuis octobre 2024, indépendamment du calendrier français. D'autre part, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) n'a pas attendu le vote de la loi pour outiller les futurs assujettis : elle a publié, le 17 mars 2026, son Référentiel Cyber France (ReCyF), qui recense les mesures recommandées pour atteindre les objectifs de sécurité fixés par NIS2, et met à disposition le portail MonEspaceNIS2, avec un simulateur d'éligibilité et des outils d'autoévaluation. L'appareil dans un mot technique de la conformité fonctionne déjà : seul son habillage législatif et ses sanctions restent suspendus au vote du Parlement.

Un changement d'échelle : de 500 à 15 000 entités régulées

L'ampleur du changement à venir mérite d'être mesurée. Le régime antérieur, issu de la loi de programmation militaire et de la directive NIS1, concernait environ 500 entités régulées en

France – essentiellement des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels déjà identifiés de longue date. Avec la transposition de NIS2, ce sont désormais près de 15 000 entités qui entreront dans le champ de la régulation, classées en deux catégories : entités « essentielles » et entités « importantes », réparties sur dix-huit secteurs critiques – santé, énergie, transport, eau, infrastructures numériques, et bien d'autres où les systèmes de gestion technique du bâtiment jouent un rôle opérationnel de premier plan.

Ce changement d'échelle transforme la nature même de l'exercice de conformité. Il ne s'agit plus d'un cercle restreint de grands opérateurs disposant de moyens dédiés à la cybersécurité, mais d'un ensemble beaucoup plus large d'organisations – hôpitaux de taille intermédiaire, gestionnaires de parcs immobiliers tertiaires, exploitants de data centers régionaux – pour qui la sécurisation des systèmes d'information, y compris ceux qui pilotent le bâtiment, devient une obligation légale et non plus seulement une bonne pratique.

Ce que la loi imposera concrètement

L'article 14 du projet de loi transpose l'article 21 de la directive NIS2 : les entités essentielles et importantes devront prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées au regard des risques auxquels elles sont exposées. Le principe de proportionnalité est ici central et directement transposé dans le ReCyF : le niveau d'exigence attendu varie selon que l'entité est classée « essentielle » ou « importante », l'ANSSI donnant l'exemple d'exigences allégées en matière de sauvegardes pour les entités les moins critiques. Ce référentiel reste, à ce stade, non obligatoire par défaut, mais son application volontaire permettra aux entités assujetties de s'en prévaloir en cas de contrôle de l'ANSSI – une manière, pour l'administration, d'inciter à l'anticipation avant même l'entrée en vigueur des sanctions.

Ces obligations couvrent l'ensemble du système d'information de l'entité régulée – une formulation qui, dans la pratique, n'exclut pas les réseaux de gestion technique du bâtiment. Un

automate de CVC connecté, une passerelle de supervision exposée sur le réseau IT de l'organisation, un système de contrôle d'accès interfacé au système d'information : ces éléments relèvent, au sens de la directive, du périmètre à sécuriser, dès lors qu'ils participent du fonctionnement de l'entité régulée. C'est là que la frontière entre obligations réglementaires générales et pratiques métier de la GTB cesse d'être une question théorique.

Ce que cela signifie pour nos membres et le marché

Pour les intégrateurs, fabricants et bureaux d'études qui interviennent sur des sites appelés à devenir des entités essentielles ou importantes – établissements de santé, sites industriels, gestionnaires de grands parcs tertiaires –, l'enjeu n'est plus de se demander « si » la cybersécurité des systèmes BACnet sera un jour un sujet de conformité, mais de constater qu'elle l'est déjà en pratique, avant même le vote définitif de la loi. Les donneurs d'ordre engagés dans une démarche d'anticipation via MonEspaceNIS2 commencent à interroger leurs prestataires sur la robustesse de leurs installations de GTB : authentification des équipements, chiffrement des échanges, traçabilité des accès.

Des réponses techniques existent déjà et sont directement mobilisables dans ce cadre réglementaire encore en formation. BACnet/SC, avec son authentification mutuelle par certificats et son chiffrement TLS des communications, répond directement aux catégories de mesures que recense le ReCyF – authentification des identités, protection des communications, gestion des accès. Le référentiel de l'ANSSI n'impose pas de solution technique nommée, mais les objectifs qu'il fixe convergent avec ce que BACnet/SC apporte structurellement au réseau de terrain.

Le Cyber Resilience Act : ce que les fabricants de matériel BACnet doivent anticiper

Un règlement qui déplace la responsabilité vers la source

Jusqu'ici, la plupart des textes de cybersécurité examinés dans ce journal – NIS2, ReCyF, le

guide ANSSI GTB/GTC – s'adressent aux exploitants et aux intégrateurs : ce sont eux qui doivent sécuriser des installations construites avec du matériel dont la robustesse native n'est pas garantie. Le Cyber Resilience Act (CRA), règlement européen entré en vigueur le 10 décembre 2024, change cette focale : il s'adresse directement aux fabricants de produits comportant des éléments numériques, et impose des exigences de sécurité dès la conception, avant même la mise sur le marché. C'est le texte qui, structurellement, répond à la critique souvent adressée aux guides précédents – que la charge de sécurisation retombe uniquement sur celui qui achète et exploite le matériel.

Le CRA couvre un périmètre volontairement très large : tout produit matériel ou logiciel connecté, dès lors qu'il est susceptible d'échanger des données avec un réseau ou un autre appareil. Les automates de GTB, les contrôleurs BACnet, les passerelles de supervision et les logiciels de gestion technique entrent sans ambiguïté dans ce périmètre – un fabricant de matériel BACnet vendant dans l'Union européenne devient un fabricant assujéti au CRA, au même titre qu'un fabricant d'objet connecté grand public.

Un calendrier en quatre échéances, pas une seule

Le CRA ne bascule pas en un seul jour : son application se déploie sur quatre échéances distinctes, dont deux sont déjà derrière nous et deux restent à venir.

- 10 décembre 2024 – entrée en vigueur du règlement, ouvrant la période transitoire.
- 11 juin 2026 – mise en place des organismes notifiés chargés d'évaluer la conformité des produits, une étape déjà franchie qui structure l'écosystème de certification à venir.
- 11 septembre 2026 – entrée en application des obligations de notification des vulnérabilités activement exploitées : tout fabricant devra signaler à l'ENISA et au CSIRT compétent, sous 24 heures pour une notification d'alerte précoce, toute vulnérabilité exploitée activement dans l'un de ses produits.
- 11 décembre 2027 – application complète du règlement, incluant l'ensemble des exigences de sécurité par conception, la documentation technique et le marquage CE cybersécurité.

Pour les fabricants qui lisent ce journal, la date qui doit retenir l'attention immédiate est celle de septembre 2026 : l'obligation de notifica-

tion rapide des vulnérabilités exploitées s'applique dans les prochains jours, alors même que l'échéance de décembre 2027, plus lointaine, concentre encore l'essentiel de l'attention du secteur.

Ce que le CRA exigera des fabricants de matériel BACnet

À l'échéance de décembre 2027, un fabricant de produits connectés devra démontrer, pour chaque produit mis sur le marché européen, une sécurité intégrée dès la conception : gestion sécurisée des mises à jour, absence de vulnérabilités connues exploitables au moment de la commercialisation, mécanismes d'authentification appropriés, et une politique de gestion des vulnérabilités maintenue pendant toute la durée de support annoncée du produit. Un dossier de documentation technique devra être constitué et tenu à disposition des autorités de surveillance du marché, retraçant l'analyse de risque effectuée et les mesures de sécurité mises en œuvre.

Pour un fabricant d'automates ou de passerelles BACnet, cela signifie concrètement : documenter la capacité – ou l'incapacité – d'un produit à supporter BACnet/SC et son cycle de mise à jour firmware, formaliser une procédure de traitement des vulnérabilités remontées par la communauté ou par des tiers, et anticiper l'intégration d'un marquage de conformité cybersécurité en plus du marquage CE existant. Les produits qui ne pourront pas démontrer cette maîtrise à l'échéance de 2027 risquent, à terme, de ne plus pouvoir être commercialisés sur le marché européen – une perspective qui doit peser dès aujourd'hui dans les feuilles de route produit des fabricants.

Une convergence à lire avec NIS2, pas en silo

Le CRA et NIS2 ne sont pas deux textes indépendants pour notre filière : ils couvrent les deux faces d'une même chaîne de responsabilité. NIS2 impose à l'exploitant régulé de sécuriser son système d'information, y compris ses systèmes de GTB. Le CRA impose au fabricant de livrer un produit dont la sécurité native limite précisément l'effort que l'exploitant devra ensuite déployer. Un automate conforme au CRA, doté d'une gestion native des mises à jour et d'une politique de vulnérabilités documentée, réduit d'autant la charge de sécurisation que l'exploitant devra assumer pour être conforme à NIS2 – et inversement, un matériel qui ne répond pas au CRA reporte cette charge intégralement sur l'intégrateur et l'exploitant, exactement le schéma

critiqué à propos du guide ANSSI GTB/GTC.

Ce que nos membres fabricants doivent engager dès maintenant

Pour les fabricants membres de l'association, l'échéance de septembre 2026 sur la notification des vulnérabilités actives n'est plus une perspective : elle est immédiate. Il est temps de vérifier qu'un point de contact et une procédure de remontée vers l'ENISA sont opérationnels, de cartographier les gammes de produits qui entrent dans le périmètre du règlement, et d'engager, dès maintenant, les travaux de mise en conformité visant l'échéance de décembre 2027 – un délai qui, à l'échelle d'un cycle de développement produit industriel, laisse moins de marge qu'il n'y paraît.

Anticiper plutôt que subir

Le message que porte ce numéro est simple : le flou du calendrier législatif ne doit pas être confondu avec l'absence d'obligation. L'ANSSI a publié ses outils, la Commission européenne fait pression sur le calendrier français, et les entités qui seront demain classées essentielles ou importantes commencent déjà, aujourd'hui, à revoir leurs exigences vis-à-vis de leurs prestataires. Pour nos membres, l'anticipation de ces exigences – plutôt que l'attente passive de la promulgation de la loi – constitue le meilleur levier pour transformer une contrainte réglementaire en avantage concurrentiel.

Rejoignez-nous dans cette action, devenant membres de BACnet France. Contactez donc notre Délégué Général, Mr Florent Trochu, en écrivant à florent.trochu@acr-regulation.com. À suivre aussi l'espace BACnet/SC sur notre site web www.bacnetfrance.org.

Sécuriser BACnet n'est plus une option, c'est une obligation d'ingénierie

Il faut le dire sans détour : une part significative du parc de superviseurs et d'automates déployés aujourd'hui communique encore en clair, sur des réseaux BACnet/IP non segmentés, sans authentification des équipements ni chiffrement des trames. Ce constat n'est pas une hypothèse théorique – c'est l'état réel de nombreuses installations tertiaires, hospitalières et industrielles que nos membres audient chaque année. Un attaquant disposant d'un accès réseau – via un poste de télémaintenance mal isolé, un réseau invité mal cloisonné ou un automate exposé sur Internet – peut lire, rejouer ou falsifier des trames BACnet sans rencontrer aucune résistance protocolaire. Ce n'est plus un risque résiduel, c'est une surface d'attaque documentée.

BACnet/SC (Secure Connect), normalisé dans l'Addendum BACnet 135-2020, change cette donne structurellement. Il ne s'agit pas d'un correctif superficiel mais d'un changement de couche de transport : abandon de la diffusion UDP au profit de connexions WebSocket sur TLS 1.3, authentification mutuelle par certificats X.509 entre chaque nœud, et une architecture de confiance reposant sur une autorité de certification propre au site ou à l'organisation.

Concrètement, cela signifie la fin des BBMD non authentifiés et la possibilité réelle de faire transiter le trafic BACnet sur des infrastructures IP partagées, y compris via des passerelles cloud, sans exposer le protocole nu.

Cette évolution s'inscrit dans un cadre normatif plus large que nos membres ne peuvent plus ignorer. La norme IEC 62443, référentiel de cybersécurité des systèmes d'automatisation et de contrôle industriels (IACS), impose une logique de zones et conduits, de niveaux de sécurité (SL 1 à 4) et d'exigences par composant (IEC 62443-4-2) que les fabricants d'équipements BACnet doivent désormais intégrer dès la conception. La directive NIS2, élargit par ailleurs le périmètre des entités soumises à obligation de sécurité des réseaux à nombre de gestionnaires de bâtiments tertiaires et d'exploitants d'infrastructures critiques – hôpitaux, data centers, sites industriels classés. La conformité protocolaire n'est plus dissociable de la conformité réglementaire.

Or la migration vers BACnet/SC ne se décrète pas au niveau du seul protocole. Elle exige une gestion du cycle de vie des certificats (émission, renouvellement, révocation), un inventaire précis

des dispositifs hérités incapables de supporter TLS, et bien souvent une architecture hybride BACnet/IP classique et BACnet/SC coexistant via des routeurs de passerelle le temps de la transition. C'est un chantier d'ingénierie réseau à part entière, pas une simple mise à jour de firmware.

L'association BACnet France a engagé depuis mars 2024 un effort renforcé d'information et d'accompagnement sur le déploiement de BACnet/SC et sur la lecture opérationnelle d'IEC 62443 à l'usage des intégrateurs. Ce numéro en présente aussi les premiers retours de terrain. Notre conviction est simple : un système d'automatisation du bâtiment qui ne peut pas prouver l'identité de ses propres nœuds n'est plus un système fiable, quelle que soit par ailleurs la qualité de sa régulation.

Rejoignez-nous dans cette action, devenant membres de BACnet France. Contactez donc notre Délégué Général, Mr Florent Trochu, en écrivant à florent.trochu@acr-regulation.com. À suivre aussi l'espace BACnet/SC sur notre site web www.bacnetfrance.org.

Migration vers BACnet/SC : méthode et retours de terrain

Un chantier réseau, pas une mise à jour de firmware

La migration de BACnet/IP vers BACnet/SC est assurée par conception !

La seule condition de bon sens et conseillée est de faire la migration après que le projet fonctionne selon le cahier de charge en BACnet/IP ! Ceci évite des heures d'ingénierie et efforts coûteux et inutiles !

Migrer un parc BACnet/IP vers BACnet/SC est

souvent présenté, à tort, comme une opération de mise à niveau logicielle. Dans les faits, c'est un projet d'architecture réseau à part entière, qui touche à la fois le terrain (automates, contrôleurs, passerelles), l'infrastructure IT (autorité de certification, segmentation, supervision) et l'organisation (répartition des responsabilités entre exploitant, intégrateur et service informatique). Les retours d'expérience convergent sur un point : les projets qui échouent ou qui s'enlisent sont presque toujours ceux qui ont sous-estimé cette dimension d'ingénierie au profit d'une approche « on bascule un équipement à la fois ».

Ce constat appelle une méthode structurée, que l'on peut décomposer en quatre phases : l'audit du parc existant, la conception de l'architecture cible, le déploiement progressif en cohabitation, puis la gouvernance du régime permanent.

Phase 1 – Auditer avant de migrer

Aucune migration sérieuse ne commence par l'achat de certificats. Elle commence par un inventaire précis du parc : quels automates, quelles versions de firmware, quels fabricants supportent nativement TLS et la pile WebSocket

exigée par BACnet/SC, et lesquels ne le supporteront jamais faute de puissance de calcul suffisante. Cet inventaire doit être croisé avec une cartographie réseau réelle – et non la cartographie théorique du schéma d'installation d'origine, souvent obsolète après plusieurs années d'exploitation et d'ajouts successifs.

Cet audit révèle presque systématiquement trois catégories d'équipements : ceux qui peuvent migrer par simple mise à jour de firmware, ceux qui nécessitent un remplacement de carte de communication, et ceux – souvent les plus anciens – qui ne migreront jamais et devront être traités par une passerelle de protocole jusqu'à leur remplacement en fin de vie. Établir cette cartographie avant de fixer un calendrier de projet évite l'écueil le plus fréquent : découvrir, en cours de déploiement, qu'un tiers du parc est incompatible et remettre en cause le budget et le planning initiaux.

Phase 2 – Concevoir l'architecture cible

BACnet/SC repose sur un modèle hub-and-spoke : un hub central – avec, recommandé pour toute installation critique, un hub de secours en redondance – distribue les messages entre les nœuds du réseau. Concevoir cette architecture cible suppose de répondre à plusieurs questions structurantes avant tout déploiement : combien de hubs faut-il par site ou par bâtiment ? Où sont-ils hébergés – sur une infrastructure serveur dédiée à la GTB ou mutualisée avec l'infrastructure IT générale ? Qui porte la responsabilité de leur disponibilité ?

La question de l'autorité de certification est ici centrale et trop souvent traitée en fin de projet plutôt qu'en amont. Chaque nœud et chaque hub du réseau BACnet/SC doit disposer d'un certificat X.509 signé par une autorité de confiance commune. Deux options s'offrent aux organisations : s'appuyer sur une PKI d'entreprise déjà existante – lorsque le service IT en dispose et accepte d'ouvrir un usage GTB – ou déployer une autorité de certification dédiée au périmètre bâtiment. La seconde option, plus autonome pour l'équipe GTB, exige néanmoins une compétence de gestion de cycle de vie de certificats qui n'existait pas dans le monde BACnet/IP traditionnel.

Phase 3 – Déployer en cohabitation

Un basculement intégral d'un site en une seule opération est rarement réaliste, sauf sur une installation neuve. La quasi-totalité des migrations réelles passe par une phase de cohabitation hybride, où coexistent des segments BACnet/IP

classiques et des segments BACnet/SC, reliés par des routeurs de passerelle assurant la traduction entre les deux mondes. Cette période transitoire peut s'étendre sur plusieurs années pour un patrimoine immobilier de taille significative, au rythme des remplacements de parc et des disponibilités budgétaires.

