www.bacnetfrance.org

ISSN 2190-9431

BACnet France Journal

Numéro 18

Septembre 2025

Contexte réglementaire pour la Cybersécurité en France/EU 5

La filière BACS au service de la performance énergétique et environnementale des bâtiments 12

Pourquoi faire remonter les informations BACnet jusqu'au jumeau numérique ? 20

Stratégie énergétique intelligente : les clés de la transition avec PcVue 27

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

SIEMENS

La Cybersécurité pour la Convergence IT/OT avec BACnet/SC

L'énoncé de cet EDITO 2025 est d'ans l'air du temps. Le sujet est développé dans l'environnement du bâtiment, même s'il y a aussi la convergence IT/OT pour l'environnement industriel.

Il y a trois sujets dans le titre qui ont besoin d'être abordés aussi séparément. Ce qui va être fait dans 3 articles séparés dans ce BACnet Journal France, à savoir :

- La réglementation Cybersécurité en Europe et sa transposition en France. Une attention particulière va être accordée à la Directive EU NIS2 (Network and Information Security)
- La Convergence IT/OT dans les bâtiments. L'utilisation accrue de l'informatique dans les bâtiments font que la distinction entre les moyens utilisés à la fois pour l'infrastructure technique du bâtiment (traitement des données en temps réel) et celle des applications utilisateur qui nécessitent aussi des données issues de l'infrastructure technique (traitement des données en temps différé) amènent des conséquences sur des domaines qui jusqu'à lors, n'ont pas eu des nécessités de convergence. L'article va développer plusieurs aspects de cette convergence, en fonction des définitions et hypothèses arrêtées, validées par le marché à ce jour.
- Fondamentaux et Prescriptions en vue du déploiement de BACnet/SC

Les sujets peuvent être traités indépendamment. Mais l'évolution et le changement de ces trois aspects sont différents et faits par des acteurs différents, qui a priori n'ont pas seulement des buts différents, mais pour la plupart des cas, ne communiquent pas entre eux. Voir pire, ils s'ignorent. Mais, hélas, les sujets sont reliés à la vie et l'évolution qui est pratiquement spécifique pour chaque bâtiment. In fine, le sujet revient au propriétaire (ou ses délégués) pour chaque type de bâtiment de se conformer à la réglementation correspondante, de s'assurer du bon marché de son infrastructure technique, avec les aspects de maintenance et exploitation et mises à jour de son BACS affèrent, ainsi que des applications (nommons les « API ») adaptées pour tous les types d'utilisateurs.

Il faut dire qu'il y a une distinction entre les deux cas : bâtiment neuf ou évolution, mise à jour d'un bâtiment existant.

Le bâtiment neuf est au début du processus de construction, et par conséquent toutes les phases du processus à partir du programme, suivi par la conception jusqu'à la réception seront franchies, à la fois pour le marché public et pour le marché privé.

Pour un bâtiment neuf, la première obligation est la conformité réglementaire. Cela, veut dire par exemple que l'obligation de consommation énergétique réglementaire et le calcul de l'empreinte carbone, seront imposés et évalués avec le moteur de calcul réglementaire national. En fonction du résultat, le permis de construire sera accordé ou pas. Les règles de l'art seront ensuite appliquées pour l'enveloppe et toute l'infrastructure technique et pour tous les 5 usages réglementaires (ex. équipements, capteurs, actionnaires, système BACS, ordinateurs, réseaux, etc..). Le bon sens voudra que tous les composants, produits et systèmes qui seront mis en œuvre seront aux derniers niveaux technologiques connus et disponibles sur le marché. Ceci aura comme résultat un bâtiment qui assurera l'optimum équilibre technico- économique pour l'ensemble: l'enveloppe, les équipements bien dimensionnés et un système BACS qui sera conçu pour une consommation à la demande.

Ce ne sera pas le même cas pour un bâtiment existant. La première barrière est la disponibilité et la qualité des données concernant sa conception et la traçabilité sur tous les aspects pour son évolution. Il s'agit aussi de savoir dans quelles conditions ont été assurées la maintenance et l'exploitation du bâtiment et avec quels investissements dans les équipes en charge de ces missions. En fonction de ces paramètres, non exhaustifs, plusieurs défis vont être devant une opération de mise à jour du bâtiment existant sur les angles réglementaires, techniques, et financièrement raisonnable.

Nous allons vous citer plusieurs défis (non exhaustifs) dans les trois domaines.

Premièrement, la réglementation change dans des domaines imprédictibles, avec l'évolution des Directives EU (nous sommes à la 4ème version DPEB de mai 2024 et sa transposition dans la réglementation française n'est pas intégralement achevée). Il est clair qu'un bâtiment construit dans les années 2000 par exemple, était réglementaire s'il été construit CONFORME à la réglementation RT2000. Il ne sera plus réglementaire au regard des Décrets BACS I et II et du Décret Tertiaire en 2025. Et sa mise à jour amènera des spécifications très précises à respecter concernant sa consommation et son empreinte carbone.

Ensuite, au point de vue technique, si le réseau de communication utilisé était BACnet, il faut revoir peut-être sa mise en œuvre pour le support physique à BACnet/IP. Mais bonne nouvelle, la compatibilité ascendante de BACnet assurera la protection des investissements des utilisateurs et les régulateurs pourront continuer à fonctionner tel quel. L'évolution pourra venir seulement si la réglementation cybersécurité va devenir entre temps obligatoire. Plusieurs articles de ce numéro du BACnet Journal France traite de ce sujet. De nouveau une bonne nouvelle, le déploiement à grand échelle de BACnet/SC répondra parfaitement à la réglementation cybersécurité.

Le troisième défi (l'argent) est en effet très important car à ce jour, le non-respect de la réglementation et/ou les règles de l'art technique ne sont pratiquement jamais sanctionnés. Ce qui induit que le parc installé non réglementaire à date reste important, et cela empêche l'atteinte des objectifs de réduction des consommations énergétiques et de l'empreinte carbone. L'exemplarité demandée aux bâtiments publics pourra influencer positivement le marché public.

L'Association BACnet France s'est donnée comme mission, avec d'autres organisations professionnelles comme le Syndicat ACR, Alliance BACS et KNX France, de faciliter le déploiement de la réglementation et les règles de l'art de BACS sur le marché français. BACnet/SC est maintenant une solution présente dans les produits et systèmes de série de constructeurs BACS.
Une attention particulière sera accordée aux projets multi constructeurs pour donner satisfaction aux utilisateurs. Les membres de BACnet France seront les premiers à bénéficier et nous faisons appel pour nous rejoindre en déposant votre candidature au Délégué Général de BACnet France, Mr Florent Trochu (florent.trochu@acr-regulation.com).

Dan Napar
Président BACnet France, Membre Advisory Group BIG-EU

Édito

La Cybersécurité pour la Conver-gence IT/OT avec BACnet/SC 3

Tendances et évolutions technologiques

Contexte réglementaire pour la Cybersécurité en France/EU 5

Convergence IT/OT dans les bâtiments et BACnet/SC 8

Fondamentaux et Prescriptions en vue du déploiement de BACnet/SC 10

La filière BACS au service de la performance énergétique et environnementale des bâtiments 12

HTTPS sécurisé offre une sécurité renforcée dans un système de gestion de bâtiment 14

Les aspects de sécurité gagnent en importance 16

Références

Rénovation du groupe scolaire Petit Val a Sucy en Brie (94) 18

Pourquoi faire remonter les informations BACnet jusqu'au jumeau numérique ? 20

L'interopérabilité des équipements techniques BACnet IP 23

ATEMIA
Intégrateur de solutions multimarques, multi-protocoles 25

GTB et enseignement : le pari gagnant de Marcq Institution pour mieux maîtriser ses consommations. 26

Produits

Stratégie énergétique intelligente : les clés de la transition avec PcVue 27

Consommation d'énergie AREE : Le suivi simplifié grâce à BACnet 28

BACnet News

Optimisez la cybersécurité de vos bâtiments grâce à BACnet/SC et à l'interopérabilité multimarques 30

BACnet France lance son nouveau site web intégré à la présence web unifiée de la communauté BACnet mondiale 31

BACnet/SC : Comprendre la norme dédiée à la sécurité des bâtiments 32

Notes de la rédaction 35

Dix-huitième édition | Septembre 2025

Photo de couverture
Bâtiment ESTP-ESEO inauguré en 2022 et faisant partie des premières réalisations de France labellisées Ready 2 Services ***
© Lycée Hyppolite Fontaine

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

Contexte réglementaire pour la Cybersécurité en France/EU

Contexte réglementaire pour la Cybersécurité en France/EU

Le mot **cybersécurité** est un néologisme désignant le rôle de l'ensemble des lois (réglementations), politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies. La Cybersécurité est à utiliser pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des États et des organisations (avec un objectif de disponibilité, intégrité et authenticité, confidentialité, preuve et non-répudiation).

Le terme cybersécurité est construit à partir du préfixe « cyber », d'origine grecque, réapparu au milieu du XXe siècle avec le mot cybernétique. En 1947, le mathématicien Norbert Wiener a introduit cette notion de « cybernétique » pour la classification d'une science interdisciplinaire. Son but était de donner une vision unifiée des domaines naissants de l'automatique, de l'électronique et de la théorie mathématique de l'information, en tant que « théorie entière de la commande et de la communication, aussi bien chez l'animal que dans la machine ».

La cybernétique introduit la notion de rétroactivité (feedback en anglais), à savoir : l'action en retour d'un effet sur l'origine de celui-ci. Au niveau supérieur, un système comportant une boucle de rétroaction a un effet de stabilisation des écarts par rapport à une consigne. Le feedback négatif est la base de la régulation (sa définition même) et la REGULATION EST LA BASE DE LA GTB! Cette discipline est reconnue par la réglementation en France sous le nom de Building Automation and Controls Systems, BACS, tels que définis das les Décrets BACS I et II!

Ce préfixe « cyber » a donné avec le développement d'Internet et la généralisation du numérique, un grand nombre de mots tels que cyberespace, cyberdéfence, ciberattaque, cybercrime, cybercagé, cyberculture, cyberdémocratie, cybermarché, cyber-réputation.

C'est par réaction contre les risques liés à l'omniprésence des TIC's (Technologies de l'information et de la communication) et à leur capacité d'interconnexion et d'échange de données que la cybersécurité se constitue progressivement en tant que nouvelle discipline (spécialité) pleine et entière. Par conséquent, elle a fait l'objet de réglementations sans cesse évolutives par des directives Européennes transposées en France par la réglementation cyber. Nous nous concentrons dans cet article sur la réglementation NIS2.

En France, la transposition de cette Directive en droit national est en cours.

Chaque État membre est tenu d'adapter ses réglementations internes pour se conformer aux exigences de NIS 2. Cette transposition implique l'identification des entités concernées, l'établissement de mesures de sécurité obligatoires et la mise en place de mécanismes de notification des incidents.

Pour accompagner les organisations dans cette transition, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) fournit des ressources et des outils dédiés. Par exemple, la plateforme "Mon Espace NIS 2" offre des informations actualisées sur l'avancement de la transposition et des conseils pratiques pour se conformer aux nouvelles obligations.

Il est essentiel pour les entités concernées de se préparer dès maintenant à ces évolutions réglementaires, en renforçant leurs mesures de cybersécurité et en s'informant sur les nouvelles obligations qui leur incombent.

En quoi consistait la précédente directive NIS 1 ?

La transformation numérique (digitalisation) des sociétés européennes et l'interconnexion des pays membres ont exposé le marché européen a de nouvelles cybermenaces. Il devenait alors urgent de garantir, collectivement, les conditions de sécurité adéquates pour toute l'Union Européenne.

C'est pourquoi le Parlement Européen et le Conseil de l'Union Européenne ont adopté, en juillet 2016, la Directive « Network and Information Security » (NIS 1).

Transposée au niveau national en 2018, cette Directive avait pour objectif d'augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activités stratégiques (ce qui représente quelques centaines d'entités en France).

Avec ce premier dispositif, ces grands acteurs ont été soumis à l'obligation de déclarer leurs incidents de sécurité à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), et de mettre en œuvre les mesures de sécurité nécessaires pour réduire fortement l'exposition de leurs systèmes les plus critiques aux risques cybers

Qu'est ce qui va changer avec l'adoption de la directive NIS 2 ?