Cette cohabitation impose une vigilance particulière sur un point souvent négligé : le segment BACnet/IP restant, tant qu'il n'a pas migré, conserve l'intégralité des vulnérabilités qui ont motivé le projet – absence de chiffrement, absence d'authentification. La segmentation réseau du segment non encore migré, via des VLAN dédiés et un contrôle d'accès strict aux passerelles, devient donc une mesure compensatoire indispensable pendant toute la durée de la transition, et non une option secondaire.

Phase 4 – Gouverner le régime permanent

Une fois le déploiement achevé, la migration ne s'arrête pas : elle entre dans un régime de gouvernance continue que le monde BACnet/IP n'exigeait pas. Les certificats ont une durée de vie limitée et doivent être renouvelés avant expiration, sous peine de coupure de communication d'un équipement critique. Une procédure de révocation rapide doit être opérationnelle pour retirer immédiatement la confiance à un équipement suspecté compromis ou physiquement remplacé sans désinstallation propre. Cette gouvernance suppose des outils de suivi – le monitoring des dates d'expiration à l'échelle du parc devient vite ingérable sans outillage dédié dès lors que le nombre de nœuds dépasse quelques dizaines d'unités.

C'est à ce stade que la question du partage de responsabilités entre l'équipe GTB et le service IT se pose avec le plus d'acuité. La gestion d'une autorité de certification, la supervision des expirations, la procédure de révocation : ce sont des compétences historiquement IT, que l'équipe bâtiment doit soit acquérir, soit déléguer formellement par une convention de service claire avec la DSI. Les projets qui laissent cette question non tranchée accumulent, avec le temps, une dette opérationnelle qui finit par se traduire par des pannes de communication au moment le moins opportun – un certificat expiré un vendredi soir n'attend pas la prochaine réunion de comité de pilotage.

Ce que les retours de terrain enseignent

Trois enseignements reviennent, projet après projet, chez les intégrateurs qui ont mené des migrations BACnet/SC à terme :

Le budget temps est systématiquement sous-estimé côté organisation, jamais côté technique. Le remplacement matériel et la configuration des hubs se planifient bien ; la mise en place d'une gouvernance de certificats pérenne, elle, est presque toujours découverte en cours de route.

Une migration pilote sur un bâtiment ou une aile limitée vaut mieux qu'un déploiement massif d'emblée. Elle permet de calibrer les procédures de certificats et la charge d'exploitation réelle avant de généraliser, et d'ajuster le budget prévisionnel sur des bases mesurées plutôt qu'estimées.

L'implication du service IT dès la phase de conception, et non au moment du déploiement, conditionne la fluidité du projet. Les migrations qui échouent à obtenir cette implication en amont se heurtent, en aval, à des blocages sur l'ouverture de ports, la gestion de la PKI ou la supervision réseau – des sujets que l'équipe GTB seule ne peut pas trancher.

Conclusion : une migration qui se pilote comme un projet d'infrastructure

Migrer vers BACnet/SC n'est pas un basculement binaire mais une trajectoire, dont la durée et la complexité dépendent directement de la qualité de préparation initiale. Les organisations qui réussissent ce chantier sont celles qui l'abordent avec les réflexes d'un projet d'infrastructure IT – audit préalable, architecture cible documentée, déploiement progressif maîtrisé, gouvernance pérenne – plutôt qu'avec ceux d'une simple campagne de mise à jour d'équipements. C'est cette rigueur méthodologique, plus que la seule disponibilité technique du protocole, qui déterminera la vitesse à laquelle notre filière achèvera cette transition.

L'action d'information/formation/conseil est donc une action prioritaire pour l'association BACnet France, en vue du parc installé en France en BACnet.

Rejoignez-nous dans cette action, devenant membres de BACnet France. Contactez donc notre Délégué Général, Mr Florent Trochu, en écrivant à florent.trochu@acr-regulation.com. À suivre aussi l'espace BACnet/SC sur notre site web www.bacnetfrance.org

Référentiels ANSSI – Décryptage et liaison avec BACnet/SC

Cet article propose le décryptage de deux référentiels publiés par l'ANSSI, à savoir :

- ReCyF – Référentiel Cyber France – issu le 17 mars 2026
- Recommandations de sécurité relatives à la gestion technique et centralisée du bâtiment (GTB/GTC) – issu le 27 avril 2026

Le décryptage consiste, en dehors d'une lecture compréhensible des contenus, à faire la liaison et donner les conséquences pour BACnet/SC.

Le ReCyF, référentiel ANSSI pour NIS2 : ce que la GTB doit en retenir

Un document d'accompagnement avant d'être une obligation

Depuis le 17 mars 2026, l'ANSSI met à disposition le Référentiel Cyber France (ReCyF), diffusé pour l'instant en version de travail. Ce document n'est pas encore un texte contraignant : il correspond au référentiel de cybersécurité mentionné à l'article 14 du projet de loi Résilience, celui-là même qui transpose l'article 21 de la directive NIS2 en droit français. Tant que la loi n'est pas promulguée, le ReCyF reste, par défaut, non obligatoire. Mais l'ANSSI a construit un mécanisme incitatif clair : les entités qui décident de l'appliquer dès maintenant pourront s'en prévaloir en cas de contrôle ultérieur de l'agence. Anticiper le référentiel n'est donc pas un exercice gratuit – c'est un investissement qui pourra se faire valoir le jour où le régime deviendra pleinement contraignant.

Le ReCyF a une vocation claire : traduire les objectifs de sécurité fixés par NIS2 en mesures concrètes et vérifiables, applicables à l'ensemble du système d'information de l'entité régulée – ce qui, on le verra, ne laisse pas les systèmes de gestion technique du bâtiment hors périmètre.

Une architecture en vingt objectifs, répartis en deux niveaux d'exigence

Le référentiel s'organise autour de vingt objectifs de sécurité, regroupés en quatre blocs thématiques couvrant la gouvernance de la sécurité numérique, la protection des systèmes, la défense face aux incidents et la résilience opérationnelle. Sa structure repose sur une distinction volontairement simple à appliquer : les quinze premiers objectifs s'imposent à toutes les entités régulées, qu'elles soient classées « importantes » (EI) ou « essentielles » (EE). Les

cinq objectifs suivants, relevant d'un niveau de maturité plus avancé, ne concernent que les entités essentielles – celles dont la défaillance aurait un impact jugé plus critique sur la société ou l'économie.

Cette architecture différenciée matérialise directement le principe de proportionnalité qui irrigue tout le texte : le niveau d'effort de sécurisation demandé varie selon la criticité réelle de l'entité, plutôt que d'imposer un socle uniforme à des organisations aux moyens et aux enjeux très inégaux. L'ANSSI illustre ce principe par des exemples concrets – les exigences relatives aux sauvegardes, par exemple, sont volontairement allégées pour les entités les moins critiques. C'est un choix de méthode assumé : ne pas noyer une PME sous des exigences taillées pour un opérateur d'importance vitale, tout en maintenant un plancher de sécurité commun à tous.

Un outillage déjà disponible, indépendant du calendrier législatif

Au-delà du document lui-même, l'ANSSI a mis en ligne un outil de comparaison de référentiels, qui permet de rapprocher les exigences du ReCyF d'autres normes ou référentiels déjà en usage – une aide précieuse pour les organisations déjà engagées dans une démarche ISO 27001 ou dans un dispositif sectoriel existant, qui peuvent ainsi identifier les écarts réels plutôt que repartir d'une feuille blanche. Le portail MonEspaceNIS2, accessible sur cyber.gouv.fr, complète ce dispositif avec un simulateur d'éligibilité permettant à une organisation de déterminer si elle sera vraisemblablement classée entité essentielle, importante, ou hors périmètre, ainsi que des modèles de documentation pour structurer la démarche de mise en conformité.

Ce découplage entre l'outillage technique, disponible dès aujourd'hui, et le calendrier législatif, toujours suspendu à l'examen parlementaire, est un point que l'ANSSI a explicitement assumé : les organisations concernées sont invitées à engager leur démarche de sécurisation sans attendre la version finale du texte, la logique du référentiel n'étant pas appelée à changer substantiellement d'ici sa consolidation définitive.

Ce que le ReCyF signifie pour les systèmes de gestion technique du bâtiment

Le référentiel s'applique à l'ensemble du système d'information de l'entité régulée – une formulation qui, dans la pratique, ne distingue pas le système d'information « bureautique » du système de gestion technique du bâtiment dès lors que celui-ci participe au fonctionnement de l'entité. Un automate CVC connecté au réseau de l'organisation, une passerelle de supervision accessible depuis le système d'information général, un contrôle d'accès interfacé aux annuaires de l'entreprise : ces éléments relèvent, au sens du ReCyF, du périmètre à sécuriser au même titre que n'importe quel serveur applicatif.

Les objectifs du socle commun – authentification des utilisateurs et des équipements, protection des communications, gestion des accès, journalisation et détection des incidents – trouvent une correspondance directe avec ce qu'apporte BACnet/SC au niveau du réseau de terrain : authentification mutuelle par certificats X.509, chiffrement TLS des échanges, architecture de confiance centralisée autour d'un hub. Le référentiel ne prescrit pas de solution technique nommément – il fixe des objectifs de sécurité, pas un cahier des charges protocolaire – mais la cohérence entre les deux démarches est directe pour qui les lit en parallèle.

Une invitation à agir, pas à attendre

Pour nos membres, le message porté par le ReCyF est sans ambiguïté : la version de travail publiée en mars 2026 constitue déjà une base de travail suffisamment stable pour engager les premiers audits de conformité, en particulier sur le périmètre GTB, trop souvent absent des premières cartographies de risque établies par les directions des systèmes d'information. Attendre la promulgation définitive de la loi Résilience pour engager cette démarche revient à retarder un chantier dont l'ANSSI a déjà donné le mode d'emploi – un luxe que peu d'organisations, au vu de l'ampleur du parc à sécuriser, peuvent réellement se permettre.

Le guide ANSSI GTB/GTC : la doctrine officielle enfin publiée

Une première doctrine publique pour un angle mort de la cybersécurité

Le 27 avril 2026, l'ANSSI a publié son guide « Recommandations de sécurité relatives à la gestion technique et centralisée du bâtiment (GTB/GTC) », référencé ANSSI-PA-110. Ce document de quarante pages constitue la première doctrine publique de l'agence spécifiquement consacrée à la cybersécurité des GTB/GTC – jusqu'ici traitées, au mieux, en marge des guides plus généraux sur les systèmes industriels. Il s'appuie largement sur des exemples issus du monde hospitalier et de la santé, tout en restant applicable à d'autres secteurs – laboratoires, sites manufacturiers, tertiaire sensible.

Le constat de départ que pose l'ANSSI est moins technique qu'organisationnel. Contrairement aux systèmes informatiques classiques, pilotés par un DSI et intégrés aux politiques de sécurité de l'entreprise, la GTB est très souvent gérée sous forme de prestation externalisée, confiée à un prestataire de maintenance qui intervient sur un périmètre que les services techniques internes connaissent mal, voire pas du tout. Cette externalisation, couplée à une méconnaissance du périmètre exact de l'installation par l'entité qui en est responsable, constitue selon l'agence la cause première de la vulnérabilité structurelle du secteur – bien avant les failles protocolaires elles-mêmes.

Vingt-six recommandations, une architecture cible en trois niveaux

Le guide décline vingt-six recommandations, assorties de deux annexes protocolaires détaillées. L'architecture de sécurité qu'il promeut repose sur un principe central : l'isolation stricte du réseau d'administration. Les recommandations R1 à R3 en posent le socle : séparer physiquement ou logiquement le réseau d'administration des automates du reste du système d'information, et, lorsque les outils d'administration fournis par les constructeurs n'intègrent pas nativement un chiffrement robuste – ce qui reste fréquent sur du matériel GTB –, encapsuler ces flux dans un tunnel VPN IPsec avec authentification mutuelle par certificats. Cette dernière disposition (recommandation alternative R3) est particulièrement significative : elle reconnaît explicitement que le parc installé ne peut pas, dans l'immédiat, se reposer sur la seule sécurité native des protocoles de terrain, et qu'un chiffrement de transport doit être ajouté

en périphérie tant que cette maturité protocolaire n'est pas atteinte.

Au-delà de ce socle réseau, le corps des recommandations suit une logique défense-in-depth classique – cloisonnement, filtrage des flux, durcissement des équipements, journalisation des événements, isolation des segments sensibles – appliquée spécifiquement aux contraintes du monde GTB : équipements aux capacités de calcul limitées, cycles de vie longs (quinze à vingt ans), et disponibilité continue plus critique que la confidentialité stricte des données échangées.

Les annexes protocolaires : Modbus et BACnet sous la loupe

Le guide consacre deux annexes détaillées à l'analyse de sécurité des protocoles de terrain les plus répandus. L'annexe consacrée à Modbus part d'un constat sans détour : le protocole n'intègre aucune fonction de cybersécurité native par défaut. L'ANSSI recommande en conséquence un filtrage strict, en exploitation normale, des codes fonction jugés à risque – en particulier ceux qui permettent l'écriture de registres ou la modification de paramètres de configuration, dont l'usage doit être exceptionnel et surveillé en production plutôt que permanent.

L'annexe consacrée à BACnet procède selon la même logique d'analyse par service et code fonction, avec une attention particulière portée aux mécanismes de découverte réseau (Who-Is/I-Am) et aux écritures de propriétés à distance, deux surfaces d'exposition classiques sur les installations BACnet/IP non segmentées. Cette approche par filtrage applicatif – plutôt que par simple isolation réseau – reflète une maturité d'analyse notable : elle traite le protocole non comme une boîte noire à cloisonner, mais comme un flux dont chaque fonction doit être évaluée au regard du risque qu'elle porte.

Il est spécifié clairement qu'il y aura une mise à jour concernant BACnet/SC dans une version à suivre. L'ANSSI se propose de faire des tests grandeur nature sur des produits réels des fabricants pour ce faire.

Une lecture critique, mais une base de travail solide

La publication de ce guide n'a pas manqué de susciter des commentaires plus critiques dans la communauté professionnelle, certains observateurs relevant que l'intégralité des vingt-six recommandations s'adresse à l'exploitant

ou à l'intégrateur – cloisonner, filtrer, durcir, journaliser – sans qu'aucune n'engage directement le fabricant du matériel sur des exigences de sécurité natives dès la conception. C'est une lecture qui a sa part de justesse : le guide décrit l'enveloppe de sécurité à construire autour d'un matériel dont la sécurité n'est pas, par construction, garantie à la source.

Cette limite n'invalide cependant pas l'apport du document. Pour la première fois, l'État dispose d'une doctrine publique, opposable en pratique dans les cahiers des charges et les audits, qui structure précisément ce que doit couvrir la sécurisation d'une installation GTB – et qui donne aux intégrateurs un langage commun avec les directions des systèmes d'information, trop souvent absentes des projets GTB jusqu'ici.

Ce que cela change pour nos membres

Ce guide s'inscrit dans la même dynamique que le référentiel ReCyF publié quelques semaines plus tôt pour NIS2 : l'ANSSI construit, guide après guide, l'outillage documentaire d'une conformité qui deviendra obligatoire pour un nombre croissant d'entités régulées. Les recommandations R1 à R3 sur l'isolation du réseau d'administration et le chiffrement des flux d'exploitation convergent directement avec ce qu'apporte BACnet/SC – authentification mutuelle par certificats, chiffrement natif des communications – sans attendre le déploiement d'un tunnel VPN en complément d'un protocole qui reste, lui, non sécurisé nativement.

Pour les intégrateurs qui répondent à des appels d'offres GTB dans le secteur de la santé ou sur des sites sensibles, ce guide devient, de fait, une référence à connaître et à citer : il fixe un niveau d'exigence que les maîtres d'ouvrage les mieux informés commencent déjà à intégrer dans leurs cahiers des charges, avant même que la réglementation NIS2 ne rende cette exigence formellement obligatoire.

L'action d'information/formation/conseil devient donc très importante pour l'Association BACnet France, et en même temps urgente pour la montée en puissance des acteurs économiques du bâtiment. La base installée de BACnet est la plus importante en France comparée à l'utilisation d'autres protocoles.

Rejoignez-nous dans cette action, devenant membres de BACnet France. Contactez donc notre Délégué Général, Mr Florent Trochu, en écrivant à florent.trochu@acr-regulation.com. À suivre aussi l'espace BACnet/SC sur notre site web www.bacnetfrance.org.

BACnet/SC pour les nuls

Un rappel technique nécessaire

À mesure que les échéances réglementaires se rapprochent – NIS2, le CRA, le guide ANSSI GTB/GTC – le sigle BACnet/SC revient dans toutes les conversations sans que sa mécanique interne soit toujours bien comprise. Avant d'aller plus loin dans nos analyses réglementaires, il paraît utile de revenir aux fondamentaux : que fait réellement BACnet/SC, et en quoi diffère-t-il de BACnet/IP classique ?

Le problème que BACnet/SC vient résoudre

BACnet, normalisé en 1995, a été conçu pour un objectif précis : garantir l'interopérabilité entre équipements de fabricants différents sur un même réseau de gestion technique du bâtiment. Sa version la plus répandue aujourd'hui, BACnet/IP, s'appuie sur le protocole UDP et diffuse ses messages sur un réseau IP classique, souvent partagé avec d'autres usages informatiques du bâtiment.

Cette conception n'a jamais intégré de mécanisme de sécurité natif. Les trames BACnet/IP circulent en clair : n'importe quel équipement présent sur le même segment réseau peut les lire, et rien n'empêche un émetteur de se faire passer pour un autre – il n'existe aucune authentification des équipements qui communiquent entre eux. Tant que les réseaux de GTB restaient physiquement isolés du reste du système d'information, cette absence de sécurité native restait un risque théorique. La convergence avec les réseaux IT et l'exposition croissante des installations à la supervision distante ont changé la donne : cette faiblesse protocolaire est devenue une vulnérabilité concrète et documentée.

Ce que change BACnet/SC : une nouvelle couche de transport

BACnet Secure Connect (BACnet/SC), défini par l'Addendum 135-2016bj à la norme BACnet, ne se contente pas d'ajouter un chiffrement en périphérie d'un protocole inchangé. Il remplace la couche de transport elle-même : au lieu de diffuser des trames UDP en clair, BACnet/SC établit des connexions WebSocket sur TLS entre les équipements. Concrètement, chaque échange devient une session point à point, chiffrée et authentifiée, alors que BACnet/IP diffusait ses messages en clair sur un segment réseau partagé.

Ce changement de transport apporte trois garanties que BACnet/IP classique n'offre pas :

- La confidentialité – les échanges sont chiffrés par TLS, ce qui empêche un tiers présent sur le réseau de lire le contenu des trames.
- L'authentification mutuelle – chaque équipement doit prouver son identité avant de pouvoir communiquer, grâce à un certificat numérique.
- L'intégrité des messages – un message modifié en transit est détecté et rejeté, ce qui empêche la falsification de commandes envoyées à un automate.

L'architecture : un modèle hub-and-spoke piloté par certificats

BACnet/SC repose sur une topologie hub-and-spoke : un hub central assure le routage des messages entre l'ensemble des nœuds du réseau, avec la possibilité de déployer un hub de secours pour la redondance sur les installations critiques. Des connexions directes entre deux nœuds, sans passer par le hub, restent possibles en option pour certains échanges nécessitant une latence minimale.

Ce qui rend cette architecture sûre, c'est le mécanisme d'authentification qui la sous-tend : chaque équipement du réseau – qu'il s'agisse d'un simple contrôleur de terrain ou du hub lui-même – doit disposer d'un certificat numérique (norme X.509) signé par une autorité de certification reconnue par l'ensemble du réseau. Lorsqu'un équipement tente d'établir une connexion, il présente son certificat ; le récepteur vérifie qu'il a bien été signé par l'autorité de confiance attendue avant d'accepter l'échange. Un équipement qui ne dispose pas d'un certificat valide ne peut, par construction, rejoindre le réseau – ce qui élimine le risque qu'un appareil non autorisé, branché sur le réseau physique, puisse se faire passer pour un automate légitime.

Une conséquence organisationnelle à ne pas sous-estimer

Cette architecture de confiance a une implication concrète pour ceux qui l'exploitent : gérer un réseau BACnet/SC, c'est gérer un cycle de vie de certificats – leur émission initiale, leur renouvellement avant expiration, et leur révocation rapide si un équipement est suspecté compromis ou remplacé sans procédure propre. C'est une compétence que le monde BACnet/IP traditionnel n'exigeait pas, et qui rapproche la gestion d'un réseau de GTB des pratiques classiques d'une direction des systèmes d'information.

Pourquoi ce protocole compte aujourd'hui plus qu'hier

BACnet/SC n'est plus un simple raffinement technique optionnel. Il répond directement aux objectifs que portent les textes réglementaires traités dans ce journal : authentification des équipements et chiffrement des communications figurent parmi les mesures attendues par le référentiel ReCyF de l'ANSSI pour la mise en conformité NIS2, et les recommandations du guide ANSSI GTB/GTC sur l'isolation des flux d'administration trouvent, avec BACnet/SC, une réponse native et par conception là où elles imposaient jusqu'ici un tunnel VPN ajouté en périphérie d'un protocole resté vulnérable. La compatibilité ascendante continue avec BACnet/SC, et donc l'investissement déjà fait pour BACnet sera préservé pour l'utilisateur.

Comprendre ce que fait réellement BACnet/SC – et pas seulement retenir qu'il s'agit de « la version sécurisée de BACnet » – est la condition pour engager une migration cohérente : un chiffrement mal compris se traduit vite par une architecture de certificats bâclée, qui finit par coûter plus cher en exploitation que la vulnérabilité qu'elle était censée corriger.



Dan Napar

Président BACnet France | Membre Advisory Group BIG-EU
dan.napar@outlook.com | DN Consulting

Poursuivre le déploiement massif de BACS performants, pérennes, réglementaires et cyber-sécurisés avec BACnet !

Après un été 2026 caniculaire et dans un contexte géopolitique de tensions durables pour l'accès aux énergies, le déploiement des produits et systèmes de régulation et gestion technique du bâtiments – i.e. Building Automation and Control Systems, BACS – est de plus en plus au centre des préoccupations des acteurs de la performance énergétique des bâtiments.

Dans l'exercice 2025 d'analyse statistique du marché des BACS, les industriels BACS réunis au sein du syndicat ACR confirment la bonne santé du secteur avec une croissance estimée à +3,5%, et souligne qu'elle repose principalement sur l'installation de solution BACS standards en rénovation, avec une dynamique plus forte dans le tertiaire, et une priorité donnée à la régulation des systèmes CVC. Ainsi, les fabricants associés à l'ensemble de la filière, notamment ceux réunis au sein de l'ALLIANCE BACS, font état de leur optimisme quant à la suite du développement pour les prochaines années, en insistant sur l'importance cruciale pour les nouveaux entrants sur ce marché, comme pour les acteurs historiques, de continuer à s'appuyer sur les référentiels standards de marché portés par ces organismes.

Il faut le rappeler sans cesse : le but des BACS est de maximiser le confort avec le minimum de consommation énergétique. Et pour ce faire, il est nécessaire de déployer des solutions permettant d'assurer une gestion de la consommation énergétique en fonction de la demande réelle, i.e. selon le niveau de confort demandé par l'utilisateur en situation réelle. Il s'agit alors de mettre en œuvre des BACS autorisant une communication bidirectionnelle entre les postes consommateurs d'énergie et ceux qui la produisent dans le bâtiment pour « produire uniquement l'énergie nécessaire au confort demandé ». Nos lecteurs habituels le savent, cette condition est remplie grâce à l'utilisation des protocoles de communication standardisés ouverts comme BACnet, KNX, etc. Cet objectif de gestion optimale de la consommation énergétique correspond désormais aux standards de marché pour les bâtiments neufs, mais il requiert une approche pragmatique par étape dans les bâtiments existants, en lien avec la réalité du rythme de rénovation des équipes

techniques du bâtiment et de son enveloppe. Pour utiliser la terminologie des normes en vigueur, notamment la norme NF EN ISO 52120-1:2022, il s'agit de faire passer progressivement le parc des bâtiments existants d'un fonctionnement manuel (BACS de classe D) à un niveau minimum réglementaire (BACS de classe C) puis à un niveau de performance haute (BACS de classes A et B) avec les systèmes de gestion en fonction de la demande réelle ou « demand-based control ».

En France, cette réalité technique et économique s'est traduite politiquement par le choix de reporter les exigences du Décret BACS II (« Décret n° 2023-259 du 7 avril 2023 relatif aux systèmes d'automatisation et de contrôle des bâtiments tertiaires ») à 2030. En effet, à la suite de l'entrée en vigueur au 1er janvier 2025 de l'obligation d'installer des BACS dans les bâtiments tertiaires équipés d'un système CVC d'une puissance supérieure à 290kW (cf Décret BACS I), les pouvoirs publics ont confirmé que la date d'abaissement du seuil à 70kW pour l'application obligatoire ne serait plus le 1er janvier 2027 comme initialement prévu, mais bien le 1er janvier 2030. On notera que cette disposition ne correspond ni plus ni moins qu'à un alignement avec les exigences de la Directive européenne révisée en 2024 (cf Directive Performance Énergétique des Bâtiments 2024 / 1275).

Ce report de calendrier ne doit pas néanmoins enrayer la dynamique de déploiement des BACS par la filière qui reste plus mobilisée que jamais pour contribuer à atteindre les objectifs réglementaires de réduction de la consommation énergétique des bâtiments et de leur poids carbone.

Les contraintes climatiques vécues dans leur chair par tout un chacun cet été, et qui continueront à s'aggraver dans les années à venir, constituent à la fois un rappel, si nécessaire, de l'importance de réduire la consommation énergétique des bâtiments pour lutter contre le réchauffement climatique, et de permettre de continuer à vivre confortablement dans ces lieux de vie et de travail que sont les bâtiments en améliorant également le confort d'été. Cette demande fait alors peser une contrainte

encore plus forte sur les bâtiments : développer les usages énergétiques du refroidissement et de la ventilation avec le minimum de consommation énergétique. Quand bien même ces nouveaux usages devraient être réservés aux bâtiments jugés prioritaires tels les hôpitaux, les bâtiments de santé ou encore les écoles, il n'en demeure pas moins qu'ils placent encore une fois les BACS dans un rôle central pour assurer une gestion optimale de ces usages énergétiques.

Dans ce contexte, les inspections réglementaires des BACS constituent un outil puissant pour le déploiement harmonieux des solutions les plus pertinentes selon le bâti et les investissements disponibles, et qui puissent être efficaces tout au long du cycle de vie du bâtiment. Obligatoire 2 ans après l'installation d'un nouveau BACS puis tous les 5 ans, l'inspection des BACS ne doit pas être une énième étape administrative avec pour seul but d'obtenir un tampon de validation réglementaire, mais bien un outil au service de l'ensemble la filière pour tirer le maximum de bénéfices des BACS et permettre leur évolution et adaptation aux nouvelles contraintes des bâtiments. Ainsi, les organismes de contrôles, qui doivent anticiper une montée en puissance des demandes d'inspections dans les mois et années à venir selon le calendrier réglementaire, sont mobilisés avec la filière BACS pour déployer leur savoir-faire en s'appuyant sur les référentiels standards en vigueur. En effet, il est essentiel d'avoir une compréhension commune des BACS et de leur fonctionnement depuis leur conception par les fabricants, jusqu'à leur exploitation en passant par l'étape cruciale de leur mise en œuvre.

C'est dans cette optique que l'ALLIANCE BACS poursuit ces travaux d'accompagnement de la filière, notamment en développant un module de formation permettant de mieux comprendre et appliquer les référentiels de marché, comme la norme NF EN ISO 52120-1, tout au long du cycle de vie du bâtiment. L'objectif visé est d'avoir une compréhension commune des tenants et aboutissants de l'efficacité des BACS par toute la filière et quelle que soit l'approche métier.

On le sait, la performance des BACS varie

fortement entre la phase de conception qui repose principalement sur une approche fonctionnelle (ex : régulation modulante par pièce du chauffage) et la précision des dispositifs de régulation, et les phases de mises en œuvre et d'exploitation des BACS dont le paramétrage doit permettre d'obtenir la performance demandée. Ainsi, de nombreuses installations BACS sont mal conçues, mal installées ou mal exploitées.

La caractéristique fondamentale des produits et systèmes BACS est qu'ils ont une performance in-situ. Cette dernière désigne la capacité réelle du système à piloter les équipements selon les besoins réels (occupation, météo, apports internes), produire des données fiables et exploitables, détecter les dérives et les corriger, ou encore maintenir les économies d'énergie promises. Il s'agit donc d'une performance d'usage, mesurable uniquement en exploitation réelle, avec des données de consommation, via un suivi continu, et en tenant compte des conditions d'occupation réelle et de fonctionnement. Elle dépend largement de la qualité des données (capteurs, compteurs), de la supervision, de la maintenance, de la capacité du système à détecter et corriger les dérives, et de la compétence des exploitants. **Or la performance réellement obtenue dans le bâtiment est la seule qui compte pour remplir les objectifs réglementaires du Décret Tertiaire, et surtout pour le confort des occupants.** A l'avenir donc, il deviendra de plus en plus important de déployer des outils de mesure de la performance énergétique réelle. On passera alors de l'évaluation d'une performance selon des conventions de calculs, à une performance réelle mesurée.

Enfin, un autre élément décisif vient désormais structurer la demande de BACS performants : la cybersécurité ! Cette exigence ne pèse pas seulement sur les propriétaires des bâtiments assujettis aux futurs textes réglementaires français qui doivent transposer la Directive NIS 2, mais s'impose à une part significative du parc de superviseurs et d'automates déployés aujourd'hui et qui ne respectent pas les bonnes pratiques de cybersécurité (ex : chiffrement, reconnaissance par échange de certificats, etc.). Les industriels BACS ont largement anticipé ce besoin en développant BACnet/SC dont il est

largement question dans ce numéro du Journal BACnet France. Mais si les offres sont aujourd'hui existantes et disponibles sur étagère, leur déploiement constitue là aussi un défi majeur pour les organisations qui doivent également anticiper et se structurer pour assurer la migration vers BACnet SC de manière pragmatique et efficace pour en réduire les coûts. Notre président de l'Association BACnet France, Monsieur Dan NAPAR, revient largement et en détail dans ce numéro du Journal BACnet France sur l'ensemble des enjeux, solutions techniques et recommandations à suivre pour assurer la convergence IT/OT indispensable pour maîtriser les investissements.

Vous le savez, les défis posés par l'objectif de déploiement massif de BACS performants pérennes, réglementaires et cyber-sécurisés sont nombreux. Nous remercions donc chaleureusement l'ensemble des parties prenantes de l'Association BACnet France et leurs partenaires que sont notamment le Syndicat ACR et l'ALLIANCE BACS et nous invitons toutes celles et ceux qui le veulent à nous rejoindre.

L'année 2027 marquera d'ailleurs la 20ème année d'existence de l'Association BACnet France. Nous vous y attendons nombreux dès à présent pour couronner son succès.



Florent Trochu

Délégué Général Association BACnet France | Syndicat ACR, ALLIANCE BACS
florent.trochu@acr-regulation.com

Performance énergétique et cybersécurité : Comment concilier les deux enjeux majeurs du bâtiment moderne ?

Le bâtiment tertiaire doit se décarboner et s'ouvrir au pilotage intelligent sans exposer ses infrastructures. Décret BACS, IA, BACnet/SC, certification IEC 62443 : la supervision s'affirme comme la pierre angulaire d'une GTB performante et résiliente.

À l'heure de la transition écologique et numérique, le secteur du bâtiment tertiaire fait face à un double défi : réduire drastiquement son empreinte carbone tout en protégeant ses infrastructures contre des cybermenaces de plus en plus sophistiquées. Entre obligations réglementaires, intégration de l'intelligence artificielle et sécurisation des réseaux de terrain, la supervision est au cœur des enjeux des bâtiments modernes.

L'urgence de la performance énergétique : réglementation et IA

Sous l'impulsion du décret BACS (Building Automation & Control Systems) et de la norme ISO 52120-1, les édifices tertiaires (neufs comme en rénovation) ont désormais l'obligation de s'équiper de systèmes d'automatisation et de contrôle avancés. L'objectif principal est clair : optimiser le fonctionnement des équipements de Chauffage, Ventilation et Climatisation (CVC) pour atteindre les objectifs de réduction d'énergie fixés pour 2030.

Cependant, les données actuelles montrent qu'un retard important reste à combler pour respecter ces échéances. Pour accélérer cette transition, l'apport de l'Intelligence Artificielle (IA) s'avère déterminant. Grâce à la régulation dynamique et à la maintenance prédictive, l'IA permet d'anticiper les besoins énergétiques en fonction de l'occupation ou de la météo, offrant des gains d'efficacité significatifs à très court terme.

De même, le bâtiment ne doit plus être un simple consommateur passif, mais un acteur actif du réseau électrique. Il est évident qu'il devient difficile de garantir l'équilibre uniquement en augmentant la production électrique à tout moment. L'usage et l'exploitation doivent s'adapter en temps réel à la disponibilité de la ressource. La flexibilité énergétique du bâtiment n'est pas une contrainte, mais bien une opportunité d'optimisation économique et environnementale.

Le revers de la connectivité : une surface d'attaque élargie

Pour participer aux mécanismes de flexibilité énergétique et permettre un pilotage optimal, les bâtiments modernes doivent être connectés. Mais cette ouverture indispensable présente un risque majeur : elle élargit la surface d'attaque exposée aux cyberattaques.

La vulnérabilité ne provient pas uniquement des accès distants ou Internet (connectivité externe) : elle résulte aussi d'infiltrations via les accès distants de télémaintenance ou les API de services tiers, ainsi que d'interventions physiques ou logicielles non sécurisées par divers prestataires sur les équipements de terrain.

Pour garantir l'intégrité du bâtiment, il est donc crucial de sécuriser l'ensemble de la chaîne de communication, du réseau IT central jusqu'aux équipements de terrain les plus élémentaires.

Cela inclut d'une part l'architecture et la segmentation réseau IT et de terrain et d'autre part le durcissement de la mise en place des systèmes.

BACnet/SC : la réponse technologique aux exigences de sécurité du terrain

C'est dans ce contexte que le protocole BACnet Secure Connect (BACnet/SC) s'impose comme une évolution majeure pour les réseaux de terrain IP. Il apporte une réponse concrète aux contraintes de sécurité et de déploiement : l'ensemble des données transmises est chiffré et chaque équipement est authentifié par certificat numérique. Son intégration en IP est simplifiée, limitant ainsi la complexité des règles de pare-feu nécessaires, notamment grâce à l'utilisation de connexions TLS sortantes vers le Hub.



L'architecture s'appuie sur un concentrateur (Hub Primaire) qui centralise les connexions sécurisées et achemine les messages entre les différents appareils. Ce concentrateur peut être redondé (Hub Secondaire) pour garantir une haute disponibilité des échanges.

L'intégration de ce protocole sécurisé au sein de la supervision PcVue constitue un gage de fiabilité supplémentaire. La fourniture BACnet/SC bénéficiera de la certification BTL (BACnet Testing Laboratories) correspondante.

PcVue : Une supervision certifiée au cœur du bâtiment durable et sécurisé

La plate-forme de supervision PcVue répond à la fois aux enjeux de performances énergétiques grâce à son ouverture vers l'ensemble des systèmes de production et de consommations et l'intégration de l'IA et aux enjeux de cybersécurité avec l'intégration et le déploiement de protocoles et d'architectures sécurisés. Au-delà des seules recommandations et bonnes pratiques de mise en œuvre de nos solutions, la double certification IEC 62443-4-1 et 4-2, valide à la fois le processus de développement sécurisé et la cybersécurité des composants de PcVue.