La directive NIS 2 s'appuie sur les acquis de la directive NIS 1 pour marquer un changement de paradigme, tant à l'échelon national qu'à l'échelon européen.
Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2 élargit en effet ses objectifs et son périmètre d'application pour apporter davantage de protection.

Avancement de la transposition de la directive NIS 2

La directive NIS 2 a été publiée le 27 décembre 2022 au Journal Officiel de l'Union Européenne et elle prévoit que chaque Etat membre transpose en droit national les différentes exigences réglementaires.

La transposition de la Directive se déroule en deux temps principaux :

La phase de préparation du projet de loi, qui a été présenté en Conseil des Ministres le 15 octobre 2024, en vue de son dépôt au Parlement et de son adoption. Les 11 et 12 mars 2025, le Sénat a examiné puis adopté en séance publique le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Porté par Madame Clara Chappaz, Ministre déléguée chargée de l'Intelligence artificielle et du Numérique, ce projet de loi transpose trois directives européennes : REC (en français REC = Résilience des Entités Critiques ; en anglais CRA

= Cyber Resilience Act), NIS 2 et DORA (Digital Operational Resilience Act), dont les objectifs sont de renforcer la sécurité et la résilience des infrastructures.

Ce passage au Sénat est une première étape clé dans la transposition de la Directive NIS 2 et l'élévation générale du niveau de cybersécurité en France. Grâce au travail des Rapporteurs, des membres de la commission spéciale et des Sénateurs, le texte a été renforcé afin de mieux répondre aux besoins de sensibilisation et de lisibilité sur ces enjeux.

Enfin, la phase de production des décrets et arrêtés aboutira à l'issue des consultations, afin de les soumettre à une validation interministérielle pour publication des textes dans les mois suivants la promulgation de la loi.

NIS 2 rentrera donc en vigueur en France dès lors que l'ensemble des textes de transposition (loi, décrets, arrêtés) auront été promulgués. Il est utile de préciser que la date d'entrée en vigueur ne correspond pas à la date d'application de l'ensemble des exigences réglementaires qui seront imposées aux entités régulées.

Les entités essentielles (EE) et entités importantes (EI)

Pour garantir une proportionnalité de traitement, la directive NIS 2 distingue deux catégories d'entités régulées :
EE -> Entités essentielles et **EI** -> Entités importantes.

Cette catégorisation s'établit selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises).

La Directive désigne deux catégories distinctes d'entités qui entrent dans le champ d'application de ses exigences :

- **Entités essentielles** – organisations opérant dans un secteur crucial au sein duquel une cyber-perturbation pourrait causer un préjudice grave à l'économie ou à la société (par exemple, la santé et l'énergie). Un seuil de taille s'applique également : les entités essentielles de ces secteurs clés doivent avoir au moins 250 employés OU un chiffre d'affaires annuel d'au moins 50 millions d'euros OU un bilan annuel d'au moins 43 millions d'euros.
- **Entités importantes** – il s'agit soit d'organisations de taille moyenne opérant dans un secteur clé, soit d'organisations de taille moyenne ou grande opérant dans n'importe quel secteur autre que les secteurs critiques. Pour atteindre le seuil de taille moyenne, les organisations doivent avoir au moins 50 employés OU un chiffre d'affaires annuel (ou un total de bilan) d'au moins 10 millions d'euros.

Les deux catégories d'entités doivent se conformer à la Directive. La différence principale étant que si vous faites partie des entités essentielles, votre conformité est supervisée de manière proactive ; les entités importantes ne sont contrôlées que si un incident de non-conformité se produit et est signalé.

Étant donné que pour le moment la transposition a pris du retard, la CSNP (La Commission Supérieure du Numérique et des Postes) propose d'accorder « une certaine souplesse dans l'appréciation des infractions aux obligations et les sanctions relatives jusqu'au 31 décembre 2027 ».

Les trois principaux changements entre NIS 1 et NIS 2 sont les suivants :

- La NIS 2 ajoute une série de nouveaux secteurs économiques afin d'étendre son champ d'application à un plus grand nombre d'organisations jouant un rôle important dans les écosystèmes numériques modernes.
- Élimination des incohérences dans la mise en œuvre en clarifiant les exigences en matière de sécurité, de signalement des incidents et d'application valables pour toutes les organisations et tous les États membres.
- Mise en place d'une planification, d'une gestion de crise et d'une collaboration accrue entre les États membres en cas d'incidents de cybersécurité à grande échelle susceptibles d'entraîner des répercussions systémiques

Le champ d'application de la NIS 2

Pour comprendre l'importance de l'extension du champ d'application de la NIS 2, examinons les nouveaux secteurs qui y sont inclus :

- Réseaux ou fournisseurs de services publics de communications électroniques ;
- Gestion des eaux usées et des déchets ;
- Fabricants de produits clés comme les produits chimiques et les dispositifs médicaux ;
- Alimentation ;
- Services numériques comme les réseaux sociaux et les services de centres de données ;
- Aérospatiale ;
- Services postaux ;
- Administration publique.

Ces secteurs s'ajoutent aux **sept secteurs** déjà concernés par la première version du NIS 1 : santé, infrastructures numériques, transports, approvisionnement en eau, fournisseurs de services numériques, énergie, banques et infrastructures des marchés financiers.

NIS 2 : 10 obligations clés

Pour permettre aux entités de mieux comprendre leurs obligations et d'atteindre un niveau élevé de cybersécurité commune, la NIS 2 définit 10 mesures essentielles de gestion du risque cybernétique.

- Disposer de politiques décrivant les approches en matière d'évaluation des risques et de sécurité générale de l'information.
- Mettre en place des plans appropriés pour le traitement des incidents de sécurité.
- Disposer de politiques et de procédures comme des tests et des audits permettant d'évaluer l'efficacité des mesures de sécurité.
- Aborder la question de la sécurité de la chaîne d'approvisionnement et définir les relations et la connectivité entre une entreprise et ses fournisseurs.
- Renforcez l'authentification grâce à l'authentification multifactorielle ou à des solutions d'authentification continue. De même, sécurisation des communications vocales, vidéo et textuelles grâce au cryptage.
- Assurer une formation à la cybersécurité et une cyber hygiène de base pour les utilisateurs.
- Disposer de plans de continuité des activités comprenant des mesures de gestion des sauvegardes, de reprise après sinistre et de gestion de crise.
- Donner la priorité à la sécurité lors de l'acquisition de réseaux et de systèmes d'information, du développement et de la maintenance de ces systèmes grâce à des mesures telles que le traitement et la divulgation des vulnérabilités.
- Établir des politiques et des procédures concernant l'utilisation de la cryptographie et, le cas échéant, du chiffrement.
- Assurer la sécurité des ressources humaines, mettre en œuvre des politiques de contrôle d'accès et assurer une gestion efficace des actifs.

Gouvernance et mise en œuvre de la NIS 2

Comme pour beaucoup d'autres réglementations, des sanctions sont prévues en cas de non-respect des mesures de gestion des cyber-risques ou des obligations de déclaration. La NIS 2 impose des sanctions pécuniaires élevées pour encourager les organisations à s'aligner sur ses exigences et à s'assurer que la gravité des risques encourus est réellement comprise.

Chaque État membre peut décider de ses propres amendes, mais la limite supérieure des amendes maximales applicables au non-respect de la NIS 2 est :

- Pour les entités essentielles : soit 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial ;
- Pour les entités importantes : 7 millions d'euros ou 1,4 % du revenu annuel global.

Le montant le plus élevé des deux chiffres pour chaque type d'entité constitue la sanction finale à payer. La directive NIS 2 ne se limite toutefois pas aux sanctions pécuniaires. Les mesures punitives de la directive comprennent des dispositions sur la responsabilité des personnes occupant des postes de direction en cas d'incidents cybernétiques au cours desquels une entreprise ferait preuve de négligence grave.

L'objectif est de retirer la charge de la sécurité aux seuls départements informatiques et de veiller à ce que les cadres supérieurs prennent leur part de responsabilité dans la mise en œuvre des mesures de protection de la NIS 2. Les autres conséquences potentielles peuvent être les suivantes :

- Devoir rendre publiques les violations de la conformité et, par conséquent, affecter la réputation de votre organisation;
- Faire des déclarations publiques identifiant le cadre supérieur responsable de la violation ;
- En cas de violations répétées dans des entités essentielles, une interdiction temporaire pour les personnes responsables d'occuper des postes de direction dans l'entreprise.

La gestion des vulnérabilités basée sur les risques comprend également une documentation et un rapport détaillé sur les vulnérabilités identifiées, les risques associés et les mesures prises pour y remédier. Ces informations sont essentielles pour répondre aux exigences de la NIS 2 en matière de rapports d'incidents.

Pour l'application de la NIS2 dans les bâtiments, il faut porter une attention particulière aux différents types de bâtiments utilisés pour des sujets et/ou processus sensibles.

On peut citer notamment :

- Les hôpitaux
- Bâtiments des forces de l'ordre (armée, police, gendarmerie,)
- Banques
- Laboratoires
- …

Dan Napar
Président BACnet France | Membre Advisory Group BIG-EU
dan.napar.ext@siemens.com | DN Consulting

Convergence IT/OT dans les bâtiments et BACnet/SC

Quelques précisions pour le glossaire (terminologie) utilisé et qui donnera le sens de l'énoncé du titre utilisé. L'article fait référence au domaine du bâtiment. Le terme Convergence IT/OT a été utilisé pour la première fois dans le domaine industriel, mais dorénavant il a été adopté aussi pour les bâtiments.

IT est un terme anglais (Information Technologies) qui désigne les technologies de l'information et que nous appelons tout court informatique. Dans le contexte de cet article il s'agit d'un système informatique.

OT est un terme anglais (Operational Technology) qui désigne les technologies de contrôles et actions maitrisés dans le processus physique, qui détectent et/ou provoque un changement, par le biais de la surveillance ou du contrôle direct d'équipements dans les bâtiments. Dans le contexte de ce chapitre il s'agit d'un système BACS (système de régulation et GTB).

Convergence est un terme en soi pour définir une action d'aboutir au même résultat, de tendre vers un but commun. Dans le contexte de cet article il s'agit de la convergence numérique (monde digital), un phénomène qui tend à fusionner l'information, le support et le transport des données, avec les processus physiques dans les bâtiments (monde physique).

La convergence des technologies de l'information (IT) et des technologies opérationnelles (OT) est un phénomène encore et toujours en pleine expansion, et est accentué par la digitalisation tous azimuts en route, qui touche aussi les bâtiments. Alors que les deux domaines ont historiquement fonctionné de manière distincte, ils se rejoignent désormais pour apporter ensemble les buts attendus par les utilisateurs.

Dans ce contexte, le déploiement par les constructeurs de BACS de la solution BACnet/SC est la solution appropriée pour rendre conforme les bâtiments neufs avec la réglementation et assurer l'évolution des bâtiments existants.
Cependant, cette convergence apporte avec elle un ensemble complexe de défis, notamment des problèmes organisationnels, de gouvernance et de cybersécurité, et par la même occasion technique, pour respecter la réglementation à jour. Il ne faut pas oublier que premièrement un bâtiment doit être réglementaire.

Convergence des données

Simplifions les choses en répertoriant les données en 4 grandes catégories :

Du côté OT :
- Les données et processus métiers : celles qui servent à réaliser la mission de la régulation des usages, les quatre phases de transformation physique de l'énergie, commandes, programmation horaire, qualité environnementale de l'intérieur (IEQ en anglais), maintenance, exploitation, conditionnement, transport, sureté …) REMARQUE : La qualité environnementale de l'intérieur (IEQ) couvre 4 domaines : Qualité de l'air intérieur (IAQ), confort thermique (principalement la température), l'éclairage et l'acoustique.

- L'infrastructure qui support les processus: Les données techniques des BACS, celles-là même qui permettent de maintenir et faire évoluer le système BACS lui-même (documents d'architecture, sauvegarde, configuration, supervision, administration, maintenance, gestion des données etc. …), monitoring, établir des scenarios d'automatisme, définir et mettre en œuvre des optimisations, etc…

Du côté IT :
- Les données de gestion : consommations énergétiques sur les processus administratifs du bâtiment, information des utilisateurs inclus avec celles des données de qualité environnementale et consommation énergétiques, (paie, ressources humaines, clients, fournisseurs, facturation, juridique etc. ...)