En plaçant la supervision au carrefour de la performance énergétique et de la cybersécurité, PcVue permet aux bâtiments tertiaires de répondre sereinement aux exigences environnementales sans jamais compromettre la sécurité de leurs infrastructures numériques.

PLUS DE SÉCURITÉ. PLUS DE PERFORMANCE.

L'UBR-03 pour les grands réseaux BACnet/SC.



Cryptage, certificats et mécanismes de failover exigent une infrastructure robuste. Le UBR-03 répond à ces besoins grâce à une CPU plus puissante et à davantage de mémoire.

- Certifié BACnet.
- Deux interfaces IP.
- Made in Germany.
- Des réserves supplémentaires pour BACnet/SC.

ET LES CERTIFICATS ?
LEUR GESTION PEUT ÊTRE AUTOMATISÉE.

Contactez-nous.



François Fleche

Head of Global Marketing
PcVue – ARC Informatique

f.fleche@arcinfo.com | www.pcvue.com



Données BACnet et IA : Détecter l'anormal avant l'incident



Détection d'anomalies :
un cas d'usage de l'IA
appliqué aux données
BACnet

Les réseaux BACnet exposent de nombreux points de mesure et d'état. Mais qui repère les dérives avant qu'elles ne deviennent surconsommations, inconfort ou panne ? L'IA apporte ici une capacité d'analyse complémentaire.

Les données BACnet : une base d'analyse pour la GTB

Dans une installation GTB, BACnet permet de faire dialoguer automates, capteurs, équipements CVC, compteurs et systèmes de supervision. Températures, consignes, états de fonctionnement, débits, pressions, puissances ou alarmes techniques décrivent en continu le comportement réel du bâtiment.

Mais le volume de données rend leur exploitation difficile. Suivre chaque courbe, interpréter chaque évolution et coder toutes les situations possibles dans des règles devient vite complexe. Certaines anomalies restent donc peu visibles : débit d'air trop élevé la nuit, vanne ouverte sans effet mesurable, température qui dérive malgré une consigne stable, groupe froid dont le rendement baisse, capteur incohérent avec les autres valeurs d'une zone.

Ces signaux faibles ne déclenchent pas toujours d'alarme classique. Ils peuvent pourtant annoncer une surconsommation, une perte de confort ou une dégradation d'équipement.

Les limites des seuils classiques

Les alarmes sur seuils restent nécessaires. Elles détectent des défauts francs : température trop haute, équipement à l'arrêt, défaut de communication, pression insuffisante. En revanche, elles sont moins adaptées lorsque l'anomalie dépend du contexte.

Sur une installation CVC, une valeur « normale » varie selon l'occupation, la météo, l'heure, le jour de la semaine ou la phase de fonctionnement. Un débit peut être cohérent en journée et anormal la nuit. Une consommation peut être acceptable à pleine charge, mais excessive à charge partielle.

Dans ces cas, l'anomalie ne dépasse pas forcément un seuil fixe. Elle se manifeste plutôt par une dégradation progressive : même débit pour plus d'énergie, temps de chauffe plus long, refroidissement moins efficace, cycles plus fréquents, simultané chaud/froid.

DAA : appliquer l'IA aux historiques BACnet

DAA, pour Détection Automatique d'Anomalies, est une nouvelle fonctionnalité de la plate-forme Panorama Suite destinée à automatiser cette surveillance. Son principe consiste à apprendre une situation normale à partir des historiques de données BACnet, puis à détecter les comportements qui s'en écartent.

L'objectif n'est pas de remplacer les alarmes existantes, mais de les compléter. Les seuils détectent des situations connues et définies à l'avance. DAA cherche à identifier des comportements inhabituels, y compris lorsqu'aucune règle métier n'a été explicitement codée.

L'analyse peut porter sur une donnée BACnet isolée, un équipement, une zone ou un ensemble de points liés entre eux. Elle tient compte des phases de fonctionnement : jour/nuit, semaine/week-end, occupation/inoccupation, montée en charge, arrêt ou fonctionnement nominal. Cette distinction permet de comparer des situations comparables.

Lorsqu'un comportement s'écarte de ce qui est

attendu, une alerte peut être générée en temps réel afin d'attirer l'attention de l'exploitant.

Exemples d'usage en GTB

Sur des installations CVC supervisées via BACnet, la détection automatique d'anomalies peut contribuer à repérer plusieurs types de dérives.

■ Confort et qualité d'air

À l'échelle d'un étage, d'une pièce ou d'une zone, les données de température, humidité, température extérieure ou présence peuvent être analysées ensemble pour détecter un inconfort persistant ou une réponse insuffisante de la ventilation.

■ Ventilation et CTA/VAV

Les données de débits, états, consignes, températures de soufflage ou modes de

marque peuvent aider à identifier des débits trop élevés la nuit ou le week-end, ou des périodes où chaud et froid fonctionnent simultanément.

■ Énergie et performance CVC

Les données BACnet issues de groupes froids, pompes à chaleur, chaudières ou compteurs peuvent révéler des surconsommations, une perte de performance, un COP qui baisse, des cycles courts ou des équipements actifs hors horaires.

■ Maintenance et signaux faibles

Une dérive de ΔP filtre, une baisse de débit à vitesse identique, un compresseur dont la consommation électrique dérive ou une vanne ouverte avec faible variation de température peuvent orienter une intervention préventive.

■ De la donnée BACnet à l'information exploitable

BACnet structure l'échange d'informations entre équipements et supervision. Mais la valeur opérationnelle apparaît lorsque ces informations sont historisées, comparées et interprétées dans leur contexte. L'IA appliquée à ces historiques ne fournit pas automatiquement un diagnostic complet. Elle permet surtout de prioriser l'attention sur des situations qui méritent une analyse.

Avec DAA, les données BACnet peuvent ainsi contribuer à une supervision davantage orientée prévention : mieux qualifier les écarts, détecter plus tôt les dérives et aider les équipes à intervenir avant que l'anomalie ne devienne un incident.



Charles Tabath

Responsable Marketing Produit | CODRA
c.tabath@codra.fr | codra.net

CODRA

DAN NAPAR CONSULTING

Expertise BACS, BACnet & BACnet/SC — Cybersécurité et conformité réglementaire des bâtiments connectés

Sécuriser et interconnecter la gestion technique de vos bâtiments

DAN NAPAR CONSULTING accompagne la maîtrise d'ouvrage et d'œuvre, installateurs et intégrateurs système, exploitants dans la conception, commissionnement et exploitation des installations de GTB pour atteindre leurs conformités réglementaires et de cybersécurité.

■ Audit & diagnostic de vos infrastructures GTB (OT)

■ Soutien aux responsables de projets sur les spécifications techniques propre au projet

■ Conseil & accompagnement pour la conception et rédaction de vos spécifications techniques

■ Formation et sensibilisation des équipes opérationnelles à la construction de la cybersécurité

JDN

« **DAN NAPAR CONSULTING** accompagne les entreprises dans leurs décisions stratégiques en apportant un diagnostic clair, une méthodologie éprouvée et des solutions immédiatement applicables. »

Un projet neuf, de rénovation ou de mise en conformité BACS / BACnet/SC ? Parlons-en.

Une GTB « cybersécurisée » pour un opérateur d'importance vitale



Projet : Une Gtb « cybersécurisée » pour un operateur d'importance vitale

Après 18 mois de travaux, l'intégrateur ALVA SYSTEMS a réceptionné une installation GTB complètement sécurisée en s'appuyant sur les protocoles de communication standardisés et sécurisés BACnet Secure Connect (BACnet/SC) et KNX Secure.

Le système de Gestion Technique du Bâtiment gère l'ensemble des installations de chauffage, ventilation et climatisation d'un site classé OIV (Opérateur d'Importance Vitale) au travers de la gamme de contrôleurs Desigo PXC de Siemens certifiés BTL. L'intégrateur a été force de proposition pour suggérer la mise en place de protocoles chiffrés afin de sécuriser ce site hautement sensible.

Le protocole BACnet/SC comme élément de réponse aux enjeux de cybersécurité

La GTB traditionnelle, celle que l'on installe dans 99 % des bâtiments tertiaires ou industriels aujourd'hui, est une passoire en termes de cybersécurité.

Jusqu'à présent, les protocoles historiques BACnet IP ou KNX avaient été conçus pour l'in-

teropérabilité et non pour la sécurité.

Les protocoles BACnet/SC et KNX Secure conservent le côté standardisé et ouvert mais offrent désormais une extension de sécurité.

Selon Thomas HEDOUX, sécuriser ne veut pas dire se fermer : « L'intérêt de BACnet/SC, c'est d'ajouter une couche de sécurité sans renoncer au standard : l'installation reste ouverte et multi-constructeurs. On ne troque pas la cybersécurité contre l'interopérabilité, on garde les deux. »

Selon Thomas HEDOUX, la maîtrise des concepts de cybersécurité devient cruciale.

Par concepts, le directeur technique d'ALVA SYSTEMS entend la connaissance des principes de la cryptographie (comprendre les bases des certificats numériques, des clés publiques/privées, du chiffrement (TLS) et de l'authentification) ; la gestion des certificats (savoir générer, déployer, gérer et révoquer des certificats incluant la compréhension des autorités de certification et de leur rôle), la sécurité réseau (connaissance des pare-feu, des VPN, des listes de contrôle d'accès et des bonnes pratiques de

segmentation réseau) et enfin la gestion des identités et des accès (comprendre comment les utilisateurs et les appareils sont authentifiés et autorisés à accéder aux ressources).

Selon Thomas HEDOUX, le protocole n'est pas une baguette magique : « BACnet/SC sécurise les échanges, mais il s'inscrit dans une défense en profondeur : segmentation réseau, pare-feu, gestion des accès. Chiffrer les communications est nécessaire, ce n'est pas suffisant à soi seul. »

Un métier de l'intégrateur en profonde mutation

Réaliser ce projet pour notre client nous a confirmé une chose : le métier d'intégrateur GTB a muté. On ne peut plus se contenter de savoir câbler une sonde ou de régler une loi d'eau.

L'intégration du protocole BACnet/SC dans un projet GTB combine le monde de l'automatisation du bâtiment (BACnet) et celui de la cybersécurité (IT).

Au sein d'une même équipe il devient primordial de disposer d'ingénieurs et de techniciens



ter les règles de cybersécurité minimales imposées par la directive NIS2 et par les référentiels de l'ANSSI.

Yann PLEVIN, notre responsable Normalisation et Réglementation chez Siemens, met en lumière une réalité cruciale pour l'avenir de nos infrastructures : l'impératif de proposer des solutions de Gestion Technique du Bâtiment (GTB) robustes, ouvertes et interopérables. Cette approche est la pierre angulaire pour garantir la pérennité et l'évolutivité de chaque installation. Dans un monde où la convergence entre la Technologie Opérationnelle (OT) et la Technologie de l'Information (IT) est de plus en plus prononcée, les standards de l'industrie des BACS (Building Automation and Control Systems) comme BACnet/SC (Secure Connect) évoluent constamment. Ils s'adaptent sans relâche pour intégrer les exigences minimales en matière de cybersécurité, assurant ainsi que nos systèmes restent à la pointe de la technologie tout en étant protégés contre les menaces émergentes. C'est une démarche essentielle pour bâtir des environnements intelligents, sécurisés et durables !

avec la double compétence, où les individus sont capables de jongler entre ces différents domaines rendus dorénavant indissociables.

Selon Thomas HEDOUX, le vrai changement se joue après la mise en service : « Sur une GTB classique, une fois le site livré, il tourne. Avec BACnet/SC, on hérite d'une infrastructure à clés

qu'il faut exploiter dans la durée : les certificats expirent, doivent pouvoir être renouvelés et révoqués. Livrer une installation sécurisée, c'est aussi livrer un plan de gestion des certificats sur toute sa durée de vie. »

Selon Thomas HEDOUX, les intégrateurs doivent se préparer rapidement à connaître et respec-



Thomas Hedoux

Directeur Technique | Alva Systems
thomas@alva-systems.fr | www.alva-systems.fr

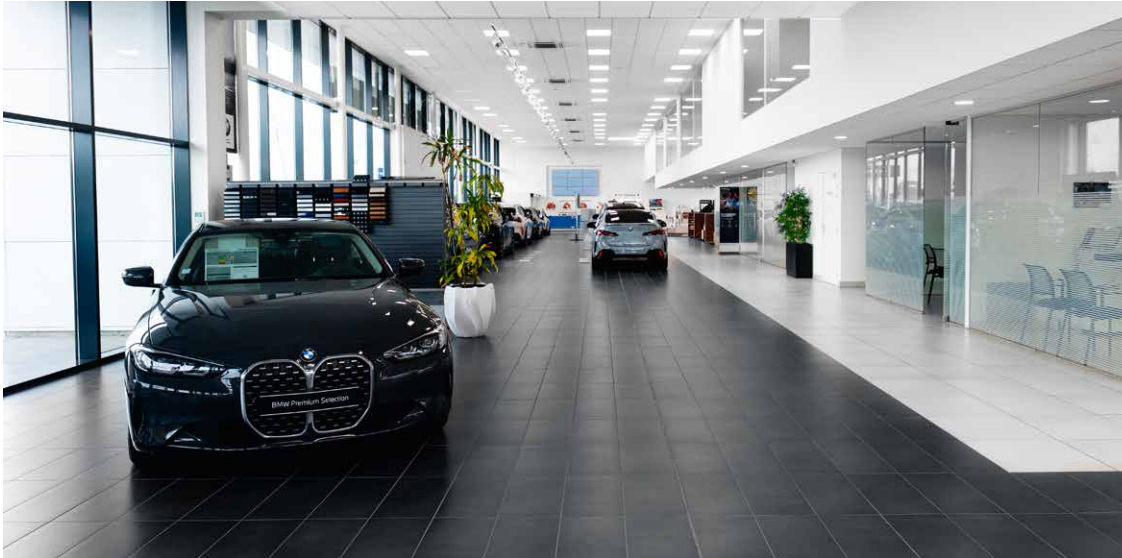


Yann Plevin

Responsable Normalisation et Réglementation Siemens | Smart Infrastructure
yann.plevin@siemens.com | www.siemens.fr/smart-infrastructure



L'humain, facteur clé de succès pour l'intégration d'une GTB



Exemple de locaux de déploiement de la GTB

Déployer une GTB ne s'improvise pas. Si le cadre réglementaire pousse les gestionnaires de patrimoine tertiaire à s'équiper, la réussite d'un tel projet tient autant à la technique qu'à la démarche : les facteurs humains et organisationnels sont aussi déterminants que la solution elle-même. Pour franchir le pas, les Certificats d'Économies d'Énergie (CEE) sont aujourd'hui une aide indispensable à mobiliser à condition d'être bien entouré pour en tirer le meilleur parti. Retour sur un déploiement à grande échelle avec le groupe automobile Lempereur et L&Smart pour comprendre ce qui fait vraiment la différence.

Décret tertiaire et décret BACS : le cadre réglementaire qui structure le marché de la GTB

Le Décret Tertiaire fixe aux bâtiments de plus de 1 000 m² des objectifs progressifs de réduction des consommations énergétiques, avec un premier palier de -40 % à l'horizon 2030. De son côté, le Décret BACS impose l'installation de systèmes d'automatisation et de contrôle des bâtiments capables de suivre, analyser et piloter les principaux équipements techniques afin d'améliorer leur efficacité énergétique. Enfin, les CEE viennent apporter une prime pour la mise en œuvre d'une GTB de classe A ou B. L'ensemble des critères sont remplis pour une massification.

Cependant, le marché reste encore sous-équipé : selon le GIMELEC, seulement 16 % des sites

concernés étaient équipés en 2025. Mais si la réglementation pousse à l'action, la réussite d'un projet repose avant tout sur la méthode de déploiement.

Les facteurs clés de succès d'une démarche GTB : l'humain au cœur de la démarche

La société éditrice et intégratrice de logiciels de gestion technique du bâtiment (GTB) L&Smart accompagne depuis 2 ans la transition énergétique des concessions automobiles du groupe Lempereur basé dans les Hauts-de-France. Pour le CEO Louis Vanetti, plus qu'un outil, L&Smart est une démarche. La GTB ne crée pas de valeur seule : ce sont les usages, les équipes et l'accompagnement qui transforment un équipement réglementaire en véritable levier de performance.

Choisir une solution adaptée à son patrimoine

La première étape consiste à choisir une solution compatible avec la réalité de son parc immobilier. Dans le cas de plusieurs concessions à gérer, le groupe Lempereur a opté pour une approche standardisée et facilement déployable. L'utilisation de la technologie sans fil « LoRa » et de la plateforme cloud centralisée L&Smart permet de superviser l'ensemble des bâtiments depuis une interface unique. Installée intelligemment, la GTB constitue ainsi une aide à la décision dans les investissements des clients de L&Smart.

Prioriser les équipements les plus énergivores

Tous les usages ne présentent pas le même potentiel d'économies d'énergie : les systèmes CVC représentent généralement près de 60% des consommations d'un bâtiment tertiaire.

La démarche consiste ainsi à cibler en priorité ces équipements avant d'intégrer progressivement les spécificités propres à chaque activité. Dans le secteur automobile, par exemple, le pilotage coordonné des portes de garage et du chauffage qui s'éteint lorsque celles-ci sont ouvertes constitue un levier d'optimisation essentiel pour L&Smart.

Faire des utilisateurs de véritables acteurs de la GTB

Une GTB ne peut pas être perçue comme un simple outil de contrôle imposé aux occupants d'un bâtiment. Forte de son expérience terrain, L&Smart a fait de l'accompagnement des utilisateurs un élément central de sa démarche. L'objectif est de faire comprendre les enjeux de la GTB et de transformer les collaborateurs en acteurs de la performance énergétique.

Cette conviction a conduit L&Smart à développer une démarche d'accompagnement qui va bien au-delà de l'installation technique. À travers son programme « L&Smart School », l'entreprise accompagne les collaborateurs dans l'appropriation des outils, la compréhension des enjeux énergétiques et l'évolution durable des usages.

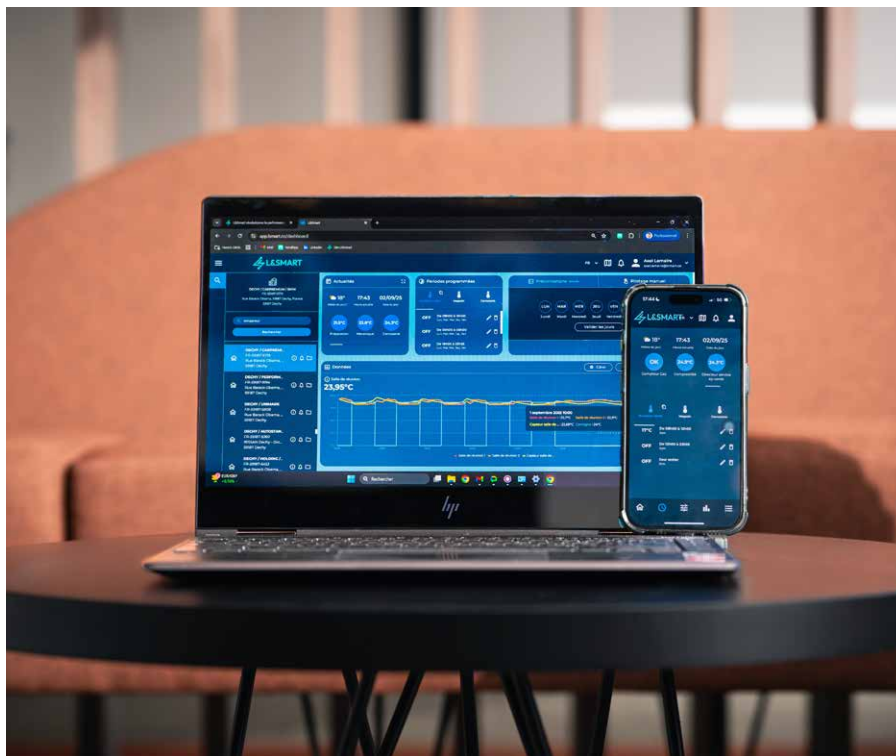


Illustration de la plateforme et de l'application L&SMART

Et l'approche L&Smart fonctionne : un an après l'installation de la GTB, le groupe Lempereur est prêt à investir de nouveau pour aller plus loin.

Convaincu par l'efficacité de l'approche, Louis Vanetti a lancé début 2026 le « L&Smart Partners », un réseau de partenaires à l'échelle nationale pour déployer sa solution et sa méthode d'accompagnement dans toute la France. Par ailleurs, L&Smart a officiellement lancé les premiers Trophées de la Décarbonation Automobile lors d'un événement organisé à Valenciennes (59), réunissant concessionnaires, groupes automobiles et experts de la transition énergétique. Cette initiative nationale vise à valoriser les concessions les plus engagées dans la réduction de leur consommation d'énergie et la décarbonation du secteur.

Car même les systèmes GTB les plus performants ne peuvent délivrer leur plein potentiel sans l'adhésion des équipes qui occupent les bâtiments au quotidien.

Communication interne, sensibilisation aux consommations ou encore challenges entre concessions permettent ainsi de créer une dynamique collective autour des économies d'énergie. L'objectif n'est pas seulement de réduire les consommations mais d'installer durablement une culture de la performance énergétique au sein de l'entreprise.

Les CEE comme accélérateur financier à condition d'être bien accompagné

Même si les CEE ne constituent pas forcément le déclencheur principal d'un projet, ils permettent souvent de lever les freins financiers liés à l'investissement.

« La gestion des CEE était souvent un casse-tête pour nous : lenteurs, contrôles COFRAC négatifs, manque d'accompagnement... travailler avec SOBREN est une bouffée d'air frais. Expertise, réactivité et vrai contact humain : tout se passe sans le moindre accroc. » témoigne Louis Vanetti.

L'expérience menée par le groupe Lempereur en témoigne : accompagné par L&Smart & SOBREN depuis 2 ans, le groupe a pu bénéficier de **plus d'un million d'euros de prime CEE** pour équi-

per une cinquantaine de concessions. Après une seule période de chauffe, les économies observées sur le chauffage atteignent environ 25%.

La réussite d'un projet GTB repose donc sur un équilibre entre technologie, accompagnement financier et engagement humain car derrière chaque bâtiment intelligent, ce sont avant tout des équipes impliquées qui font la différence.



Léopold Fossé

Cofondateur | SOBREN

l.fosse@sobren.fr | sobren.fr

SOBREN



Louis Vanetti

CEO | L&Smart

louis@lsmart.co | www.lsmart.co

L&SMART



Axel Lemaire

Responsable Commercial | L&Smart

axel.lemaire@lsmart.co | www.lsmart.co

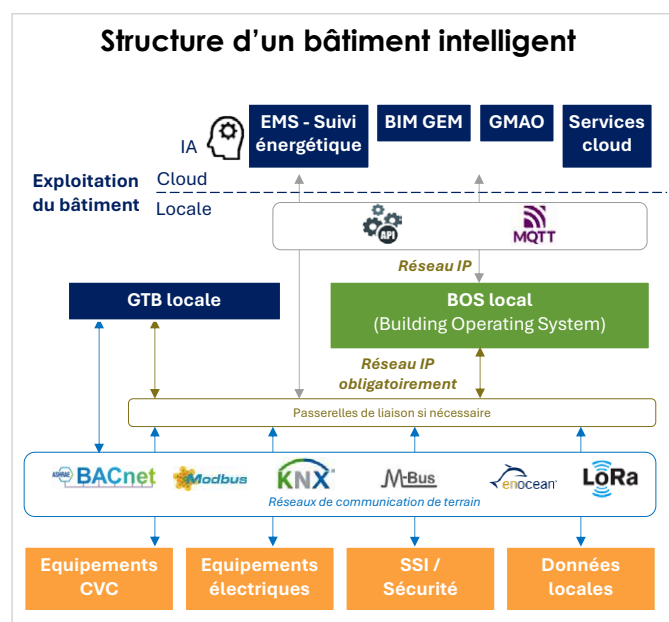
L&SMART

Initiation des futurs techniciens à la sécurisation des communications numériques

Le lycée Hippolyte Fontaine de Dijon forme des techniciens en bâtiments communicants (BTS Fluides Energies Domotique option Domotique et Bâtiments Communicants) dans le but d'être des spécialistes des automatismes et des réseaux de communication du bâtiment.

A ce titre, ils doivent maîtriser le fonctionnement des équipements techniques des bâtiments (CVC, CFO, CFA) afin de savoir concevoir, installer, paramétrer/programmer et mettre en service leurs solutions de pilotage. Les objectifs sont de concilier performance énergétique, confort et sécurité du bâtiment ainsi que de ses usagers.

Cela implique aussi l'exploitation de communications numériques afin d'échanger les informations entre les différents systèmes et services. Au-delà de la maîtrise fondamentale de leurs mises en œuvre, il est important d'initier les étudiants aux problématiques de cybermalveillance qui peuvent les toucher.



Communications exploitées dans les bâtiments communicants et connectés

Démarche générale de cybersécurité des bâtiments communicants et connectés

Les étudiants sont sensibilisés aux actions de base pour sécuriser les communications numériques :

- Limitation des accès physiques aux médias de communication filaires internes au bâtiment.
- Segmentation logique ou physique des réseaux IP du bâtiment.
- Utilisation si possible des communications IP en https, en VPN...
- Changement des mots de passe par défaut dès la mise en service des équipements communicants par des mots de passe forts.

- Attribution de profils d'accès aux équipements adaptés à chaque utilisateur.
- Création d'utilisateurs nominatifs pour le suivi des accès,
- Activation de l'expiration des sessions en cas d'inactivité.
- Mises à jour de firmware des composants et des logiciels pour combler les failles et apporter de nouvelles fonctionnalités de sécurité.

Les équipements techniques pédagogiques du lycée Hippolyte Fontaine de Dijon sont intégrés dans un VLAN spécifique (Virtual Local Area Network) avec une gestion fine du pare-feu.

Sécurité dans l'interopérabilité des échanges et la connectivité des solutions

Les communications entre les différents systèmes du bâtiment, avec le système de GTB, avec le Building Operating System (BOS) ou avec les plateformes hébergées dans le cloud doivent se faire sans fragiliser la sécurité des systèmes d'information numériques.

Dans le cadre du programme de la Distech Académie, des échanges techniques ont été initiés entre la société Distech Controls et le lycée Hippolyte Fontaine. Ils ont permis de former les étudiants à l'utilisation des protocoles de communication sécurisés.

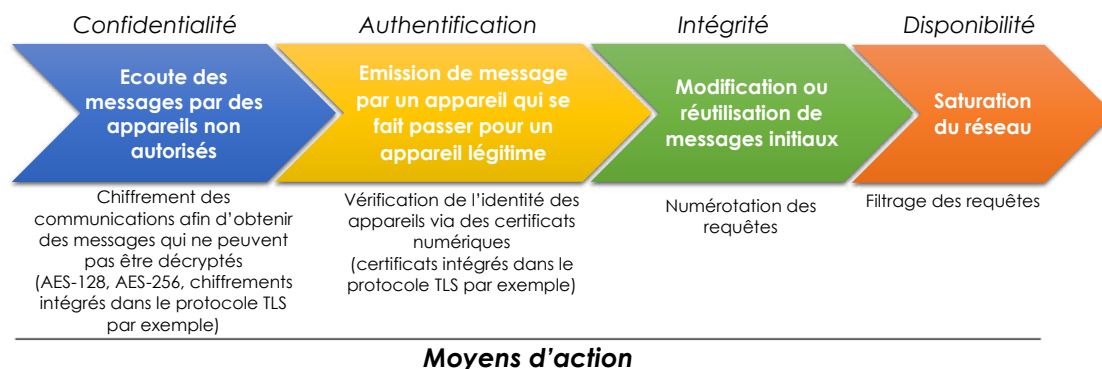


Formation d'enseignants dans les locaux de la société Distech Controls

Les protocoles de communication numériques internes au bâtiment doivent, si possible, être ouverts, standardisés et non propriétaires afin que les équipements communiquent entre eux : BACnet, Modbus, KNX, DALI, LoRa, EnOcean... Les versions évoluées de certains de ces protocoles permettent d'atteindre un niveau de sécurité supérieur.

Les protocoles API REST (Application Programming Interface) et MQTT (Message Queuing Telemetry Transport) permettent également une interopérabilité des systèmes, notamment via le cloud, et doivent aussi être sécurisés.

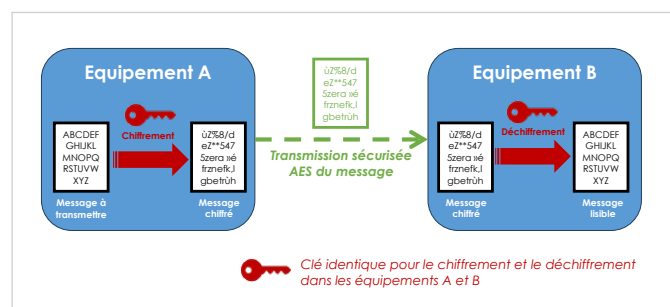
Enjeux principaux des communications sécurisées



Chiffrement des messages en AES

AES (Advanced Encryption Standard) est un algorithme de chiffrement utilisant la même clé pour chiffrer et déchiffrer les données. On parle de clés symétriques.

Le message à transmettre est découpé par blocs de 128 bits et subit des opérations mathématiques complexes de modification pour brouiller au maximum les informations d'origine et pour empêcher tout décryptage sans la clé. La taille de la clé de chiffrement/déchiffrement peut mesurer 128 bits (AES-128) ou 256 bits pour encore plus de sécurité (AES-256).



Principe de la communication chiffrée AES

Cependant, cette clé doit rester secrète... Or, la clé doit être échangée à un moment donné et cet échange peut être intercepté, rendant le chiffrement inutile... De plus, la clé est définie par l'un des participants et n'est pas forcément renouvelée automatiquement, ce qui la rend plus vulnérable aux attaques.

Cette méthode de chiffrement est notamment utilisée pour les communications WiFi WPA2 et WPA3, KNX Secure, LoRa, TLS (après l'établissement de la connexion à l'aide d'un chiffrement asymétrique).

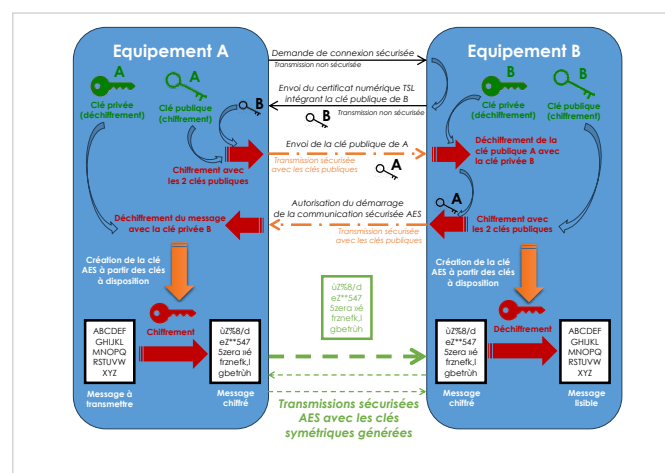
Chiffrement des messages en TLS

TLS (Transport Layer Security) est un protocole qui permet de sécuriser les communications sur un réseau en utilisant du chiffrement asymétrique pour aboutir à un chiffrement symétrique. Le protocole cryptographique TLS remplace le protocole SSL (Secure Socket Layer) qui est plus ancien et moins sécurisé mais qui fonctionne avec le même principe.

Le chiffrement asymétrique utilise deux clés générées dans chaque équipement communicant : une clé publique pour chiffrer des données et une clé privée pour déchiffrer des données (clé qui n'est jamais communiquée).

Ce chiffrement asymétrique est utilisé au début de la communication pour établir ensuite une communication sécurisée avec clé symétrique AES qui est plus rapide et moins gourmande en ressource.

Les clés sont générées dynamiquement pour chaque session de communication.

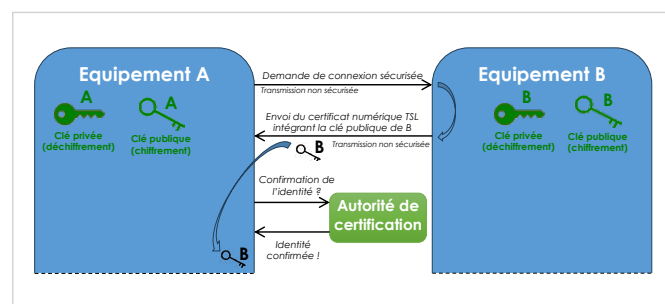


Principe de demande de communication sécurisée TLS de l'équipement A (client) à l'équipement B (serveur)

Ce protocole est notamment exploité pour les échanges client/serveur d'un réseau IP en HTTPS, MQTT avec TLS, Bacnet/SC...

Authentification des appareils communicants en TLS

Un certificat numérique TLS/SSL est un document électronique qui associe une identité (nom de domaine, adresse IP, identifiant d'équipement) à la clé publique utilisée pour le chiffrement asymétrique avec une durée de validité limitée.



Vérification de l'identité de l'équipement B (serveur) par l'équipement A (client)

Lors d'une connexion sécurisée en TLS, le serveur envoie son certificat au client en réponse à une demande de connexion sécurisée. Ce certificat permet au client de vérifier l'identité du serveur et de récupérer la clé publique du serveur pour établir une communication chiffrée. Dans certains cas, il est possible que le serveur vérifie aussi l'identité du client avec le certificat de celui-ci.

Pour les communications avec le cloud, il est nécessaire d'utiliser des certificats de confiance qui sont signés numériquement par une autorité de certification (CA) pour en garantir l'authenticité et l'intégrité, protégeant ainsi contre l'usurpation d'identité.

Pour des communications internes au bâtiment, les certificats auto-signés sont une solution pratique qui ne nécessite pas de vérification auprès d'une autorité de certification. La confiance est maintenue par cet usage interne mais l'absence de validation externe peut générer des risques. La plupart des navigateurs web affichent des avertissements lorsqu'ils doivent échanger avec un certificat TLS/SSL auto-signé et ceux-ci peuvent inquiéter les utilisateurs. Les contrôleurs Distech Controls exploitent des certificats auto-signés.

Les protocoles HTTPS, API, VPN, MQTT et BACnet/SC utilisent des certificats TLS pour authentifier de manière fiable les équipements connectés au réseau et garantir que les échanges de données sont à la fois sécurisés et chiffrés.

Pour renforcer davantage la sécurité du réseau, il est possible d'ajouter le protocole 802.1X. Celui-ci permet de vérifier systématiquement l'identité de chaque appareil ou utilisateur avant même qu'il ne puisse accéder au réseau IP, que ce soit en connexion filaire ou en Wi-Fi. Cette vérification s'effectue via un serveur d'authentification (comme un serveur RADIUS), qui valide les informations d'identification avant d'autoriser l'accès.

Les contrôleurs Eclipses de Distech Controls sont compatibles avec le protocole 802.1X qui est recommandé pour les sites manipulant des données sensibles (secrets industriels, informations bancaires...).

Communications avec le cloud

MQTT est un protocole de messagerie publication-abonnement, courte,

simple et rapide. Le Broker (serveur central) reçoit les messages des émetteurs et les redistribue aux destinataires qui se sont abonnés. Ce protocole est idéal pour les capteurs sur batterie en raison du peu d'énergie à mobiliser.