- L'infrastructure qui supporte l'informatique de gestion : Les données techniques du système informatique, celles-là même qui permettent de maintenir et faire évoluer le système d'information lui-même (documents d'architecture, sauvegarde, configuration, supervision, administration, maintenance, gestion des données etc. …)

REMARQUE : Les fonctions importantes assurées par l'IT sont : acquisition des données, archivage des données, structuration des données dans des bases des données, présentation des données aux programmes utilisateurs (nommés aussi « API »)

Hier, ces données étaient sans rapport les unes avec les autres, mais l'optimisation des processus va engendrer des mouvements bidirectionnels de données entre les BACS et le Système de Gestion Informatique dans un premier temps. Et au niveau infrastructure dans un second temps, d'abord sous l'impulsion des problèmes technologiques puis par la cybersécurité.

A cela, ajoutons la problématique du lieu de stockage des données. Les besoins en stockage allant grandissant, l'émergence du Cloud permet de délocaliser tout ou partie des données du bâtiment, ce qui pose à nouveau question autour de la sécurité des données quand bien même les prestataires offriraient toutes les garanties nécessaires à ce sujet.

La convergence des moyens techniques

La convergence des moyens techniques reste un sujet très délicat en matière de cybersécurité surtout quand il s'agit de partager une infrastructure commune entre l'IT et l'OT avec des objectifs différents voire opposés. De nouveau l'émergence du Cloud et des services d'infrastructure « IaaS » (Infrastructure as a Service), « PaaS » (Platform as a Service), « Saas » (Software as a Service) offrent la possibilité aux bâtiments de délocaliser leurs moyens numériques que ce soit pour l'IT ou l'OT. Là encore la cybersécurité alerte les esprits quant à la convergence de ces moyens informatiques. Reste également la limite associée à ce scénario d'hébergement avec les processus en temps réel portés par les régulateurs et automates avec des postes opérateurs au temps de réponse critique dans l'exploitation. Ainsi que les systèmes de sureté qui sont et resteront toujours au plus proche du terrain tant que les technologies et architectures informatiques ne proposeront pas d'alternatives convaincantes à ce sujet.

La convergence des moyens humains et organisationnelle

Les équipes en charge de l'IT, vont devoir

s'intéresser aux systèmes BACS: c'est la conséquence de la convergence des données et des moyens techniques qui conduit à cet état de fait. Les équipes en charge des systèmes BACS ont l'obligation de maintenir le bâtiment en état de bon fonctionnement pour les opérateurs du système, et in fine pour les usagers et les propriétaires.

Pour les constructeurs de la régulation et GTB (système BACS), l'enjeux est d'être conforme aux réglementations (UE, FR) pour jouer son rôle de contrôle-commande et monitoring : assurer le confort (de tout type), la santé et la productivité dans les bâtiments utilisant le minimum d'énergie possible et réduire l'empreinte carbone.
Cela permet d'atteindre l'efficacité énergétique des bâtiments de l'UE et FR, réduire l'empreinte carbone du bâtiment et lutter contre le changement climatique.

La convergence des moyens humains, devient une nécessité, et demandera de la compétence et des formations, et la bonne solution est la mise en place d'une équipe mixte IT/OT.

Il y a d'abord le sujet social, avec la rencontre et parfois la confrontation d'idées divergentes quant aux moyens mis en œuvre sur certains points, mais aussi sur les processus et technologies sans qu'aucune chronologie ni stratégie puissent être parfois véritablement établies. Notamment, la réglementation donne parfois très peu d'informations fiables en termes de contenu et de calendrier. L'attribution de nouvelles responsabilités ou des nouveaux périmètres, souvent plus grands, peut-être un frein à la collaboration IT/OT.

Tout ce qui a été mis en œuvre dans les environnements IT en matière de cybersécurité par exemple, n'est pas toujours applicable en l'état dans un contexte OT, et une politique Top Down pour imposer les moyens peut être sans résultat. Et imposer des architectures peut être inappropriées au monde OT !

La solution BACnet/SC a fait le choix d'utiliser un protocole d'échange des données venant du monde IT pour minimiser les risques des dysfonctionnements, très difficiles à résoudre.

Synthèse des défis et enjeux

Problématiques Organisationnelles

L'un des premiers défis majeurs de la convergence IT et OT réside dans les problèmes organisationnels. Les départements IT et OT ont souvent des cultures, des priorités et des langages différents. Les équipes IT sont axées sur la sécurité des données, la disponibilité des systèmes et l'innovation technologique, tandis que les équipes OT sont axées sur la fiabilité des processus, la sécurité des opérations et la continuité du bâtiment.
L'intégration de ces deux mondes nécessite une collaboration étroite entre les équipes. Les employés doivent également acquérir de nouvelles compétences pour comprendre et gérer les systèmes des deux côtés.

Défis de Gouvernance

La convergence IT et OT soulève également des questions de gouvernance complexes. Le management du projet doit décider de la manière dont vont être gérés et supervisés les systèmes combinés. Il faut avoir la réponse à la question : Comment garantir la conformité réglementaire dans les deux domaines si elle existe ?
Une gouvernance claire et bien définie est cruciale pour éviter les risques potentiels. Cela implique par exemple de mettre en place des comités de direction mixtes composés de représentants de l'IT et de l'OT, d'établir des politiques et des procédures de gestion des risques, et de définir des responsabilités claires pour chaque domaine. De plus, une communication transparente est essentielle pour maintenir une gouvernance efficace.

Enjeux de Cybersécurité

La sécurité est l'autre défi majeur de la convergence IT et OT. Ce n'est plus un secret, l'intégration des systèmes signifie que les menaces qui ciblent l'IT, telles que les cyberattaques, peuvent désormais potentiellement affecter les bâtiments critiques (exemple: un hôpital).

Pour atténuer ces risques, le management du projet doit mettre en place des stratégies de cybersécurité robustes qui couvrent à la fois l'IT et l'OT. Cela comprend la mise en œuvre de mesures techniques spécifiques (telles que par exemple des pares-feux, chiffrage, etc.), la surveillance constante des réseaux et la formation du personnel pour détecter et réagir aux menaces. De plus, la gestion des identités et des accès doit être rigoureusement contrôlée pour éviter les failles de sécurité.

Pour conclure

La convergence IT et OT offre de nombreuses opportunités pour améliorer l'efficacité opérationnelle, mais elle présente également des défis organisationnels, de gouvernance et de cybersécurité significatifs. Pour réussir dans ce nouvel environnement, les équipes projet doivent investir dans la collaboration inter services, établir une gouvernance solide et mettre en place des mesures de sécurité avancées. La convergence IT et OT est une étape importante et incontournable vers l'avenir, mais sa réussite dépendra de la manière dont les équipes projet abordent ces défis de manière proactive et réfléchie

La solution du Réseau et Protocole BACnet/SC, la version cyber sécurisée de BACnet, est appropriée pour faciliter cette convergence. Elle fait évoluer BACnet par conception pour la cybersécurité, tout en gardant les autres principes de développement et notamment la compatibilité ascendante. La migration d'une installation BACnet vers sa version BACnet/SC est possible pour sécuriser une installation dans un bâtiment existant !

Dan Napar
Président BACnet France | Membre Advisory Group BIG-EU
dan.napar.ext@siemens.com | DN Consulting

Fondamentaux et Prescriptions en vue du déploiement de BACnet/SC

Le nom de BACnet a été donné comme abréviation de Building Automation and Control Network. Comme son concepteur l'a voulu, MIKE NEWMANN, professeur d'automatisme à Cornell University US, les spécifications de BACnet sont les spécifications d'une vision « management » de réseau. Son sujet était (comme aujourd'hui) de pouvoir faire dialoguer (être interopérable) des systèmes BACS de vendeurs différents qui existaient dans les bâtiments du campus de Cornell et permettre une présentation des données unifiés pour le management global des bâtiments.

BACnet/SC (BACnet Secure Connect) est une extension moderne du protocole BACnet (Building Automation and Control Networks) conçue pour offrir une **communication sécurisée** entre les dispositifs d'automatisation du bâtiment, en particulier dans des environnements de plus en plus interconnectés.

BACnet est la norme mondiale de communication de données pour les réseaux d'automatisation et de contrôle des bâtiments. Elle fournit une solution de mise en réseau indépendante du fournisseur pour permettre l'interopérabilité entre les équipements et les dispositifs de contrôle pour une large gamme d'applications d'automatisation des bâtiments. BACnet permet l'interopérabilité en définissant des messages de communication, des formats et des règles pour l'échange de données, de commandes et d'informations d'état. BACnet fournit l'infrastructure de communication de données pour les bâtiments intelligents et est mis en œuvre dans des centaines de milliers de bâtiments à travers le monde.

L'utilisation de BACnet dans les systèmes BACS simplifie les opérations, réduit la formation, rationalise la maintenance, offre de la flexibilité et permet des extensions rétro-compatibles et des ajouts interfonctionnels.

La norme BACnet a été développée et est continuellement mise à jour par le Comité BACnet, plus officiellement connu sous le nom de SSPC 135 (un comité de projet des normes permanentes) de l'American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). Elle est ensuite adoptée par les comités techniques de normalisation ISO TC 205 (international) et CEN TC247 (européen). De ce fait, BACnet est une norme ISO (EN ISO 16484-5), une norme européenne (EN ISO 16484-5) et une norme nationale dans de nombreux pays. En France, la norme est connue avec la référence NF EN ISO 16484-5.

La communauté BACnet a choisi de faire une certification de conformité à la norme NF EN ISO 16484-6. La conformité avec la norme est connue sous le nom BTL.

BACnet Testing Laboratories (BTL) supervise le programme mondial de certification des produits BACnet et d'autres activités de test d'interopérabilité. Sur le site https://bacnetfrance.org , vous trouverez la liste des produits certifiés BACnet ainsi que des informations techniques et de la documentation relative aux tests et à la certification.

Une préoccupation majeure, qui concerne le monde du bâtiment, est la sécurité des réseaux et de l'information ainsi que l'intégrité de l'infrastructure. Avec un intérêt fortement croissant pour les applications basées sur le cloud, les propriétaires, les gestionnaires, les constructeurs des systèmes BACS et les professionnels de l'informatique ont une forte volonté de créer des infrastructures BACS qui offrent des niveaux de sécurité très élevés. Dans le même temps, du côté de l'informatique, il existe un ensemble mature de meilleures pratiques pour mettre en œuvre et gérer une infrastructure de communication sécurisée.

Reconnaissant ces préoccupations, la communauté BACnet a élaboré une proposition centrée sur les communications sécurisées en utilisant exclusivement les meilleures pratiques informatiques acceptées. La nouvelle technologie s'appelle « BACnet Secure Connect (BACnet/SC) ». **En termes simples, BACnet/SC fournit les moyens de créer des connexions de communication sécurisées entre les appareils BACS à la fois dans le cloud et au sein des installations. BACnet/SC utilise les dernières techniques de sécurité et s'intègre facilement à l'infrastructure informatique. Dans le même temps, BACnet/SC préserve 100% des capacités et est compatible avec tous les déploiements et appareils BACnet existants. Aligner BACnet/SC avec les normes et meilleures pratiques informatiques existantes permet dans le monde du bâtiment de créer une infrastructure BACS très sécurisée et de débloquer de nouvelles applications basées sur le cloud. Cela permettra également de pérenniser l'investissement des utilisateurs qui ont investi dans les BACS utilisant BACnet.**

BACnet Secure Connect (BACnet/SC) fournit une infrastructure BACS qui utilise le protocole Internet standard et des méthodes de sécurité standard largement utilisées, éliminant ainsi une grande partie des préoccupations et du travail pour un département informatique. Parce que BACnet/SC est capable de traverser l'ensemble du réseau, il fournit aux exploitants du ou des bâtiments un chemin sécurisé et efficace pour obtenir les données dont les utilisateurs ont besoin.

Pourquoi BACnet/SC est-il nécessaire ? En termes simples, il y a certains aspects des systèmes BACnet existants qui sont parfois problématiques parce qu'ils s'écartent des politiques et pratiques informatiques communes,

bien que celles-ci varient d'une situation à l'autre. Du point de vue informatique, BACnet/SC résout de nombreux problèmes courants :

- BACnet/SC fournit une solution de sécurité réseau sophistiquée qui utilise des normes largement acceptées par la communauté informatique.
- BACnet/SC élimine le besoin d'adresses IP statiques, ce qui réduit la charge de travail des groupes informatiques et peut réduire les coûts de location pour les utilisateurs.
- BACnet/SC ne dépend pas de la messagerie de diffusion réseau.
- BACnet/SC élimine les dispositifs de gestion de diffusion BACnet/IP (BBMDs) et leur configuration et est tolérant aux changements dans la topologie du réseau.
- BACnet/SC fonctionne facilement avec les dispositifs de pare-feu qui sont courants dans l'infrastructure informatique.