La communication est sécurisée, car elle nécessite de connaître l'adresse du Broker, les identifiants pour s'y connecter ainsi que la description des topics (désignation des variables mises à disposition par les émetteurs). De plus, l'exploitation d'un certificat assure une communication chiffrée et authentifiée avec le Broker.

La mise en évidence de ces éléments de sécurité est réalisée par la mise en œuvre de la visualisation de la température d'un local du lycée sur un smartphone pour le suivi du confort d'ambiance de celle-ci. Dans cette activité pédagogique, l'information est d'abord transmise via le protocole EnOcean au contrôleur ECY-350, le programme graphique FBD de celui-ci la met à disposition via un point BACnet AV1 et son connecteur MQTT envoi au Broker MQTT la valeur de la température. L'application du smartphone est configurée pour s'abonner au Broker et reçoit au fur et à mesure les valeurs.

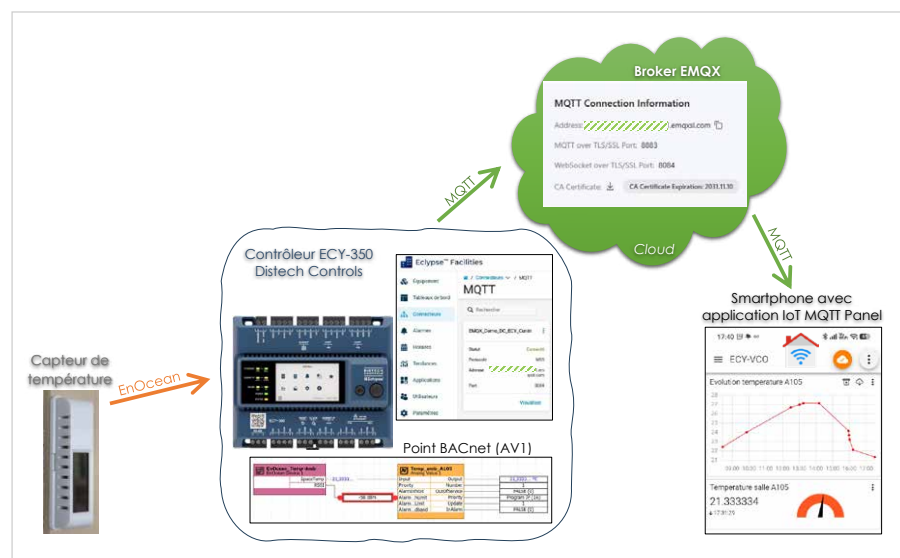
Il est à noter que la communication EnOcean constitue le point faible de la structure pédagogique étudiée puisqu'elle n'est pas sécurisée. Cependant, pour pouvoir analyser le contenu de la trame transmise, il faut connaître le profil EEP (EnOcean Equipment Profile) de l'équipement émetteur, ce qui nécessite un accès physique à celui-ci. Par ailleurs, la portée de la communication EnOcean est limitée (quelques dizaines de mètres).

API REST est une interface de programmation d'application (API) qui regroupe un ensemble de règles et de consignes pour la création d'API web.

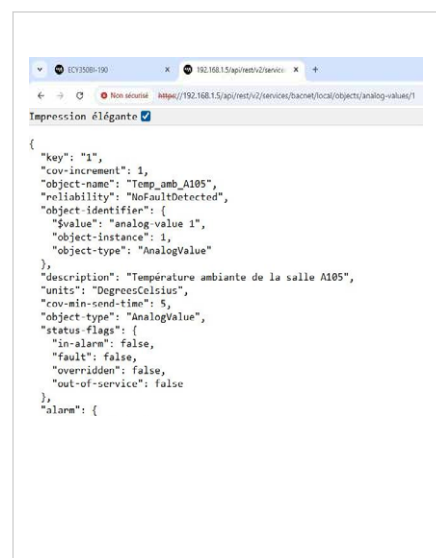
Ce protocole permet à un produit ou un service de communiquer avec d'autres produits et services sans connaître les détails de leur mise en œuvre et sans sacrifier le contrôle et la sécurité.

L'exploitation des données est plus complexe qu'avec le protocole MQTT, en raison du nombre d'informations transmises.

En revanche, la mise à disposition des informations du contrôleur ECY-350 est très facile à mettre en œuvre.



Activité pédagogique de la mesure de température d'un local du lycée et de récupération de la valeur sur un smartphone



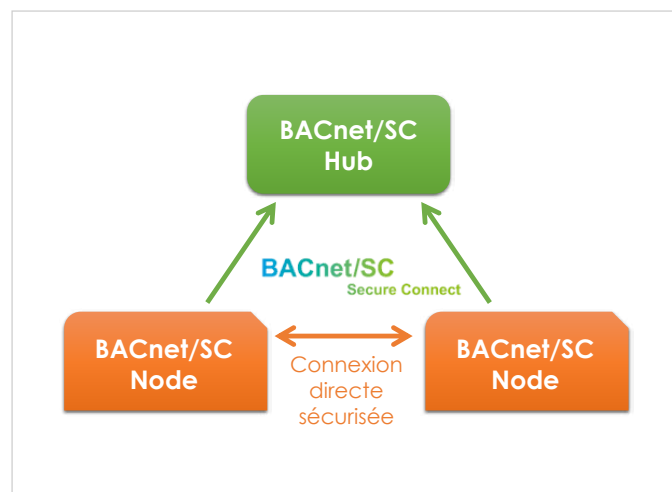
Exemple pédagogique de la mesure de température

L'activité pédagogique d'interrogation du contrôleur par une requête API avec un navigateur web permet d'étudier à nouveau les différentes propriétés mises à disposition par le point BACnet AV1 du programme FBD pour la mesure de température de la salle A105...

Communications internes au bâtiment

L'initiation à la communication BACnet/SC entre les contrôleurs Distech Controls se fait aisément en déclarant l'un d'eux en hub et les autres en nœud.

Le hub centralise la gestion des connexions, des certificats et des politiques de sécurité. Comme pour la communication MQTT, les certificats permettent de chiffrer la communication BACnet/SC et d'authentifier les équipements.

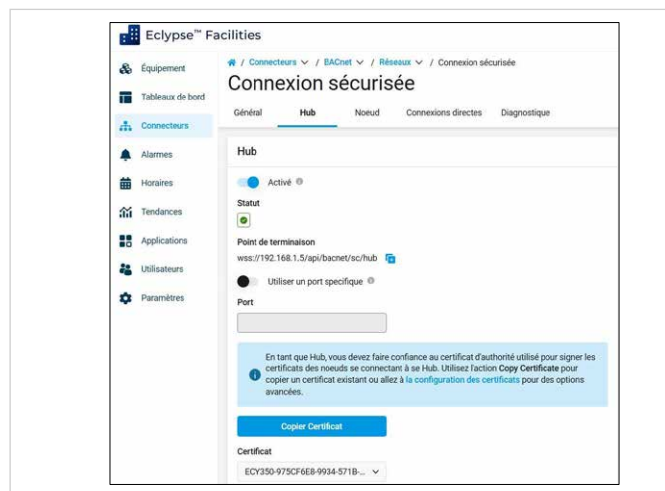


Principe de communication BACnet Secure Connect

Les mécanismes mis en place en KNX Secure sont appréhendés grâce à l'exploitation du logiciel ETS6 et du logiciel de simulation KNX Virtual. En effet, il est alors possible d'utiliser des participants virtuels certifiés KNX Secure pour le paramétrage d'une installation KNX virtuelle dont le fonctionnement est simulé.

Segment	ID	OrderNr	AES	Description	Prog/Version	Status	A	L	D	SN
S1	D25	BO tp	No	Binary Output	-	Unloaded	15	15	255	00FA-00252500
	D19*			Undefined: block/block						
S2	D19_	cIP	No	IP/TP Coupler	-	Unloaded	15	15	0	00FA-00251900
	D0	DA tp	-	Dimming Actuator	-	Unloaded	15	15	255	00FA-00250000
	D2	BS tp	-	Blinds/Shutter Actuator	-	Unloaded	15	15	255	00FA-00250200
	D4	KX tp		D1 Certificate (copied to clipboard) AD5AAJ-IBACVB-DKQRVI-IZUENK-CGVBDK-QRVIIY		Unloaded	15	15	255	00FA-00250400
	D7	SA tp				Unloaded	15	15	255	00FA-00250700
	D13	SC tp				Unloaded	15	15	255	00FA-00251300
	D14	LM tp				Unloaded	15	15	255	00FA-00251400
	D20	iIP				Loaded	1	0	255	00FA-00252000
	D5*									
S3	D5_	cTP	No	TP/TP Coupler	-	Unloaded	15	15	0	00FA-00250500
	D1	PB tp	No	Push Button Interface	-	Unloaded	15	15	255	00FA-00250100
	D3	BO tp	No	Binary Output	-	Unloaded	15	15	255	00FA-00250300

Participants virtuels certifiés KNX Secure



Configuration de l'automate ECY-350 en Hub

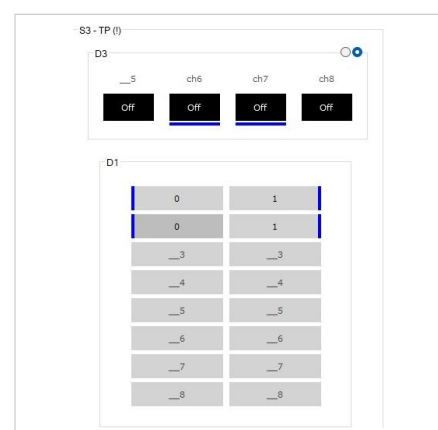
Un certificat KNX propre à chaque participant est à intégrer lors du paramétrage avec le logiciel ETS : il contient le numéro de série du participant et sa clé d'usine. Celui-ci permet l'authentification du participant KNX et le chiffrement des télégrammes KNX échangés. Pour conserver la confidentialité de ces informations, l'accès au projet ETS doit obligatoirement se faire avec un mot de passe.

Une activité pédagogique est réalisée individuellement pour mettre en évidence la démarche permettant d'atteindre le niveau de sécurité attendu.

Formation des étudiants

La sécurité des communications numériques dans les bâtiments communicants est complexe, mais incontournable.

La formation en BTS Fluides Energies Domotique option Domotique et Bâtiments Communicants au lycée Hippolyte Fontaine de DIJON s'inscrit dans cette démarche en les initiant aux risques de cybersécurité et aux mécanismes mis en œuvre.



Interface de simulation KNX Virtual



Francis Cunin

Professeur agrégé en ingénierie électrique

Lycée Hippolyte Fontaine – DIJON

francis.cunin@ac-dijon.fr | <https://lyc21-hfontaine.sd.ac-dijon.fr>

Gestion intelligente des bâtiments pour les PME : comment les petits et moyens projets immobiliers bénéficient de solutions de GTB rentables

Thersa, spécialiste belge du CVC, propose une solution de gestion innovante permettant une exploitation des bâtiments à moindre coût. Adaptée aux petits et moyens projets immobiliers, cette offre s'appuie sur les systèmes intelligents de SAUTER.

La numérisation de la gestion des bâtiments est en plein essor. Plus personne ne doute des nombreux avantages qu'offre un système de gestion technique des bâtiments (GTB) numérique. Pourtant, jusqu'à récemment, seuls les grands groupes pouvaient en profiter. En effet, les coûts élevés d'investissement et d'exploitation de l'infrastructure informatique nécessaire étaient souvent difficilement supportables pour les petites et moyennes entreprises (PME). Depuis 2023, il existe cependant une solution abordable pour les PME : en coopération avec SAUTER Belgique, Thersa – spécialiste belge du chauffage, de la ventilation, de la plomberie et des énergies renouvelables – propose aux exploitants de projets de toutes tailles une gestion intelligente des bâtiments sous forme de Software-as-a-Service. Cette offre de service innovante a déjà fait ses preuves avec succès depuis son lancement il y a environ deux ans. Un facteur clé pour l'intégration côté exploitant est le routeur BACnet/SC modu630-RT de SAUTER.

La solution

Pour que les exploitants de bâtiments puissent bénéficier pleinement des avantages d'un système de GTB numérique, une simple connexion Internet sécurisée à un hub BACnet/SC géré par Thersa suffit. Cette connexion est assurée par le routeur BACnet/SC modu630-RT, issu de la gamme modulo 6 de SAUTER. Cet appareil compact constitue l'élément central du réseau d'automatisation du bâtiment et des locaux côté client, et garantit une transmission sécurisée des données vers le logiciel de gestion externe. Le routeur modu630-RT communique exclusivement par l'intermédiaire du protocole sécurisé BACnet/SC et fonctionne selon le principe « outbound-only ». Cela permet de



Le Carré Jansson (Tournai) ©Thersa

mettre en place un chiffrement de bout en bout des transferts de données et empêche efficacement tout accès non autorisé. Il n'est pas nécessaire de configurer des pare-feux complexes ni de mettre en place des solutions VPN ; la communication reste néanmoins très sécurisée et facile à gérer.

Qu'en est-il des données justement ? En ce qui concerne la solution logicielle centrale et modulaire pour la gestion des bâtiments, de l'énergie et de la maintenance, Thersa met à disposition de ses clients la plateforme d'intégration web SAUTER Vision Center (SVC), hébergée sur ses propres serveurs. Cet outil global collecte de manière fiable et précise toutes les données transmises par le routeur BACnet/SC modu630-RT local, et permet une commande, une analyse et une visualisation confortables des fonctions du bâtiment à distance. L'accès à l'environnement SVC se fait sans risque grâce à une authentification utilisateur à plusieurs facteurs et une connexion réseau sécurisée via SAUTER Remote Management.

Le résultat

Après environ deux ans sur le marché, le constat est clair : Thersa a su capter la bonne tendance avec son approche de service innovante. En renonçant à une infrastructure propre coûteuse – incluant les mises à jour matérielles régulières, les frais de licence et le personnel informatique spécialisé – les exploitants de projets immobiliers petits et moyens, souvent très sensibles aux coûts, ont désormais accès à une GTB professionnelle et sécurisée. Et le nombre d'utilisateurs ne cesse d'augmenter : un signe évident du fort potentiel de cette solution.



Manuel Bouvier

Product Manager | SAUTER Head Office
info@sauter-controls.com
www.sauter-controls.com

Rénovation GTB-CFA du site CARAT 1 (A & B) – Projet livré en 2025 à Châtillon (92)

Contexte

ATEMIA, porteur des lots GTB-CFA a procédé à la dépose de l'ensemble des automates des armoires électriques et CVC ainsi que des équipements GTB liés à la régulation terminale des bureaux, en protocole LonWorks.

Refonte de l'architecture GTB

Le système GTB a été totalement repensé pour mettre en place une architecture réseau full IP, les nouveaux automates qui ont été mis en place communiquent désormais en protocole BACnet/IP. Afin de maintenir une continuité de service, une boucle fibre redondante a été mis en place sur les switches GTB.

Mise en place d'une gestion multi-métiers innovante

Pour ce projet, la régulation terminale multi-

métiers a été réalisée par le biais d'un double système indépendant. La CVC est de type détente direct avec des VRV DAIKIN tandis que la gestion des éclairages a été réalisée par le biais de passerelles et modules Distech Controls, couplés avec leurs multi-capteurs et télécommandes Bluetooth.

ATEMIA a procédé à de nombreux process entre les passerelles et les automates ECY-S1000 des plateaux, afin de centraliser la gestion de la CVC et des éclairages au travers d'une télécommande Allure Uniwave par bureau, dans l'objectif de faciliter la gestion aux locataires.

L'exploitation graphique des données du site

L'ensemble des données du projet remonte sur deux postes serveurs équipés du logiciel de supervision PcVue afin de faire l'acquisition des données et de les redistribuer à deux postes d'exploitation. Les postes serveurs fonctionnent

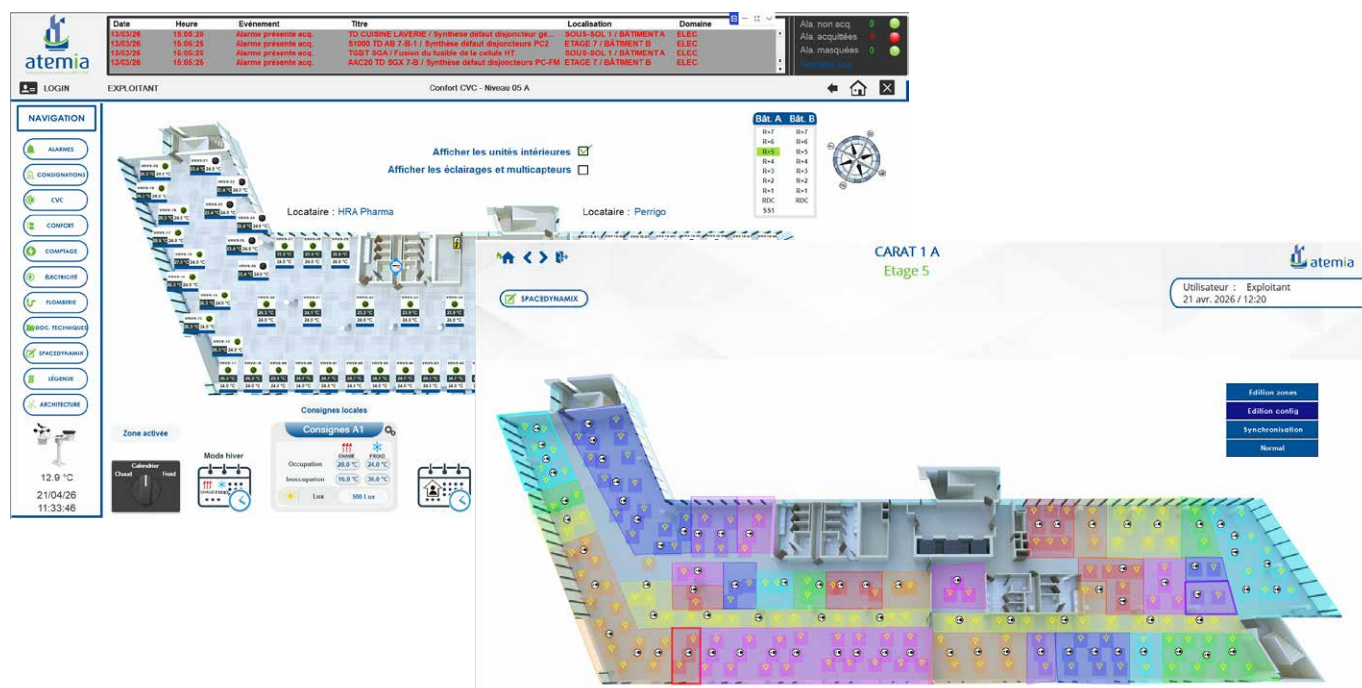
en mode actif / passif avec bascule de l'acquisition lorsque le poste serveur principal n'est pas joignable, afin de maintenir la remontée d'informations sur les postes d'exploitation.