Descriptif de BACnet/SC

BACnet/SC est une nouvelle liaison de données BACnet qui élimine bon nombre des préoccupations que les propriétaires, les gestionnaires d'installations et les professionnels de l'informatique ont avec BACnet aujourd'hui. Il est basé sur la sécurité standard TLS 1.3 (TLS = Transport Layer Security) avec des options pour la cryptographie de courbe elliptique de 128 bits et 256 bits. Cela élimine le besoin d'adresses IP statiques et de diffusions réseau. Il simplifie la configuration en éliminant les périphériques BBMD ainsi que la nécessité de les garder configurés pour correspondre à la topologie du réseau.

La proposition BACnet/SC va au-delà de ces fonctionnalités clés pour prendre en charge d'autres capacités, notamment :

- Utilisation de réseaux IP partagés sans configuration de réseau privé virtuel (VPN) requise
- Permettre une traversée transparente des configurations de réseau IP simple à complexe et local à mondial sans compromettre les mécanismes de sécurité existants, tels que les pares-feux
- Fournit un transport sécurisé des messages à l'aide du protocole d'application IP standard, Secure WebSockets, qui est une extension de HTTPS et s'exécute sur Transport Layer Security (TLS)
- Permettre des communications indépendantes de la configuration du réseau, y compris IPv4, IPv6, WiFi et cellulaire
- Compatibilité totale avec tous les systèmes et appareils BACnet existants grâce au routage BACnet normal
- BACnet/SC fournit un mécanisme sécurisé pour permettre à un appareil d'être authentifié et autorisé à utiliser le réseau.

Topologie BACnet/SC

BACnet/SC utilise une topologie en étoile où une seule fonctionnalité de hub central dirige le trafic entre un nombre quelconque de nœuds connectés. Le hub analyse le trafic pour déterminer s'il doit être dirigé vers un autre nœud ou transmis à tous les nœuds connectés.

REMARQUE : Il y a UN SEUL HUB par installation BACnet/SC ! Il peut être mis en redondance et en cas de défaillance du HUB principal, le transfert vers le HUB redondant se fait automatiquement. Parce qu'un hub est un point de défaillance unique, les nœuds BACnet/SC prennent en charge un mécanisme de basculement pour garantir que le système reste viable si le hub échoue ou est mis hors ligne pour maintenance ou mise à niveau. Tous les nœuds BACnet/SC sont mandatés pour prendre en charge la connexion au hub de basculement BACnet/SC si le hub principal ne peut pas être connecté.

Un nœud peut être un dispositif simple, ou un dispositif plus sophistiqué qui se connecte à un système BACnet existant, ou il pourrait être le poste de travail principal pour l'ensemble de l'installation. BACnet/SC définit une fonction de hub BACnet/SC dédiée et simple, mais est conçu pour permettre des extensions futures.

Dan Napar
Président BACnet France | Membre Advisory Group BIG-EU
dan.napar.ext@siemens.com | DN Consulting

La filière BACS au service de la performance énergétique et environnementale des bâtiments

Comme nos lecteurs le savent, les produits et systèmes d'automatisation et de contrôle du bâtiment font l'objet d'exigences réglementaires ambitieuses en France depuis quelques années.

Désormais appelées communément par les acteurs de marché sous l'acronyme « BACS » (pour Building Automation and Control Systems, traduction anglaise selon la Directive Européenne sur la Performance Energétique des Bâtiments), ces technologies robustes et évolutives sont installées progressivement dans les bâtiments tertiaires assujettis aux Décret BACS I et II.

En effet, depuis le 1er janvier 2025, ce sont les bâtiments à usage tertiaire avec des systèmes de chauffage, ventilation et climatisation (CVC), combinés ou non, d'une puissance supérieure à 290kW qui doivent être équipés de BACS performants (cf exigence du Décret BACS I, référencé « Décret n° 2020-887 du 20 juillet 2020 relatif au système d'automatisation et de contrôle des bâtiments non résidentiels et à la régulation automatique de la chaleur »). Et au 1er janvier 2027, le seuil est abaissé à 70kW conformément aux objectifs du Décret BACS II (référencé « Décret n° 2023-259 du 7 avril 2023 relatif aux systèmes d'automatisation et de contrôle des bâtiments tertiaires »). Dans ces bâtiments, les BACS requis par la réglementation doivent être de classe C selon la norme NF EN ISO 52120-1 :2022.

Pour faire simple, il s'agit d'installer des dispositifs de régulation sur l'ensemble des équipements pour les usages énergétiques réglementaires (chauffage, refroidissement, eau chaude sanitaire, ventilation et éclairage) et de les associer à un système de gestion technique du bâtiment (GTB, ou supervision). Condition technique nécessaire pour garantir l'interopérabilité, il est recommandé de mettre en œuvre de tels BACS avec les protocoles de communication standardisés ouverts multi-usages comme KNX ou BACnet.

Ces exigences de moyens ont notamment pour objectif de faciliter l'atteinte des exigences de résultats du Dispositif Eco-énergie Tertiaire, soit une consommation énergétique réelle des bâtiments tertiaires de plus de 1000m² réduite de 40% en 2030 (puis 50% en 2040 et 60% en 2050) par rapport à l'année de référence déterminée par les propriétaires assujettis lors de leur déclaration sur la plateforme OPERAT. A mesure que cette dernière sera complétée, celle-ci devrait d'ailleurs devenir un outil efficace de suivi du taux d'installation des BACS en France.

Dans ce contexte réglementaire exigeant, les acteurs du marché sont pleinement mobilisés pour déployer massivement les technologies BACS les plus performantes et avec le meilleur ratio d'efficacité technico-économique.

On notera d'ailleurs que celles-ci correspondent le plus souvent à des solutions avec un poids carbone intrinsèque négligeable et qui, en même temps, contribuent significativement à améliorer la performance environnementale d'un bâtiment sur l'ensemble de son cycle de vie en réduisant le poids de la consommation énergétique.

Pour la filière, il s'agit donc essentiellement de se structurer autour d'une compréhension commune des documents de références et des bonnes pratiques en vigueur depuis de nombreuses années. Les industriels fabricants de BACS conçoivent des produits, systèmes et services performants qui ont fait leur preuve, grâce aux forts investissements en Recherche et Développement suivant une logique de standardisation indispensable pour diffuser les innovations sur le plus large territoire possible en réalisant des économies d'échelles. Ces solutions sont souvent bien connues par la filière traditionnelle, de la maitrise d'ouvrage à l'exploitation en passant par les intégrateurs. Néanmoins, l'ampleur du déploiement nécessaire pour répondre aux objectifs réglementaires est telle, qu'un nombre croissant de nouveaux acteurs, issues de l'offre et de la demande, sont désormais actifs avec parfois une compréhension moins avisée de ces solutions.

Ainsi, dès Mars 2023, les partenaires historiques que sont les industriels du Syndicat des Automatiques, du génie Climatique et de la Régulation (ACR) et les membres des Associations de protocoles standardisés réunis au sein de BACnet France et KNX France, ont contribué à créer l'ALLIANCE BACS pour fédérer l'ensemble de la filière et la renforcer. Collectivement, il s'agit d'assurer un déploiement massif des BACS pour atteindre les objectifs réglementaires, en France puis en Europe, en évitant les contre-références majeures qui pourraient advenir d'une mauvaise maitrise des solutions à prescrire, de leur mise en œuvre et de leur exploitation.

Réunissant aussi bien les industriels que des acteurs issus de la maitrise d'ouvrage, de la maitrise d'œuvre que des exploitants ou bureaux de contrôles, son nombre croissant de membres confirme la volonté des acteurs les plus engagés à travailler ensemble pour réussir le défi de la

massification des BACS.

Les travaux et actions de l'ALLIANCE BACS consistent à la fois à faire connaitre les documents de références et bonnes pratiques en vigueur, notamment à travers des webinaires publics, que de continuer à travailler collégialement entre acteurs privés et avec les pouvoirs publics sur de nouveaux documents de références au sein de groupe de travail ciblés.

Sur ce modèle, l'ALLIANCE BACS a notamment contribué à la rédaction d'une FAQ publiée le 13 juin 2025 sur le site du ministère (https://rt-re-batiment.developpement-durable.gouv.fr/faq-decret-bacs-r463.html) ayant pour objectif de préciser les exigences réglementaires du Décret BACS. Ce travail collectif a d'ailleurs été présenté lors d'un nouveau webinaire organisé par l'ALLIANCE BACS le 10 juillet 2025 en présence de représentants des pouvoirs publics en charge (i.e. la Direction de l'Habitat de l'Urbanisme et du Patrimoine, DHUP) et des autres contributeurs : AGILE (maitrise d'ouvrage publique) et FILIANCE (groupement des organismes de contrôles agrées) avec le soutien de l'AFNOR.

Cet évènement a permis aux pouvoirs publics de faire un rappel des grands enjeux relatifs au respect des engagements climatiques, avec le contexte européen de transposition de la nouvelle Directive EPBD IV publiée en 2024, le cadre réglementaire français, et les besoins d'accompagnement de la filière, par exemple sur les enjeux d'accompagnements pour l'assujettissement.

Ce fut bien sur aussi l'occasion de faire un rappel des généralités et définition des BACS, l'utilisation de la norme NF EN ISO 52120-1 :2022 comme référentiel technique pour une approche pragmatique permettant de qualifier et quantifier la contribution des BACS à la performance énergétique des bâtiments sur la base d'un consensus européen et international. Le rôle d'exemplarité de la maitrise d'ouvrage publique a également été portée pour faciliter la diffusion des meilleurs pratiques, en particulier pour l'application concrète des exigences réglementaires au travers des appels d'offres à venir.

Enfin, les organismes de contrôles ont pu en particulier revenir sur les logiques d'évaluation du taux de retour sur investissement pour déterminer les assujettissements, et anticiper les exigences relatives aux inspections réglementaires (2 ans après installation puis tous les 5 ans), une des nouveautés importantes issues du Décret BACS II.

Nous invitons vivement nos lecteurs à prendre connaissance de cette FAQ pour les guider dans la compréhension commune des exigences réglementaires. Concernant la mise en œuvre de BACS performants et évolutifs, ces travaux ont permis une fois de plus de confirmer le rôle essentiel des protocoles de communication standardisés comme BACnet et KNX pour permettre une gestion en fonction de la demande réelle, l'interopérabilité à tous les étages d'un BACS, et préserver les investissements des propriétaires.

En outre, il faut ajouter que le recours aux protocoles de communication standardisés ouverts est d'autant plus pertinent aujourd'hui qu'il permet non seulement de planifier une montée en puissances des BACS (de la classe C à la classe B ou A, voire plus), mais aussi d'anticiper les exigences réglementaires à venir relatives à la cybersécurité des installations grâce aux récentes évolutions dans le domaine supportés par BACnet/SC et KNX/Secure (cf articles sur le sujet de la cybersécurité dans ce numéro par le président de l'Association BACnet France, Dan NAPAR).

Nous vous encourageons donc vivement à rejoindre les structures susmentionnées pour participer activement au déploiement harmonieux de ces technologies et contribuer à construire et rénover des bâtiments performants, évolutifs et sécurisés.

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

HTTPS sécurisé offre une sécurité renforcée dans un système de gestion de bâtiment

Les appareils conformes à BACnet qui intègrent HTTPS offrent une communication web cryptée et protègent l'intégrité des données des clients.
© Contemporary Controls

La sécurité réseau est plus critique que jamais dans les systèmes de gestion de bâtiment (BMS) d'aujourd'hui pour garantir l'authentification, l'intégrité et la confidentialité des données transférées sur Internet. Cet article décrit comment les dispositifs conformes à BACnet qui intègrent HTTPS offrent une communication chiffrée et protègent l'intégrité des données des clients. Cet article décrit également la méthode d'authentification et de chiffrement HTTPS qui utilise des clés et des certificats numériques. Il compare les certificats générés par une autorité de certification (AC) aux certificats auto-signés et fournit une ressource pour créer votre propre certificat auto-signé.