La gestion des énergies

Le logiciel de gestion énergétique AREE Building a été mis en place pour superviser l'intégralité des compteurs d'énergies du site, dans le but de surveiller les consommations d'électricité et d'eau, conformément aux décrets en vigueur.

Nos partenaires pour ce projet

ATEMIA tient à remercier ses partenaires de confiance depuis de nombreuses années, pour leurs conseils et accompagnement : Distech Controls (automates, logiciels EC-Net et Space Dynamix pour le cloisonnement), Inneasoft (logiciel de gestion énergétique AREE) et Arc Informatique (logiciel de supervision PcVue).



ATEMIA :
spécialiste en création, rénovation, maintenance
et audits de systèmes et GTB multimarques



Flavien Picart
Président Directeur Général chez ATEMIA
gestion@atemia.com | www.atemia.com



REIWA : BACnet au cœur d'une architecture ouverte au service de la performance énergétique

À Saint-Ouen-sur-Seine, SDEL IMTEC associe une GTB Schneider Electric EBO et AREE Building dans une architecture ouverte où BACnet/IP constitue une brique structurante de l'interopérabilité et de la performance énergétique.

REIWA, un projet tertiaire ambitieux

À Saint-Ouen-sur-Seine, REIWA accueille le siège de Nexity (Promoteur de l'opération) au sein d'un ensemble tertiaire neuf d'environ 25 000 m². L'actif géré par Ofi Invest Real Estate pour le compte de l'un de ses mandants, est constitué de huit étages de bureaux reposant sur un socle accueillant les services, complété par trois niveaux d'infrastructure. Les plateaux d'environ 2 500 m² ont été conçus pour offrir une grande modularité.

Le bâtiment associe espaces de travail, meeting center, salle polyvalente, coworking, plusieurs offres de restauration et locaux vélos. Les espaces extérieurs et le végétal sont au cœur du projet, avec près de 4 000 m² de terrasses, jardins, balcons et rooftop. Cette ambition s'accompagne d'objectifs élevés de performance environnementale et de connectivité, matérialisés notamment par les certifications et labels HQE® niveau Excellent, BREEAM Excellent, E+C-, BBC Effinergie 2017 et WiredScore.

SDEL IMTEC, l'intégrateur au cœur du projet

SDEL IMTEC est spécialisée dans l'intégration et l'installation de systèmes dédiés à la protection du bâtiment et au Smart Building. Ses compétences couvrent notamment la conception, les études de réalisation, la programmation et la mise en service. Habitée aux grands ensembles immobiliers tertiaires à forte valeur ajoutée en Île-de-France, l'entreprise intervient en GTC/GTB, sûreté, sécurité, Smart Building, Building Operating System et cybersécurité.

Forte de son expérience, SDEL IMTEC privilégie des architectures ouvertes et interopérables afin de préserver la capacité d'évolution des installations et de limiter la dépendance aux solutions exclusivement propriétaires. Partenaire d'INEASOFT depuis plus de dix ans, ses équipes



assurent directement l'intégration et le paramétrage d'AREE Building.

« Nous avons fait le choix de la GTB EBO et du logiciel AREE Building pour garantir l'homogénéité GTB-MES »

BACnet/IP, une brique structurante d'une architecture multitechnologique

Pour répondre aux différents usages du bâtiment, SDEL IMTEC a déployé une GTB Schneider Electric EBO reposant sur un réseau IP. L'architecture associe plusieurs technologies adaptées à leurs fonctions : BACnet/IP pour les régulateurs de terrain, DALI pour l'éclairage, Zigbee pour les sondes radio et Bluetooth pour différents équipements et interfaces utilisateurs.

Le projet compte notamment 607 régulateurs de terrain programmables BACnet/IP, 506 boîtiers d'éclairage DALI, 584 boîtiers de commande des stores, 1 124 détecteurs intégrant présence, luminosité et interface Bluetooth, 435 sondes température/CO₂/hygrométrie en Zigbee et 500 télécommandes Bluetooth.

L'interopérabilité ne consiste toutefois pas à multiplier les protocoles. Lorsqu'un projet permet des choix d'architecture, réduire leur nombre et

REIWA – Saint-Ouen

- ≈ 25 000 m²
- 8 étages de bureaux
- Plateaux ≈ 2 500 m²
- 4 000 m² de terrasses, jardins, balcons et rooftop
- 212 places de parking, dont 48 pour véhicules électriques

Certifications :

- HQE® Excellent
- BREEAM Excellent
- E+C-
- BBC Effinergie 2017
- WiredScore

REIWA, siège social de Nexity à Saint-Ouen-sur-Seine.
Architecture : Brenac & Gonzalez & Associés.

privilégier des standards ouverts, normalisés et largement supportés simplifie l'intégration, l'exploitation et la maintenance, tout en préparant les évolutions futures du bâtiment.

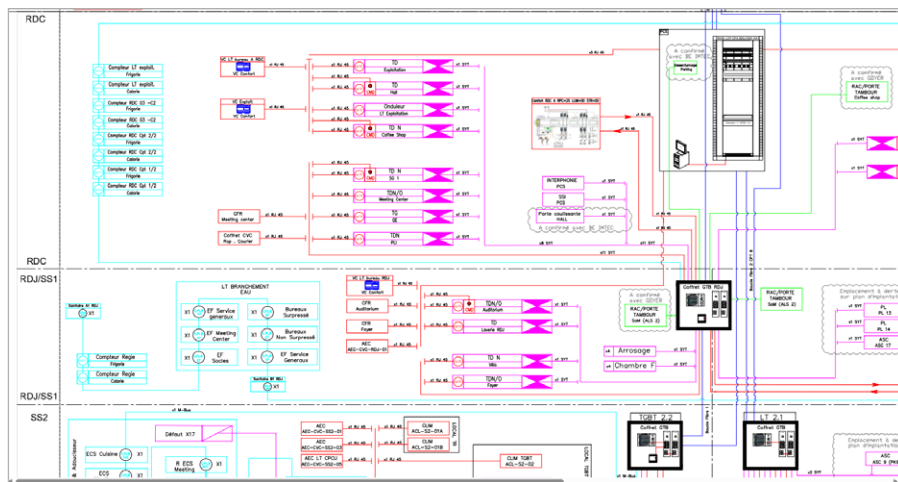
De la GTB au management énergétique

Une architecture complexe derrière une exploitation qui doit rester simple.

EBO et AREE Building : du pilotage au management énergétique

La supervision Schneider Electric EBO centralise les informations nécessaires à l'exploitation et à l'automatisation du bâtiment. Pour le management énergétique, AREE Building collecte l'ensemble des données utiles remontées dans EBO grâce à son connecteur natif à la base de données de la supervision.

Cette architecture évite de reconstruire inutilement une seconde chaîne de collecte. Lorsque certaines informations sont importantes pour le suivi énergétique mais n'ont pas vocation à remonter dans la GTB, parce qu'elles ne sont pas nécessaires à l'automatisation du site, AREE peut également les acquérir directement auprès des équipements concernés au travers de ses connecteurs.



REIWA en quelques chiffres

- 607 régulateurs BACnet/IP
- 506 boîtiers DALI
- 1 124 détecteurs présence / luminosité / Bluetooth
- 435 sondes radio Zigbee
- 500 télécommandes Bluetooth
- GTB : Schneider EBO
- EMS : AREE Building

L'Energy Management bénéficie ainsi des données déjà disponibles dans la GTB, tout en conservant la possibilité d'élargir la collecte aux données spécifiquement utiles à la performance énergétique.

AREE Building : une architecture pensée pour durer

SDEL IMTEC a déployé une licence AREE Building « compteurs illimités » pour assurer le suivi de l'ensemble des comptages du site : eau, électricité du TGBT et des tableaux divisionnaires avec répartition par usages – électricité, CVC, éclairage et stores – ainsi que les comptages de frigories.

Le nombre de points associés aux compteurs étant lui-même illimité, le dimensionnement retenu permet d'accompagner l'évolution du bâtiment sans faire dépendre le coût de licence de l'augmentation du volume de données collectées. Installé On-Premise, AREE Building permet par ailleurs au client de conserver la maîtrise de son architecture et de ses données.

BACnet aujourd'hui... BACnet/SC demain

L'ouverture des systèmes doit désormais intégrer une exigence croissante de cybersécurité. BACnet/SC constitue une évolution importante de l'écosystème BACnet pour sécuriser les communications sur les infrastructures IP. BACnet/SC n'est pas déployé sur REIWA à ce jour.

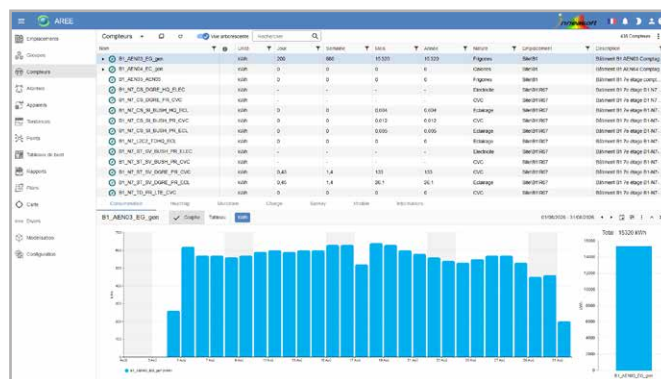
INNEASOFT travaille sur une évolution majeure de son connecteur BACnet intégrant BACnet/SC, prévue pour la fin 2026. Cette évolution sera intégrée aux nouvelles versions d'AREE et mise à disposition sans coût de licence supplémentaire pour les clients couverts par un contrat de maintenance.

L'interopérabilité comme investissement dans le temps

REIWA montre que la performance d'un Smart Building ne dépend pas de la multiplication des technologies, mais de leur capacité à communiquer au sein d'une architecture cohérente. En privilégiant les protocoles ouverts et normalisés et en faisant de BACnet/IP l'une des briques structurantes de la GTB, SDEL IMTEC construit une architecture capable d'intégrer les techno-

logies d'aujourd'hui tout en préparant celles de demain.

L'association de la GTB Schneider Electric EBO et d'AREE Building prolonge cette logique jusqu'au management énergétique : exploiter les données existantes, compléter la collecte lorsque cela est nécessaire et donner aux exploitants les moyens de mesurer, comprendre et améliorer durablement la performance énergétique du bâtiment.



Thierry Chenavas

Directeur Général | INNEASOFT
thierry.chenavas@inneasoft.com



Oliver Cognet

Chef de Groupe | SDEL IMTEC
olivier.cognet@sdel.fr



ecos : des automates polyvalents et intelligents pour l'automatisation de locaux

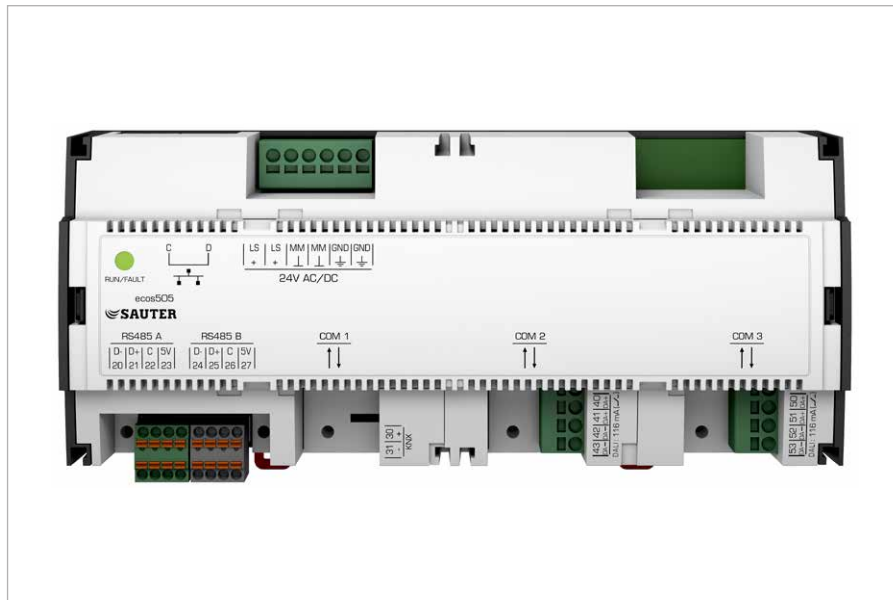
À l'heure où les coûts énergétiques sont élevés, où les objectifs climatiques sont ambitieux et où les exigences en matière de confort sont de plus en plus strictes, les systèmes d'automatisation de locaux jouent un rôle essentiel. L'accent est mis en particulier sur la capacité d'adaptation des solutions aux différents besoins. Bonne nouvelle : les automates de gestion terminale modulaires SAUTER ecos offrent une flexibilité maximale.

Dans le cadre de l'automatisation moderne des locaux, les automates ne se contentent plus de maintenir une température de consigne, mais interconnectent chauffage, refroidissement, ventilation, éclairage et protection solaire au sein d'un système intelligent qui garantit un confort optimal tout en réduisant durablement la consommation d'énergie. Pour les exploitants et les investisseurs, ils sont la clé d'une gestion efficace et pérenne des bâtiments : les flux énergétiques deviennent transparents, les coûts d'exploitation diminuent et la valeur du bien immobilier est préservée à long terme. Avec les automates de gestion terminale ecos de SAUTER, cette tâche exigeante est accomplie de manière simple, intelligente et économique.

Un seul appareil pour tout faire

Les automates programmables ecos514/515 constituent le cœur des solutions intégrées d'automatisation de locaux proposées par SAUTER. Ils regroupent toutes les fonctions centrales dans un seul et même système : de la régulation de la température ambiante à la commande de l'éclairage, en passant par la gestion du système de protection solaire en fonction de la position du soleil. Tout cela étant contrôlé avec une grande précision de réglage. Les fonctions de détection de présence, de surveillance des contacts de fenêtre, de ventilation selon les besoins, de commande de l'éclairage et des stores ainsi que les consignes temporelles optimisent la consommation d'énergie.

Les automates ecos intègrent toutes les fonctions nécessaires aux applications courantes et les capteurs et actionneurs peuvent être raccordés directement dessus. La réduction significative



L'automate ecos515 © SAUTER

des interfaces simplifie considérablement la planification, l'installation et la maintenance. De plus, le boîtier compact pour montage sur rail DIN permet une installation optimale dans les tableaux de distribution électrique. Grâce à cela, et aux bibliothèques d'applications prédéfinies, la mise en service est particulièrement simple et efficace.

Ouverts à tous les défis

L'ouverture des automates de gestion terminale ecos garantit une sécurité d'investissement à long terme, que ce soit pour des constructions neuves ou des rénovations. Ils prennent en charge tous les protocoles de communication courants et répondent ainsi sans difficulté à toutes les exigences d'une automatisation intégrée des locaux. Grâce à la communication standard via BACnet/IP ou BACnet/SC, tous les composants peuvent être connectés de manière simple et efficace à l'automatisation des installations primaires et à la couche de gestion. De plus, BACnet/SC assure une transmission de données chiffrée, garantissant ainsi une cybersécurité maximale et une pérennité du système. Même pour l'intégration des différents lots techniques, le système repose sur des standards éprouvés : DALI (Digital Addressable

Lighting Interface) pour l'éclairage permet une régulation intelligente de la lumière, essentielle pour des conditions d'éclairage optimales. La protection solaire est pilotée via le protocole SMI (Standard Motor Interface), qui assure un positionnement précis et silencieux des stores. Grâce à l'utilisation de KNX ou Modbus comme bus de terrain dans les locaux, il est possible de répondre facilement aux exigences individuelles en matière de design, de confort d'utilisation et d'extensions fonctionnelles. Par ailleurs, les protocoles Modbus et M-Bus permettent une mesure fine et fiable des consommations énergétiques, local par local ou zone par zone.

Évolutivité et flexibilité

Grâce à une gamme complète et bien pensée, l'automatisation intégrée des locaux avec les automates ecos évolue facilement en fonction des besoins du bâtiment et de ses utilisateurs. Jusqu'à 16 modules E/S, 8 boîtiers d'ambiance et 16 capteurs intelligents permettent d'intégrer tous les capteurs et actionneurs nécessaires à l'automatisation intégrée. Le connecteur Cloud IoT en option ouvre l'accès aux services cloud et aux solutions IoT. La segmentation modulaire des locaux (« moving wall ») permet de diviser les surfaces en différentes zones, de les automatiser

par zone et de les adapter à tout moment, en cours d'exploitation, sans intervention structurelle. Et grâce à BACnet, les réglages des automates peuvent être effectués confortablement via le système de gestion technique du bâtiment.

Les possibilités d'utilisation sont tout aussi variées : du boîtier à boutons filaire aux boîtiers d'ambiance radio avec communication bidirectionnelle EnOcean, en passant par des écrans tactiles élégants, les terminaux de commande ecoUnit offrent aux utilisateurs un contrôle total. Température, éclairage, stores ou ventilation peuvent ainsi être réglés de manière intuitive. En complément, les SAUTER Mobile Building Services permettent une commande sécurisée et personnalisée des locaux via l'application Mobile Room Control.