BACnet reste le protocole le plus populaire utilisé dans les systèmes de contrôle HVACR et il existe un écosystème robuste de dispositifs qui composent ces systèmes, y compris des passerelles pour intégrer d'autres protocoles, tels que Modbus et EnOcean, à BACnet. À mesure que de plus en plus de dispositifs sont utilisés pour répondre aux exigences des systèmes de gestion des bâtiments (BMS) et des infrastructures de bâtiments intelligents, la sécurité des réseaux est plus critique que jamais pour assurer l'authentification, l'intégrité et la confidentialité des données transférées sur Internet.

Les dispositifs BACnet-complaint qui intègrent HTTPS (HTTP sécurisé) offrent une communication chiffrée et protègent l'intégrité des données des clients. Les serveurs web HTTPS résidentiels permettent la mise en service, le rapport de statut et le dépannage de manière sécurisée en utilisant n'importe quel navigateur web standard, améliorant ainsi le contrôle d'accès aux dispositifs.

HTTPS (HTTP sécurisé) utilise le chiffrement pour une communication sécurisée sur un réseau IP. Le trafic HTTPS est chiffré à l'aide de la sécurité des transmissions (TLS), anciennement connue sous le nom de couche de sockets sécurisée (SSL). Le protocole est toujours désigné sous le nom de HTTP sur SSL, généralement affiché sous la forme https:// dans la barre d'adresse du navigateur.

Certificats numériques

SSL/TLS repose sur l'utilisation de clés et de certificats numériques pour le chiffrement des données, l'authentification des appareils et l'intégrité des données. Les clés existent en paires (publique/privée) et sont utilisées pour le chiffrement/déchiffrement. Une clé publique est utilisée pour le chiffrement, tandis que la clé privée est utilisée pour le déchiffrement.

Les certificats numériques sont utilisés pour l'authentification et le chiffrement, vérifiant la propriété et l'authenticité pour garantir que seuls les appareils autorisés communiquent entre eux. La clé publique fait partie du certificat, tandis que la clé privée est secrète pour l'appareil. Des mécanismes existent pour générer des certificats et des clés pour un appareil et pour étendre l'architecture à plusieurs appareils.

Digital Certificates – Certificate Authority

Les certificats sont généralement délivrés et gérés par une entreprise tierce de confiance, appelée Autorité de Certification (AC). L'installation d'un certificat SSL pour un site web par une AC bien connue, qui est de confiance par tous les appareils et navigateurs, tels que DigiCert, Comodo, GoDaddy, Lets Encrypt, peut permettre un accès au site web de manière transparente sur Internet public. L'appareil peut obtenir le certificat directement auprès de l'AC ou envoyer une Demande de Signature de Certificat (CSR) à l'AC pour obtenir le certificat correspondant. Ces AC de confiance ne délivrent des certificats qu'aux sites web ou appareils ayant une adresse IP publique. Ils ne fourniront pas de certificats pour les appareils sur un réseau interne avec des adresses IP privées.

Certificats numériques – Infrastructure à clé publique

Pour un réseau BMS interne, obtenir un certificat d'une autorité de certification publique n'est pas nécessaire et peut être coûteux compte tenu du nombre considérable de dispositifs dans un bâtiment. Le département informatique peut mettre en œuvre sa propre infrastructure pour générer ces clés et certificats. Le terme PKI (Infrastructure à Clé Publique) est utilisé pour définir cette configuration. Les fournisseurs de produits d'automatisation de bâtiment peuvent également disposer d'outils logiciels spécifiques pour mettre en œuvre la PKI, mais les certificats et clés de tous les dispositifs d'un site, quelle que soit leur marque, doivent être générés à partir du

même outil pour garantir l'interopérabilité. Les certificats sur les dispositifs expirent également et doivent être renouvelés.

Les appareils utilisés sur les réseaux internes peuvent également utiliser un certificat numérique auto-signé pour faire en sorte qu'un navigateur Web fasse confiance à vos appareils internes. Un certificat auto-signé est un type de credential SSL/TLS que vous signez vous-même plutôt que de le faire signer par une autorité de certification (CA) tierce de confiance. Si vous n'avez pas de service informatique, vous pouvez générer le certificat auto-signé vous-même. De plus, générer un certificat auto-signé pour les appareils du réseau interne élimine le coût associé à l'obtention d'un certificat d'une CA tierce de confiance.

Certificats numériques – Auto-signés

Les certificats numériques auto-signés sont créés en signant le certificat avec la clé privée du propriétaire. Ils sont créés, publiés et signés par l'entreprise ou le développeur responsable du site Web / logiciel étant signé. Contrairement aux certificats émis par une autorité de certification de confiance, aucune partie externe ne vérifie un certificat auto-signé. Les certificats auto-signés sont rapides, gratuits et faciles à émettre. Ils sont appropriés pour le développement local, les tests ou les environnements de pré-production, les sites Web d'un réseau interne et la fourniture de pages Web sécurisées pour les appareils. Cependant, vous devez être conscient de leurs limitations, car malgré le chiffrement fort qu'ils offrent, ils manquent du soutien d'une autorité reconnue, et les navigateurs sur différents PC afficheront des avertissements de sécurité à leur sujet.

Certificats numériques – OpenSSL

Vous pouvez générer et installer un certificat auto-signé en utilisant OpenSSL, un utilitaire en ligne de commande couramment utilisé pour générer des clés, créer des demandes de signature de certificat (CSR) et gérer des certificats.

Selon la documentation d'OpenSSL sur https://docs.openssl.org/master/man7/ossl-guide-introduction/ *"OpenSSL est un ensemble d'outils robuste, de qualité commerciale et complet pour la cryptographie générale et la communication sécurisée. Ses fonctionnalités sont mises à disposition via une application en ligne de commande qui permet aux utilisateurs d'effectuer diverses fonctions liées à la cryptographie, telles que la génération de clés et de certificats. De plus, il fournit deux bibliothèques que les développeurs d'applications peuvent utiliser pour mettre en œuvre des capacités basées sur la cryptographie et communiquer de manière sécurisée sur un réseau. Enfin, il dispose également d'un ensemble de fournisseurs qui proposent des implémentations d'un large éventail d'algorithmes cryptographiques.*

OpenSSL est entièrement open source. La version 3.0 et supérieure est distribuée sous la licence Apache v2."

Si vous n'avez pas OpenSSL sur votre PC Windows, vous pouvez installer un paquet OpenSSL. Si vous accédez à l'appareil HTTPS depuis un autre PC, un message d'avertissement de sécurité apparaîtra. Vous devez télécharger le certificat auto-signé et l'installer dans le magasin de certificats de confiance de votre machine locale.

Pour plus d'informations, Contemporary Controls a créé une Note d'Application: Comment créer et utiliser des certificats SSL auto-signés qui explique comment ajouter OpenSSL et créer un certificat auto-signé pour Windows en utilisant le gestionnaire de paquets Windows, WinGet. WinGet est un gestionnaire de paquets gratuit et open-source conçu par Microsoft qui permet aux utilisateurs de découvrir, installer, mettre à jour, supprimer et configurer des applications sur des ordinateurs Windows 10, Windows 11 et Windows Server 2025. La note d'application explique également comment installer ce certificat auto-signé sur l'appareil, et comment télécharger et installer le certificat auto-signé sur différentes machines Windows pour éliminer l'avertissement de sécurité. Des instructions sont fournies pour les navigateurs couramment utilisés : Google Chrome, Microsoft Edge et Mozilla Firefox, et comment surmonter le message d'Avertissement de Sécurité.

Conclusion

HTTPS chiffre le transport des données pour garantir l'intégrité des données et empêche que les informations soient modifiées, corrompues ou volées lors de la transmission. Les protocoles SSL/TLS authentifient les utilisateurs pour sécuriser les informations et s'assurer qu'elles

Les certificats numériques vérifient la propriété et l'authenticité pour garantir que la communication se déroule avec des dispositifs autorisés.
© Creative Commons

ne seront pas révélées à des utilisateurs non autorisés. HTTPS nécessite des certificats numériques pour valider la propriété du domaine et son intégrité. Pour les réseaux externes, vous devez obtenir cette attestation d'une Autorité de Certification (CA) tierce de confiance.

Les certificats auto-signés sont précieux pour créer des canaux de communication sécurisés pour les réseaux internes lorsque vous contrôlez l'environnement. Ils offrent un déploiement rapide et des économies de coûts, et sont idéaux pour les tests, le développement local ou les applications internes. Comprendre ces concepts est essentiel pour mettre en œuvre une sécurité pour les dispositifs IP en général. Pour le monde de l'automatisation des bâtiments basé sur BACnet, ils fournissent les connaissances fondamentales pour une mise en œuvre réussie et robuste de BACnet/SC.

A PROPOS DE L'AUTEUR

Harpartap Parmar est Directeur Produits chez Contemporary Controls, qui conçoit et fabrique des contrôleurs de locaux technique BACnet et des équipements de mise en réseau. Parmar se concentre sur la sécurité du réseau, les routeurs IP et leur application à l'automatisation des bâtiments. Il a plus de 22 ans d'expérience chez Contemporary Controls avec une gamme de produits de mise en réseau, de contrôle et de communication.

CONTEMPORARY CONTROLS

Harpartap Parmar
Directeur Produits | Contemporary Controls
hparmar@ccontrols.com | www.ccontrols.com

Les aspects de sécurité gagnent en importance

Communication de données sécurisée et cryptée dans les infrastructures critiques de l'automatisation des bâtiments. Sources des images : @ METZ CONNECT

Le nouveau routeur BACnet/SC BMT-(F)-RTR/SC représente une solution idéale pour la transmission sécurisée et cryptée des données dans le domaine de l'automatisation des bâtiments, en particulier dans les infrastructures critiques. BACnet/SC définit la norme pour la transmission sécurisée des données au moyen du protocole BACnet et permet d'utiliser les infrastructures informatiques existantes ainsi que l'internet à cette fin. La capacité du routeur à étendre de manière transparente le routage de MS/TP vers BACnet/IP à BACnet/SC est particulièrement avantageuse.

Metz Connect propose des routeurs BACnet/IP qui prennent en charge le raccordement de 32 appareils BACnet MS/TP par ligne. Cela permet une communication fiable et rapide entre les appareils. Metz Connect a maintenant encore plus développé son routeur : le « BMT- (F)-RTR/SC ». Ce routeur BACnet/SC (SC signifie Secure-Connect) apporte une solide contribution à la communication sécurisée et cryptée dans les réseaux BACnet.

Sécurité accrue contre les cyber-attaques

En raison de l'augmentation de la mise en réseau informatique dans les bâtiments et de la connexion des systèmes de gestion des bâtiments au cloud, il existe un risque croissant de piratage des installations des bâtiments. L'accès à des données sensibles peut causer des dommages importants au bâtiment ou aux installations.

BACnet offre en principe quelques mécanismes de sécurité à cet effet. BACnet/SC est une extension du protocole BACnet qui vise spécifiquement à améliorer la sécurité dans les réseaux d'automatisation des bâtiments. BACnet/SC définit une nouvelle norme pour la transmission sécurisée des données au moyen du protocole BACnet et permet une utilisation en toute sécurité les infrastructures informatiques existantes ainsi que de l'Internet.

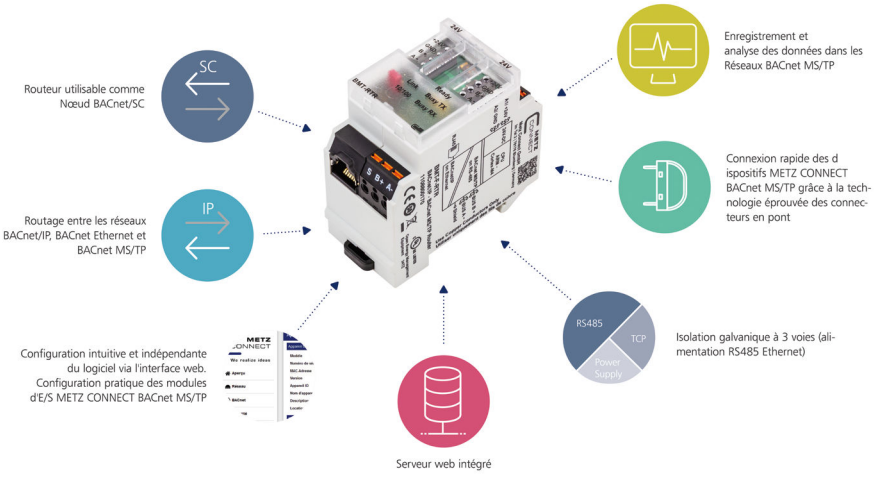
Appareils BACnet/SC pour la transmission cryptée des données

Le protocole BACnet/SC a été développé pour mieux protéger les systèmes d'automatisation des bâtiments en réseau contre les cybermenaces et les accès non autorisés. Il offre des fonctions de sécurité avancées telles que des méthodes d'authentification avancées et l'utilisation de certificats numériques. BACnet/SC crypte l'ensemble du trafic de données afin de garantir la confidentialité et d'empêcher les attaques.

Le protocole vérifie également l'intégrité des données transmises afin de s'assurer qu'elles n'aient pas été manipulées pendant la transmission. Cela permet de garantir que les données reçues soient correctes et non modifiées. En outre, BACnet/SC met en œuvre des mécanismes de prévention contre des attaques répétées, par lesquelles un attaquant tente de réutiliser des messages déjà envoyés pour manipuler le réseau.

Routage de BACnet/IP et BACnet MS/TP vers BACnet/SC

La flexibilité du routeur mérite d'être soulignée: il connecte de manière transparente les appareils BACnet MS/TP aux réseaux BACnet/IP et BACnet/SC. Cela simplifie et sécurise la communication sur de longues distances, y compris la connexion à des applications en nuage. Un accès à distance sécurisé et donc la maintenance à distance des installations est possible. Les appareils BACnet MS/TP correctement raccordés au routeur sont affichés dans le serveur web avec l'adresse d'appareil réglée.



Caractéristiques de performance. Sources des images : @ METZ CONNECT

Pascal Porté
Metz Connect France SAS | Directeur des ventes France
pascal.porte@metz-connect.com | www.metz-connect.com

Rénovation du groupe scolaire Petit Val a Sucy en Brie (94)

Un établissement historique face aux défis énergétiques modernes

Petit Val, établissement catholique privé d'enseignement est situé dans un cadre exceptionnel et historique à Sucy en Brie (94). L'établissement reçoit 1500 élèves répartis sur 3 unités : école maternelle et primaire, collège et lycée d'enseignement général.

Avec une superficie chauffée supérieure à 10 000 m², le groupe scolaire doit répondre aux exigences réglementaires du décret tertiaire et du décret BACS.

Un objectif ambitieux a été fixé : diminuer drastiquement ses consommations énergétiques de 40% d'ici 2030 et disposer au minimum d'une GTB de classe C (selon l'ISO 52120-1).

Rénovation du groupe scolaire Petit Val (94)

Mise en conformité des installations Une approche pragmatique basée sur un plan de comptage rigoureux

Le groupe scolaire a lancé un appel d'offre en 2024 pour rénover en profondeur ses installations tout en assurant la continuité des cours – un véritable défi ! L'entreprise ENEZEN s'est appuyée sur les technologies Siemens pour moderniser les bâtiments en collaboration très étroite avec le responsable technique du site.

Les plans d'actions et leviers pour répondre au décret tertiaire ont très vite été identifiés : reprise d'équipements de télérelève des consommations, suivi et management des consommations, mise en place d'une supervision Siemens Desigo CC et établissement d'un contrat de maintenance associé pour assurer un suivi et un management efficace des consommations.

L'étape suivante a consisté à déployer des équipements adaptés et un dispositif de pilotage efficace, ouvert et interopérable, remontant sur une supervision multisite pour offrir une vision holistique de l'ensemble des bâtiments.

Les premiers postes de réduction des consommations ont très vite pu être identifiés : le chauffage et la ventilation.

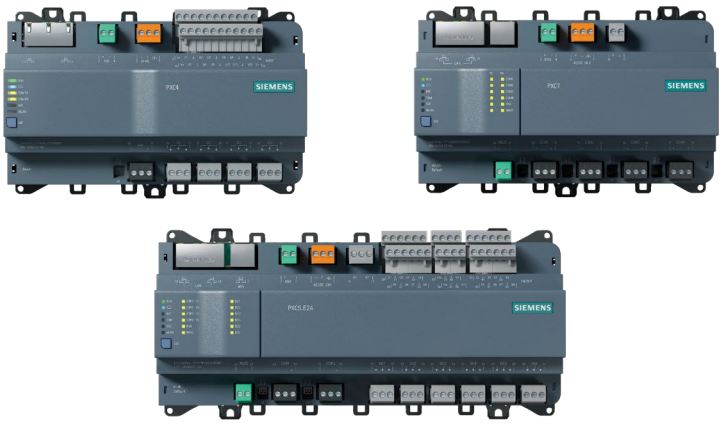
Le protocole BACNET comme élément de réponse au décret BACS : une technologie pérenne pour fédérer et piloter ses installations

Les équipements de production de chaleur existants (automates Synco KNX) ont été remontés en BACnet IP sur la supervision au travers d'un automate PXC pour la gestion des 2 chaudières alimentant un réseau de radiateurs. En complément, une régulation terminale intelligente pièce par pièce a été installée pour gérer les appareils à détente directe produisant le chaud et le froid dans les salles de classe. Cette réversibilité garantit aux élèves un confort optimal toute l'année rendant l'apprentissage plus efficace.

Des sondes de qualité d'air ont également été installées à chaque étage du bâtiment (CO_2, température et humidité relative) afin de mesurer le niveau de confort du site.

La ventilation a fait l'objet d'une étude approfondie, notamment sur le bâtiment équipé de centrales de traitement d'air alimentant le réfectoire, la hotte de compensation et le CDI (Centre de Documentation et d'Information).

Les résultats sont impressionnants : dès le premier semestre suivant la rentrée scolaire, 19% d'économies d'énergie ont été réalisés, se traduisant par une réduction de l'empreinte carbone (CO_2) de 35% !



Automates Desigo PXC

Le protocole BACnet comme faire-valoir des économies d'énergie : petit Val, plus qu'une installation GTB, un véritable projet éducatif !

Antoine Sajoux, directeur d'ENEZEN a su proposer une GTB adaptée aux besoins de son client. « L'application cloud Siemens Energy Manager permet de situer l'efficacité énergétique du bâtiment par rapport à des valeurs de référence. Le système détecte les pertes d'efficacité des systèmes techniques et informe l'exploitant des possibilités d'amélioration ».

Fort de ces excellents résultats, les acteurs du projet et le corps enseignant ont décidé d'aller plus loin en développant un projet éducatif axé sur le développement durable. Cette initiative met en avant les gains réalisés grâce aux automatismes du bâtiment tout en sensibilisant les plus jeunes à l'importance et des bonnes pratiques environnementales.

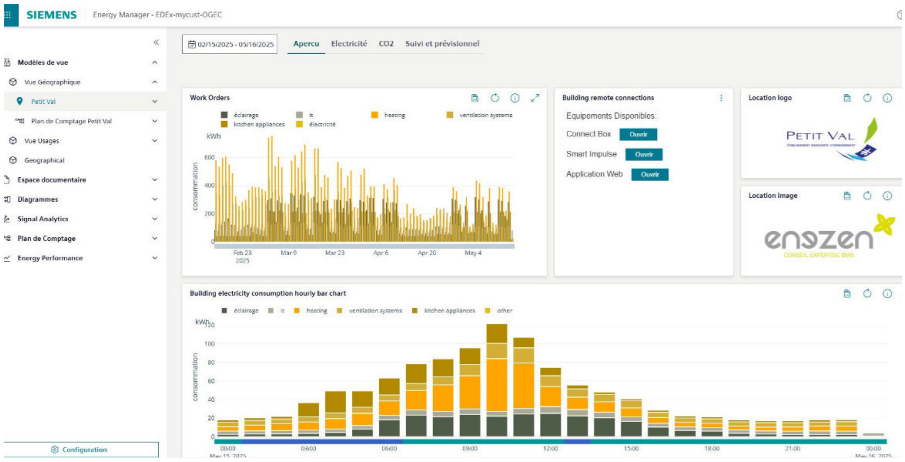
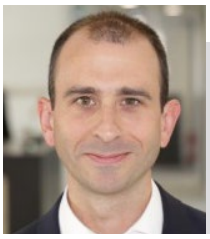


Tableau de bord : application Siemens Energy Manager intégrée par ENEZEN



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

Pourquoi faire remonter les informations BACnet jusqu'au jumeau numérique ?

Bâtiment ESTP-ESEO inauguré en 2022 et faisant partie des premières réalisations de France labellisées Ready 2 Services ***

Le campus ESTP-ESEO abrite depuis septembre 2022 deux écoles d'ingénieurs (Ecole Spéciale des Travaux Publics et Ecole Supérieure d'Electronique de l'Ouest) à DIJON. Ce bâtiment, sur 10 000 m² et sur 5 niveaux, est équipé de 44 salles d'enseignements, de 8 laboratoires de recherche et d'un amphithéâtre flexible de 400 places. Il a été construit par la SPLAAD (Société Publique Locale Aménagement de l'Agglomération Dijonnaise) pour le compte de Dijon Métropole et de la région Bourgogne-Franche-Comté.

Cet immeuble sert de laboratoire d'études, vivant et à grandeur réelle, pour les étudiants et les chercheurs dans le domaine du BIM et du smart building : les données du bâtiment sont remontées au jumeau numérique via un BOS (Building Operating System).

Que faire de toutes les data générées ? Comment donner de la valeur à celles-ci ?

Structure du système d'information du bâtiment

Les données brutes du bâtiment (issues des capteurs, actionneurs, compteurs, automates…) sont mises à disposition des différents systèmes et applications grâce au BOS Linksper (Vayandata).

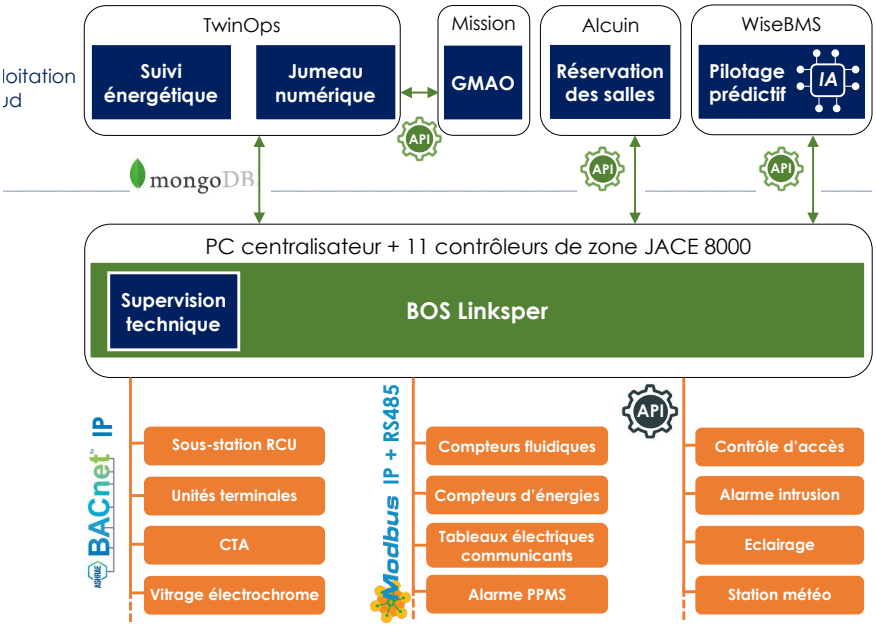
Au moment de la conception, l'objectif a été de limiter le nombre de protocoles de communication pour éviter les passerelles (sources de problèmes de traduction) tout en favorisant ceux qui sont standardisés, ouverts et interopérables.

La majorité des informations du bâtiment est véhiculée via le réseau IP (BACnet IP, Modbus TCP/IP, API, base de données mongoDB).

Le campus ESTP-ESEO a obtenu le label R2S***, socle de base du smart building garantissant les plus hautes conditions de connectivité, d'accès et de sécurité pour la transmission de ses données numériques. Ainsi, les moyens techniques sont mis en œuvre pour une architecture de communication IP performante et durable afin de mettre le numérique au service du bâtiment et de ses occupants.

BOS Linksper, cœur du système d'information

Le BOS (Building Operating System) est l'unique point de partage des données du bâtiment en permettant de partager des données contextualisées et fiables entre les différents acteurs techniques (systèmes



Architecture partielle du système d'information du bâtiment ESTP-ESEO de DIJON

Fonctions assurées par le BOS (Building Operating System) pour agréger les produits, services et données en optimisant les flux d'information

énergétiques, systèmes de sécurité des biens et des personnes, supervision technique locale, applications cloud).