Ce système global fait des automates ecos de véritables vecteurs de valeur : ils allient efficacité, ouverture et flexibilité, créant ainsi des avantages durables pour les utilisateurs, les exploitants et les investisseurs.

En résumé : les automates de gestion terminale modulaires ecos514/515

- Régulation intégrée du climat ambiant, de l'éclairage et de la protection solaire
- Conçus pour une consommation énergétique minimale et un confort utilisateur maximal
- Partie intégrante de la famille de systèmes SAUTER modulo
- Communication ouverte via BACnet/IP ou BACnet/SC, certifiés BACnet Building Controller (B-BC)
- Prise en charge de tous les protocoles courants : DALI, SMI, KNX, Modbus et M-Bus
- Quantification E/S optimisée pour la commande des stores, la régulation de l'éclairage et du climat ambiant
- Évolutivité flexible grâce à une gamme complète avec modules E/S déportés, boîtiers d'ambiance variés et connectivité avec capteurs intelligents et Cloud IoT
- Segmentation flexible des locaux en zones (« moving walls ») pour une adaptation facile en cas de changement d'usage ou d'extension
- Sécurité assurée grâce à la communication chiffrée TLS et à BACnet/SC conforme aux normes actuelles



Manuel Bouvier

Product Manager | SAUTER Head Office
info@sauter-controls.com | www.sauter-controls.com



Régulateur ecos501

Régulateur communicant pour les unités de confort

Le nouveau régulateur configurable ecos501 apporte une approche plus intelligente et plus flexible de la régulation des unités de confort. Grâce à sa communication BACnet, il assure une intégration fluide dans les systèmes de gestion technique du bâtiment.

Au-delà de la connectivité, il se distingue par l'accès via une application mobile et un logiciel de configuration, simplifiant la mise en service, le suivi et les réglages grâce à ses interfaces intuitives.

Principaux avantages en un coup d'œil :

- Régulateur configurable adaptable à différentes applications d'unités de confort
- Mise en service rapide et intuitive via l'outil de configuration PC ou l'application mobile
- Une seule application réunit la gestion du confort pour l'utilisateur final et la configuration technique avancée sur une même plateforme, adaptée aux deux profils d'utilisateurs
- La continuité de bus intégrée maintient la communication réseau même en cas de défaillance ou d'arrêt d'un appareil

Cette solution redéfinit la régulation des unités de confort grâce à une connectivité fluide, une configuration flexible et une utilisation intuitive pour les systèmes CVC modernes.

Plus d'informations disponibles en ligne.

<https://www.sauter.fr/services/produits-complementaires/>



Systems
Components
Services
Facility Management

SAUTER
Pour l'environnement durable.

De la formation à l'intégration GTB : préparer les futurs experts des bâtiments communicants

L'ISTIC de l'Université de Rennes : former les acteurs du bâtiment intelligent de demain

L'ISTIC de l'Université de Rennes propose deux formations en alternance spécialisées dans les domaines de la domotique, de l'immotique et de la gestion technique du bâtiment (GTB). Fort de plus de 30 ans d'expérience dans ces domaines, l'établissement s'appuie sur une plateforme technique dédiée aux bâtiments communicants permettant aux étudiants de se former sur des technologies proches des environnements professionnels.

Ces formations répondent aux besoins croissants du secteur du bâtiment intelligent, confronté à des enjeux majeurs : performance énergétique, amélioration du confort des occupants, exploitation des données, interopérabilité des systèmes et sécurisation des infrastructures communicantes.

Les enseignements couvrent l'ensemble de la chaîne du bâtiment connecté : automatisme du bâtiment, réseaux IP, protocoles de communication, supervision, IoT, jumeaux numériques, physique du bâtiment, ainsi que les aspects liés au conseil et à l'accompagnement des usages.

Dans ce contexte, les étudiants sont formés aux principaux standards ouverts utilisés dans les bâtiments intelligents : KNX, BACnet, LON, Modbus, MQTT, Zigbee, LoRaWAN...

BACnet occupe une place particulière dans les enseignements en raison de son rôle majeur dans les architectures GTB tertiaires.

Deux formations en alternance pour répondre aux besoins de la filière

Les formations proposées par l'ISTIC s'inscrivent dans une logique professionnalisante forte, en lien direct avec les acteurs industriels du secteur.

La Licence Professionnelle « Services et Produits pour l'Habitat » (SPH) forme en un an des techniciens et cadres techniques (Bac+3) capables d'intervenir dans l'installation, la maintenance, l'intégration et le conseil autour des solutions de bâtiments connectés.



Campus de Beaulieu - Bâtiment de l'ISTIC

Le Master 2 « Ingénierie Durable des Bâtiments Communicants Intelligents » (IDBCI) forme des ingénieurs et chefs de projets (Bac+5) capables de concevoir, déployer et piloter des architectures globales d'automatisation du bâtiment, avec une spécialisation forte en GTB/GTC, IoT et systèmes communicants.

L'alternance constitue un élément central de ces formations, permettant aux étudiants de confronter rapidement leurs connaissances aux problématiques rencontrées sur le terrain. Plus de la moitié des enseignements sont assurés par des professionnels du secteur, apportant une vision concrète des évolutions technologiques et des attentes des entreprises.

Une ouverture vers les architectures BACnet/SC

Les évolutions récentes des systèmes GTB renforcent également l'importance des enjeux de cybersécurité et d'architecture réseaux. Dans cette perspective, l'ISTIC s'intéresse depuis plusieurs années aux évolutions du standard BACnet, notamment BACnet Secure Connect (BACnet/SC).

Depuis deux ans, des projets étudiants sont menés afin de mettre en place et d'expérimenter une maquette BACnet/SC multi-constructeurs. Cette démarche vise à étudier concrètement les principes d'une architecture BACnet/SC, ainsi

que les problématiques d'intégration entre équipements issus de différents fabricants.

À moyen terme, cette plateforme expérimentale a vocation à être utilisée dans le cadre de travaux pratiques dédiés à BACnet/SC, afin de permettre aux étudiants d'aborder des thématiques aujourd'hui essentielles pour les futurs intégrateurs GTB :

- architectures sécurisées ;
- gestion des certificats ;
- échanges chiffrés ;
- interopérabilité multi-constructeurs.

Cette démarche illustre la volonté de l'ISTIC d'accompagner les évolutions technologiques du secteur et de préparer les futurs professionnels aux architectures des bâtiments communicants de demain.



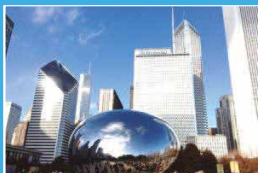
Damien Dubois

Ingénieur d'étude smart building
damien.dubois@univ-rennes.fr

Ghislain Nouvel

Responsable de la licence Professionnelle SPH
ghislain.nouvel@univ-rennes.fr

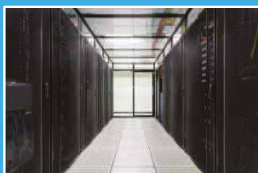
AREE
Building



AREE
Factory



AREE
Datacenter



DECRET tertiaire

-40%
en 2030

-50%
en 2040

-60%
en 2050



Logiciels de management énergétique

www.inneasoft.com

REJOIGNEZ LA COMMUNAUTÉ BACnet EN FRANCE

Devenez membre de BACnet France !

Ensemble, faisons de BACnet – et de BACnet/SC – le standard ouvert et sécurisé du bâtiment.



1 Le réseau

Profitez des contacts de la communauté et suivez de près l'évolution du standard, en lien étroit avec BIG-EU et BACnet International.

2 La visibilité

Mettez en valeur vos compétences sur les salons (IBS, EnerJ-meeting...) et publiez vos produits et références dans le BACnet France Journal.

3 La crédibilité

L'adhésion est une preuve de compétence et de votre engagement pour le protocole et ses dernières évolutions.

4 Les formations

Soyez informé en priorité des formations BACnet de tous niveaux, en France et à l'étranger.

Comment adhérer ?

Adressez-nous une **demande motivée**. Elle est examinée par les membres et soumise au vote – réponse sous quelques jours.

REJOIGNEZ-NOUS >

Votre interlocuteur

Florent Trochu

Délégué Général

[florent.trochu@](mailto:florent.trochu@acr-regulation.com)
acr-regulation.com

[bacnetfrance.org/](http://bacnetfrance.org/rejoignez-nous)
rejoignez-nous



Date	Lieu	Événement	Contact
2026-2027			
14.-15.10.2026	Paris, Porte de Versailles	IBS – Intelligent Building Systems	www.ibs-event.com
02.-03.11.2026	Teltow (près de Berlin, Allemagne)	BIG-EU Autumn Meeting	www.big-eu.org/events/autumn-meeting-big-eu-with-elections
23.02.2027	Paris, Carrousel du Louvre	EnerJ-meeting Journée de l'efficacité énergétique et environnementale du bâtiment	www.enerj-meeting.com
15.-19.03.2027	Francfort-sur-le-Main, Allemagne	ISH 2027	ish.messefrankfurt.com/frankfurt/en.htm
12.-14.05.2027	Lieu à confirmer	Plugfest 2027	
Novembre 2027	Paris, Porte de Versailles	IBS - Intelligent Building Systems	www.ibs-event.com

BACnet France Journal



Présentation du numéro 20 – Novembre 2027

Thème principal : la cybersécurité avec BACnet SC

Date limite d'enregistrement : Juin 2027

Date de parution : Novembre 2027

Nous nous réjouissons de recevoir vos contributions à l'adresse : pogliani@tema.de

Notes de la rédaction

BACnet France Journal
ISSN 2190-9431

Diffusion

Vous pouvez commander ce journal par mail à : pogliani@tema.de

Diffusion en ligne

Au format PDF sur www.bacnetfrance.org et www.bacnetjournal.org/bacnet-journale/bacnet-france-journal/

Editeur

Association BACnet France

Comité de Direction

Président :

Jean Daniel NAPAR (DN Consulting)

Vice-Présidents :

Arnaud AMALRIC (JOHNSON CONTROLS),

Lucien RIVER (KIEBACK & PETER)

Trésorier :

Florent TROCHU

Délégué Général :

Florent TROCHU

Secrétariat

E-mail : contact@bacnetfrance.org

Rédaction et publicité

TEMA Technologie Marketing AG

Marta Pogliani et Hans Symanczik

Tel : + 49 241 889 705 75

E-mail : pogliani@tema.de ; symanczik@tema.de

Photos

BACnet France et entreprises indiquées.

Copyright / Tous droits réservés

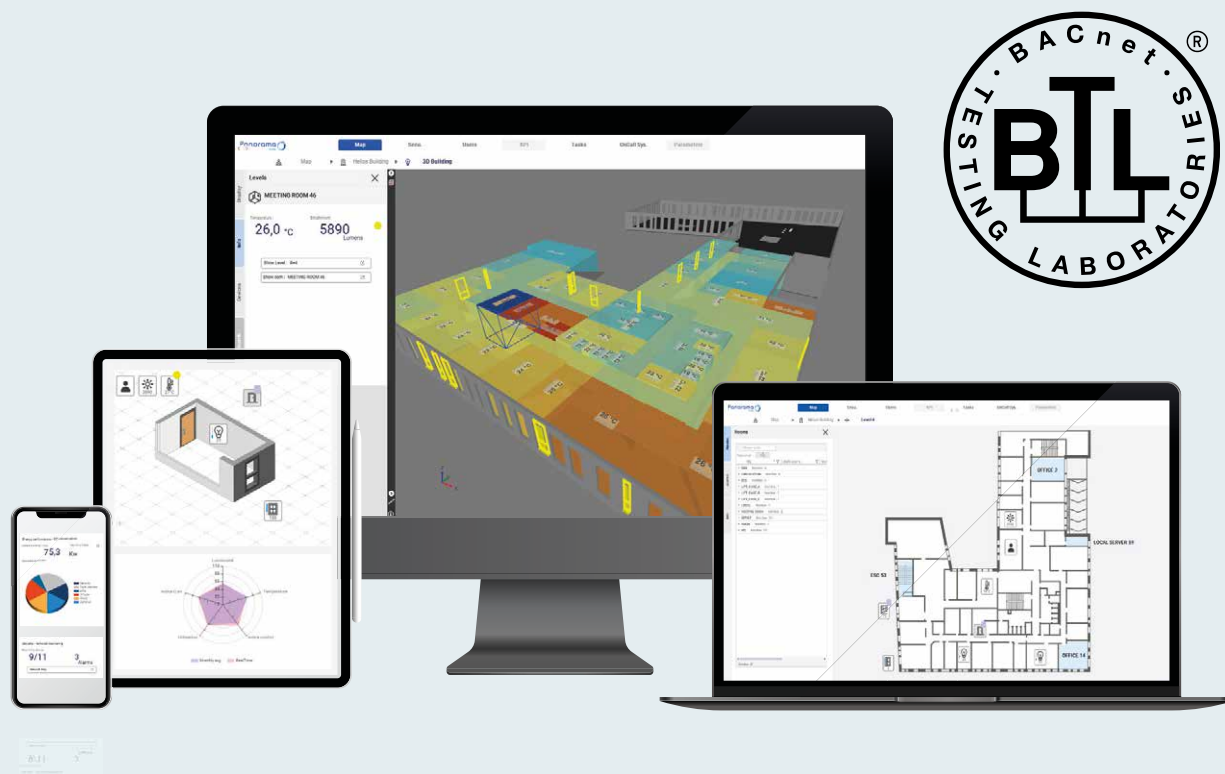
© 2026 – En cas de publication d'un des articles merci de faire référence aux sources, d'envoyer une copie de la parution ou l'URL à pogliani@tema.de

Le client est entièrement responsable du contenu ou de recevabilité juridique des annonces et photos parues dans ce magazine. Il se porte garant que les droits des tiers ne sont pas affectés par cette publication. Le cas échéant le client devra répondre de toute réclamation qui pourrait être effectuée par un tiers. Le client devra indemniser le fournisseur, en l'occurrence Tema AG, de toute réclamation découlant de la violation du droit d'auteur. Le fournisseur, n'est pas tenu de vérifier si les droits des tiers sont affectés par ses ordres et les annonces.

BACnet® est une marque déposée de l'American Society of Heating, Refrigerating, and Air Conditioning Engineers, Inc. (ASHRAE).

L'IA au cœur de votre plateforme d'exploitation

Panorama Suite, une expérience augmentée
au service de la performance de vos bâtiments



IA intégrée à l'environnement de développement



Anomalies détectées automatiquement avant l'incident



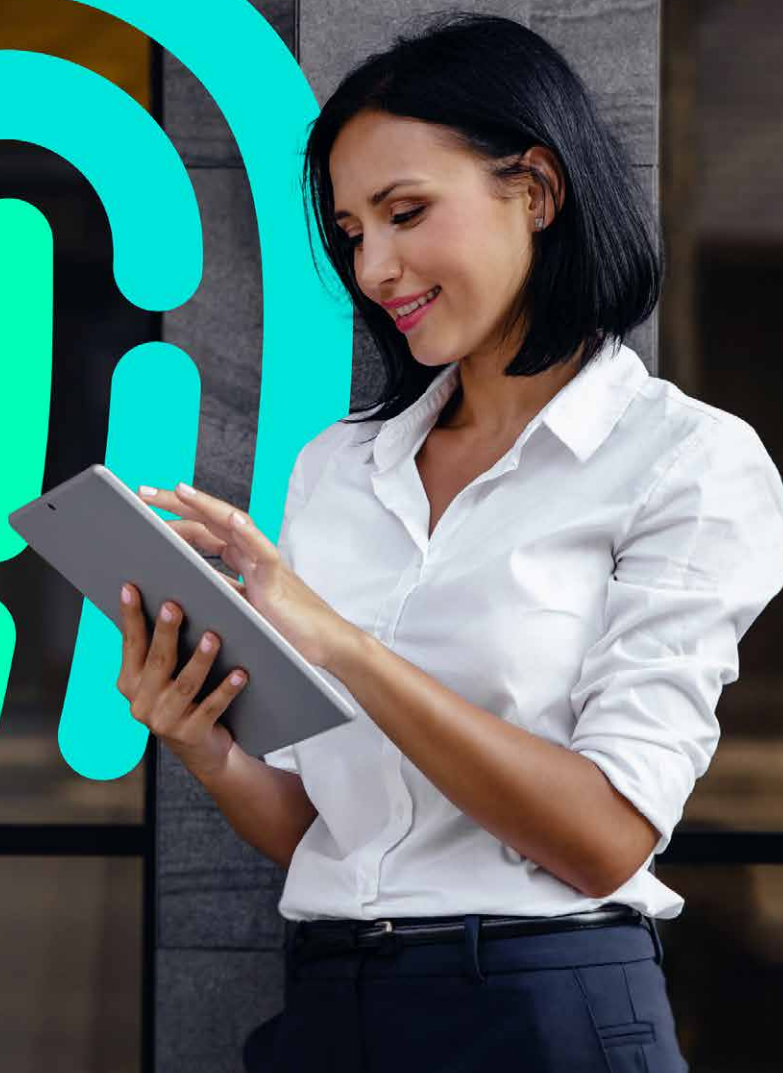
Données sécurisées dans l'application



Applications évolutives, adaptées à vos métiers

**Donnez une nouvelle dimension à votre GTB/GTC
grâce aux capacités d'IA de Panorama Suite.**





Sécurisez vos systèmes d'automatisation du bâtiment avec **BACnet Secure Connect**

Cette technologie garantit une communication sécurisée et fiable au sein de votre infrastructure, assurant ainsi la pérennité de vos investissements.

BACnet Secure Connect renforce la protection de vos systèmes d'automatisation face aux cybermenaces.

Adoptez une approche durable pour la sécurité et la longévité de vos bâtiments.

[siemens.fr/smart-infrastructure](https://www.siemens.fr/smart-infrastructure)

SIEMENS