Il fait le lien entre le bâtiment ESTP-ESEO réel, son jumeau numérique et les services tiers via un système de gestion de base de données mongoDB avec la plateforme cloud Twinops ou via des API (Application Programming Interface) : une interface de programmation d'application 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.

Le BOS permet de plus des interactions entre les différents systèmes techniques.

Sa fonction dans le smart building n'est pas uniquement d'être une passerelle de communication, elle permet aussi une réelle exploitation des données par la richesse des informations qu'elle apporte et par sa gestion des priorités de commande.
Une valeur a de l'importance si elle est contextualisée et priorisée !

La contextualisation des données (bâtiment, étage, local, grandeur physique de la valeur transmise, équipement à l'origine de la donnée…) est indispensable pour donner de l'importance à une valeur et pour une hypervision structurée. L'intégration et la contextualisation d'un point BACnet décrit de manière rigoureuse et lisible est plus facile par rapport à une communication Modbus qui nécessite notamment l'exploitation de tables d'échange.

Hypervision TwinOps, outil d'exploitation du bâtiment

L'hypervision Twinops (Vinci) héberge le jumeau numérique du bâtiment ESTP-ESEO et assure son suivi énergétique. Celle-ci permet une centralisation des données de l'activité actuelle et passée du bâtiment ainsi que de sa base documentaire (DOE, suivi des travaux de maintenance…).

Le jumeau numérique (avec sa maquette 3D GEM – Gestion Exploitation Maintenance) est épuré à partir de plusieurs maquettes BIM de conception (architecte, structure, CVC, CFO, CFA…) dans l'optique de la gestion des données.

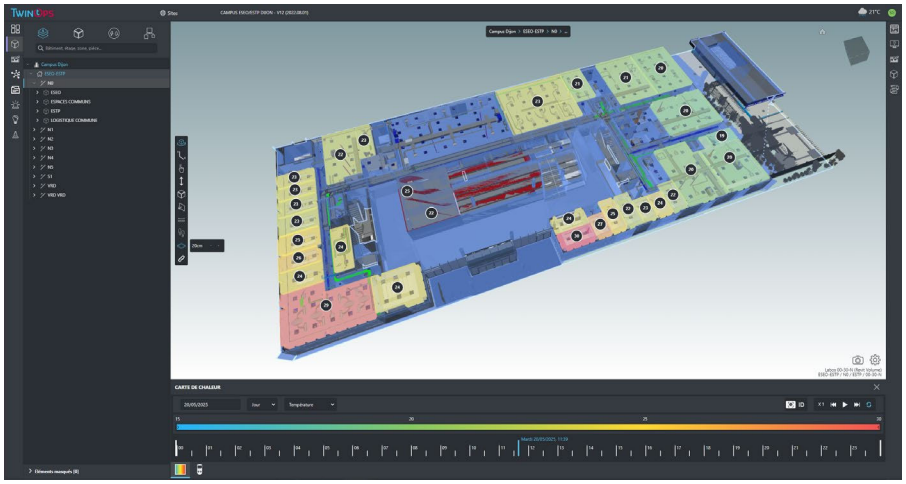
C'est un élément d'exploitation important du smart building grâce à la géolocalisation des équipements, à la visualisation dynamique et graphique des valeurs mesurées et échangées via le BOS.

Supervision technique locale vs Hypervision TwinOps

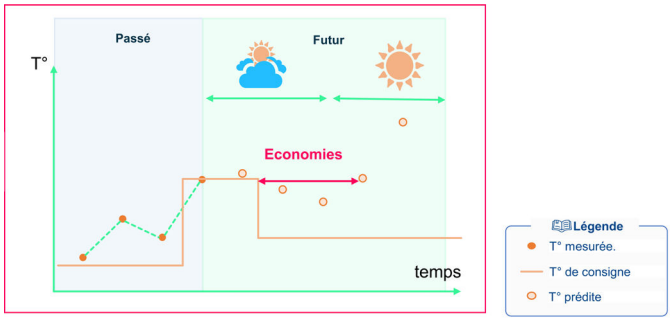
La gestion technique du bâtiment peut être réalisée depuis une supervision technique locale incluse dans le BOS Linksper (principalement via le PC centralisateur) ou avec la plateforme cloud TwinOps. En fait, ces deux solutions se complètent avec des spécificités pour chacune d'entre-elles.

Twinops donne un accès à l'ensemble des données remontées depuis le bâtiment via le BOS (90% des datas, 22000 points) ainsi qu'à la base documentaire du site. Le jumeau numérique y fournit un avatar du bâtiment ESTP-ESEO avec un environnement complet qui n'est pas forcément adapté à l'usage désiré de la GTB à réaliser. Cet environnement, puissant, est particulièrement adapté pour la surveillance, la supervision et l'analyse de l'efficacité énergétique au niveau technicien expert.

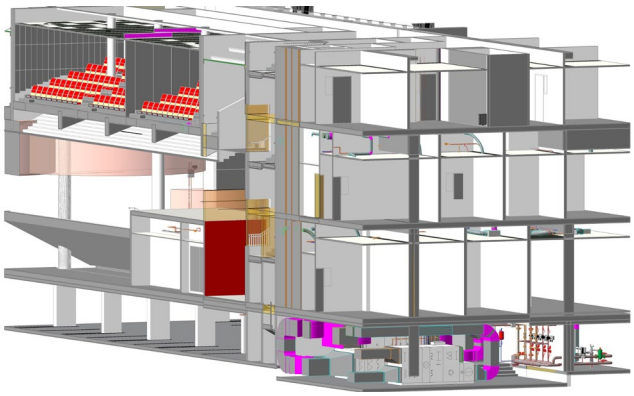
La supervision technique via le PC centralisateur du BOS se fait localement et indépendamment du cloud. La GTB y est plus accessible en ne



Exploitation du jumeau numérique de l'hyperviseur Twinops pour l'observation des niveaux de température ambiante des locaux



Pilotage CVC en tenant compte des conditions météorologiques futures et du comportement intrinsèque du bâtiment (utilisation de l'IA avec WiseBMS)



Exploitation de la maquette BIM conception en BTS Fluides Energies Domotique option Domotique et Bâtiments Communicants au lycée Hippolyte Fontaine de DIJON

représentant que les données utiles pour le niveau d'accès défini (exploitant, technicien…) avec des représentations graphiques qui ne décrivent pas forcément la réalité géographique (vues synoptiques adaptées au droit d'accès).

L'architecture de la supervision locale est distribuée entre le PC centralisateur et les différents contrôleurs, ce qui permet un bon niveau de résilience pour ne pas perdre la main en cas de panne d'un des JACE 8000. De plus sa position dans le système d'information la rend moins sensible aux cyberattaques et aux problèmes de communication via internet. Elle constitue une éventuelle solution de repli.

Exploitation future de l'intelligence artificielle

Alarmes techniques
Les alarmes techniques du bâtiment sont actuellement générées par des règles liées aux différentes situations envisagées et ces automatismes ne prennent pas forcément en compte toutes les situations possibles.

L'IA va permettre d'avoir une observation plus fine du comportement en générant des alarmes avec des origines non prévues auparavant. Pour cela, des profils de pièces du bâtiment sont définis et leurs comportements typiques sont actuellement modélisés au fur et à mesure de leur utilisation par l'acquisition des données réelles en fonction des habitudes d'usage.

Ainsi, l'intelligence artificielle détectera une anomalie si son comportement actuel s'en écarte. Cela pourrait permettre de repérer automatiquement l'ouverture de fenêtre en période de chauffe ou lors de forte chaleur en été, l'utilisation d'un chauffage électrique d'appoint pendant et/ou en dehors des périodes d'utilisation, les surconsommations énergétiques…

Amélioration de la performance énergétique

WiseBMS est une solution de pilotage intelligent du chauffage et de la climatisation qui sera prochainement mise en œuvre.

Basée sur des modèles d'intelligence artificielle, elle réalise une prédiction de l'évolution de la température du bâtiment en fonction de son comportement thermique et des conditions extérieures futures. Ainsi, le pilotage des équipements CVC devrait être optimal afin d'avoir le niveau de confort attendu au bon moment impliquant une meilleure performance énergétique.

Les systèmes de chauffage et de ventilation remontent les informations de pilotage et de comportement du bâtiment vers le BOS, notamment en BACnet IP. L'analyse de ces données qui ont été stockées (3 années d'exploitation) va réduire très nettement la durée de la phase d'apprentissage par l'IA. Cette adaptation plus rapide aura un impact plus efficace sur les économies d'énergie engendrées.

Formation des acteurs du bâtiment intelligent

Chaque bâtiment est unique avec un comportement différent et son propre mode de fonctionnement. Le smart building nécessite une compréhension globale de son fonctionnement et de son architecture.

De plus, il faut veiller à une continuité numérique de son système d'information pour la fiabilisation dans le temps de la maquette BIM GEM et pour son évolution en fonction des nouveaux cas d'usage qui apparaissent. Cela nécessite une bonne coordination de travail, un respect de la procédure de remontée des modifications opérées et un budget pour ce maintien opérationnel (besoin d'un opérateur digital).

Dans chaque domaine technique, la formation au niveau du système d'information des bâtiments doit donc permettre de comprendre les interactions et d'adapter le travail aux besoins systémiques pour une efficacité de son activité, la cybersécurité, le confort des usagers et la performance énergétique du bâtiment.

La formation en BTS Fluides Energies Domotique option Domotique et Bâtiments Communicants au lycée Hippolyte Fontaine de DIJON s'inscrit dans cette démarche. Le smart building ESTP-ESEO est un des supports d'étude des solutions de pilotage, de réseaux de communication numérique et de sa maquette BIM conception.

Francis Cunin
Professeur agrégé en ingénierie électrique
Lycée Hippolyte Fontaine – DIJON
francis.cunin@ac-dijon.fr | https://lyc21-hfontaine.sd.ac-dijon.fr/

L'interopérabilité des équipements techniques BACnet IP

L'interopérabilité est un enjeu central pour les installations techniques modernes, particulièrement dans les environnements à haute exigence tels que les salles blanches. Le protocole BACnet/IP s'impose aujourd'hui comme une référence pour assurer la communication et la coordination de multiples équipements de marques et de fonctions différentes.

Dans le cadre d'un projet pour UBBAK (CEF Nord), Asterm a réalisé les programmations et mises en service des automatisations des installations CVC d'un ensemble de 10 salles blanches – réparties en 5 salles de pesées et 5 salles de fabrication – et d'un couloir commun pressurisé pour un site de fabrication de cosmétiques situé en Haut-De-France. Les gestions de pression et débits des salles sont gérées par des régulateurs TROX Easylab TCU3 associées aux 12 CTA TROX et à la sous-station de distribution chaud/froid gérées par 13 automates Siemens PXC5.E24.

BACnet pour les asservissements des systèmes

Chaque salle dispose de son propre automate Siemens PXC5.E24 permettant l'automatisme des actionneurs selon les scénarios (positionnement des registres d'air neuf, reprise et rejet) , la régulation de température par action sur les vannes 2 voies des batteries eau glacée et eau chaude équipées d'EnergyValve Belimo et les régulations de pression de soufflage et reprise en gaine par action sur les variateurs Danfoss des ventilateurs afin de garantir le bon fonctionnement des systèmes TROX TCU3, avec au soufflage la gestion des débits et à la reprise la gestion de pression de salle.

Selon les modes d'occupation/inoccupation ou de détection de niveau de concentration d'alcool de la salle, les taux de renouvellement d'air doivent être modifiés dans les régulateurs TROX Easylab ; c'est donc au moyen du protocole BACnet/IP que l'automate Siemens PXC5.E24 vient modifier le mode de fonctionnement des EasyLab afin que ces deniers changent de point de consignes préréglés. L'automate PXC5.E24 récupèrent également les données de mesures des pressions, débits et position de la porte depuis les régulateurs EasyLab afin d'enregistrer les données dans des blocs d'historiques.
Quant au couloir pressurisé commun à l'ensemble des 10 salles et des différents Sas, il est régulé sur le même principe par 2 CTA et régulateurs EasyLab. Celles-ci sont asservis aux CTA des salles et c'est encore le BACnet/IP qui permet les échanges inter-automates Siemens PXC5.E24.

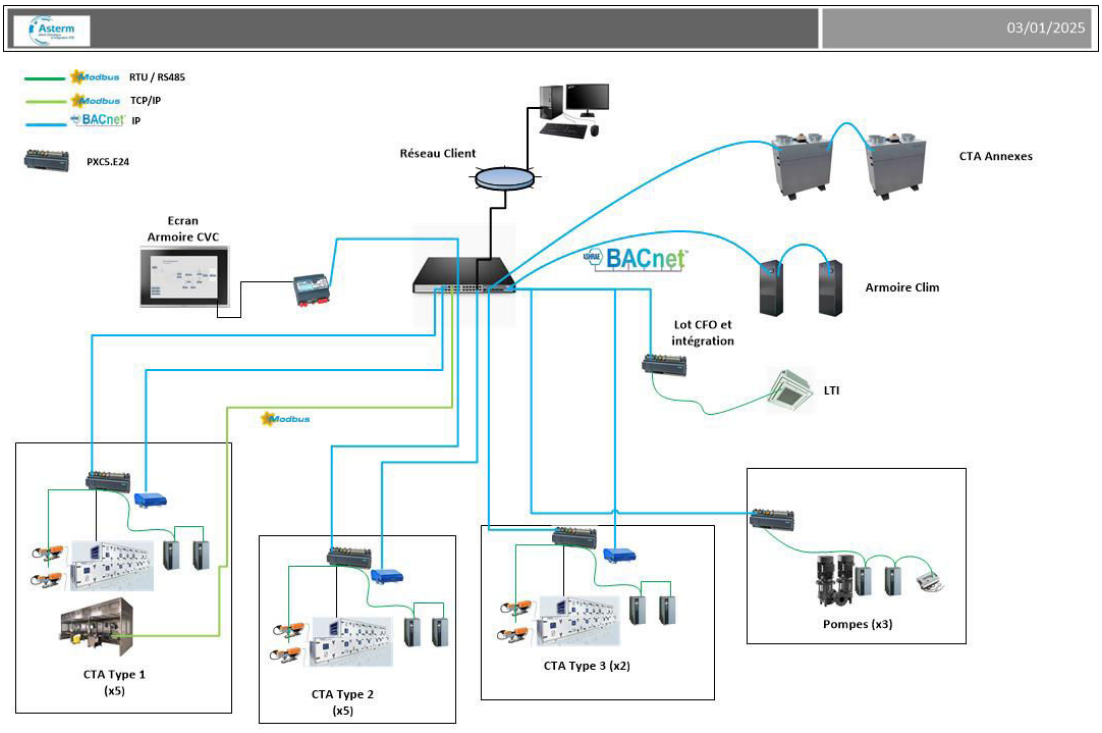
Le BACnet/IP est également utilisé pour l'asservissement des pompes à débits variables eau chaude et eau glacée selon les demandes d'ouverture des vannes 2 voies des CTA, entre les automates Siemens des CTA et l'automate Siemens de la sous-station, ceci afin de minimiser les consommations énergétiques des pompes.

Les automate Siemens PXC5.E24, munis de port RS485, permettent également la récupération des données des variateurs Danfoss et des EnergyValve via le protocole Modbus RTU, afin d'enregistrer les données

pour le suivi des installations mais aussi le pilotage de systèmes de cabine de pesées ERMA FLUX au protocole Modbus TCP.

Les données fédérées en BACnet IP

Les différents protocoles utilisés pour le pilotage et la lecture de données sont ensuite mis à disposition en BACNET/IP sur le réseau du client pour mise à disposition à la supervision GTB du site mais également pour l'IHM locale connectée au serveur Web LOYTEC de type LINX-154 qui vient communiquer directement en BACnet IP avec les automates pour afficher les différentes vues graphiques des installations et des consignes de pilotage.
La maîtrise d'une architecture multi-protocole pilotée par BACnet/IP est un atout différenciant pour ASTERM, permettant d'assurer à ses clients la performance, la traçabilité et la pérennité de leurs installations techniques les plus exigeantes.



Yann Pastorelli
Chargé d'affaires Régulation et Intégration
yann.pastorelli@asterm.com | www.asterm.com

ATEMIA
Intégrateur de solutions multimarques, multi-protocoles

Caractéristiques essentielles de l'immeuble INSPIRA – Projet livré en 2025 à Issy-Les-Moulineaux (92) :

- Surface totale : environ 11 300 m² de bureaux utiles répartis sur 7 niveaux
- Étages : 7 niveaux en superstructure
- Rénovation & certification : BREEAM In Use niveau « Very Good »

Objectifs du projet :

Mise en place d'une GTB (le site en était initialement dépourvu) afin de superviser l'ensemble des installations techniques et de gérer les consommations énergétiques de l'immeuble via un logiciel dédié à l'efficacité énergétique.

Solutions et évolutions mises en place :

Dans le cadre du projet de création d'une GTB, ATEMIA a été choisie pour le lot GTB. Nous avons pu déployer :

Un poste d'exploitation complet intégrant:

- Le logiciel de supervision PcVue,
- La solution EC-Net 4 PRO associée à Space Dynamix pour la gestion du cloisonnement des unités terminales,
- Et le logiciel AREE pour la surveillance et la maîtrise des consommations énergétiques à partir des compteurs du site.

Des automates BACnet/IP :

Le remplacement des automates des tableaux divisionnaires et des services généraux (unités terminales, boucle PAC, réseau chaud, TGBT, etc.), via des automates iSMA CONTROLLI et Distech Controls en protocole BACnet/IP. Également la reprise d'installations existantes et communicantes sous protocole Modbus, converties en BACnet/IP au travers d'automate programmable.

Une station météo :

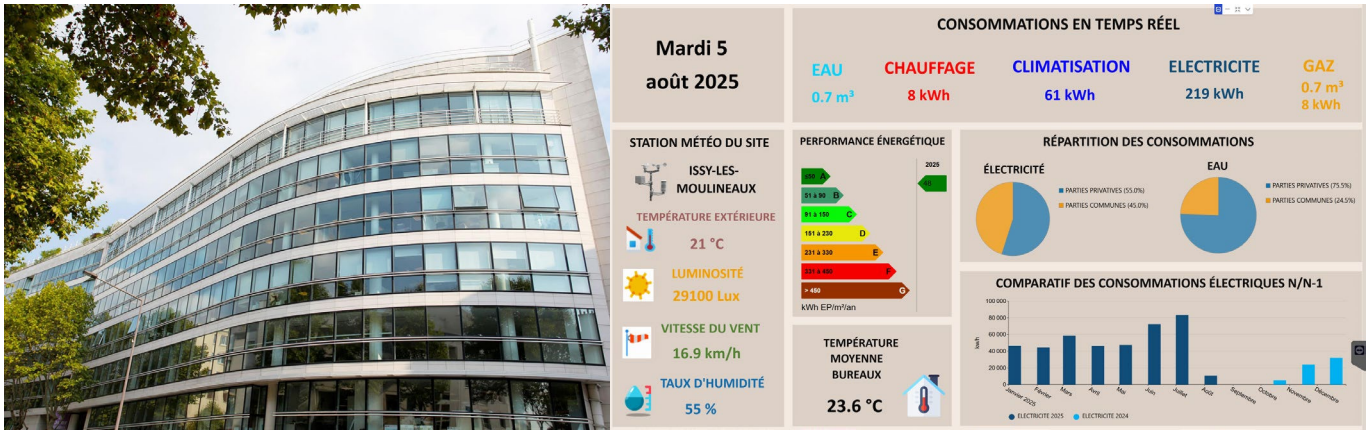
Installation d'une station météorologique et de sondes d'ensoleillement pour affiner la gestion climatique du bâtiment.

Un logiciel de gestion énergétique :

Pour mieux gérer les consommations d'énergies et se conformer aux réglementations en vigueur, nous avons remonté plusieurs compteurs (Modbus et M-Bus), exploités via le logiciel AREE Building d'Inneasoft. Chaque locataire reçoit mensuellement et automatiquement les rapports de consommation de leur plateau, assurant transparence et conformité réglementaire.

Un dashboard d'accueil :

Mise en place d'un écran dynamique dans le hall de l'immeuble, affichant en temps réel les données de consommation énergétique et les conditions météorologiques de la station météo.



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

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

GTB et enseignement : le pari gagnant de Marcq Institution pour mieux maîtriser ses consommations.

Face aux exigences des décrets Tertiaire et BACS, les établissements scolaires doivent engager des actions concrètes pour réduire leurs consommations énergétiques. A Marcq-en-Baroeul dans le Nord, l'établissement d'enseignement privé Marcq Institution a choisi la Gestion Technique du Bâtiment (GTB) comme levier prioritaire pour piloter efficacement ses installations, détecter les dérives et réduire les consommations dans le cadre d'une refonte future de la production.

L'établissement privé Marcq Institution

Pour mener à bien ce projet ambitieux, Marcq Institution s'est appuyé sur deux partenaires complémentaires : EISOX, concepteur et intégrateur de systèmes de Gestion Technique du Bâtiment basés sur l'analyse des données de présence, et SOBREN, société spécialisée dans le financement d'action d'économies d'énergie.

Objectif : reprendre la main sur les installations

Avec plus de 40 000 m² répartis sur 6 bâtiments et 2 sites distincts, ce campus représente un défi technique majeur : des bâtiments historiques anciens datant du XIXe siècle, des chaufferies multiples, des usages hétérogènes selon les bâtiments et un pilotage jusque-là entièrement manuel. A son arrivée, Christophe Videlaine, responsable immobilier de l'établissement, s'est emparé de la question du chauffage avec une conviction forte : « compte tenu de la taille du site, la GTB était l'action prioritaire pour s'engager dans une démarche d'économies d'énergie viable ». L'ancien système imposait la reprogrammation manuelle des 5 chaufferies avec des contraintes supplémentaires les week-ends et jours fériés. « Pour gérer les usages différents des bâtiments avec chacun ses horaires, il fallait un système autonome, capable d'apprendre et de s'adapter aux besoins du site », explique-t-il. C'est dans ce contexte qu'EISOX a proposé une GTB classe A (selon NF EN ISO 52120-1) pilotée via une plateforme intuitive.

Un projet sur-mesure avec EISOX

Sur un marché très concurrentiel, EISOX s'est démarqué par son système standardisé et évolutif, associé à un suivi technique de proximité de l'installation du matériel jusqu'à la formation des équipes. L'opération a nécessité l'intégration de 579 têtes de régulation et la reprise progressive d'anciens équipements. Dès la mise en service, la plateforme EISOX a permis de révéler des anomalies majeures : vannes montées à l'envers, cassées, régulations défaillantes, circuits non fonctionnels… « Dès la première semaine, certains dysfonctionnements critiques ont été détectés et corrigés. Ce sont des choses que l'on ne voit jamais avec une GTB traditionnelle » souligne Maxence Chotard, cofondateur d'EISOX. Le système de GTB classe A centralise désormais la gestion du chauffage et de l'éclairage extérieur avec planification automatique, équilibrage énergétique et alertes en temps réel.

Un financement décisif grâce à SOBREN

Ce projet n'aurait pas vu le jour sans le dispositif des Certificats d'Economie d'Energie (CEE). Grâce à l'accompagnement de SOBREN, Marcq Institution a bénéficié d'une prime de près de 145 000 € couvrant plus d'un tiers du coût global des travaux. « Les aides étaient capitales, elles ont même été l'élément déclencheur. » insiste Christophe Videlaine. SOBREN a pris en charge l'ensemble du processus CEE, de l'ingénierie financière à la conformité réglementaire, tout en anticipant les évolutions législatives pour sécuriser l'opération.

Un modèle pour d'autres établissements

Malgré une installation encore en phase d'optimisation, les résultats sont déjà au rendez-vous : 19% d'économies d'énergie L'objectif est fixé à 25% à pour l'hiver prochain. « Et au-delà de la question énergétique, c'est un véritable gain de temps pour nous. De plus, nous avons maintenant une vision claire de nos installations et un contrôle centralisé de nos équipements » note Christophe Videlaine.

Avec un retour sur investissement estimé à 4-5 ans (contre 8 ans sans la prime CEE), Marcq Institution démontre que l'installation d'un système de GTB peut être rentable et opérationnelle rapidement à condition de bien s'entourer et de bénéficier des bons leviers financiers.

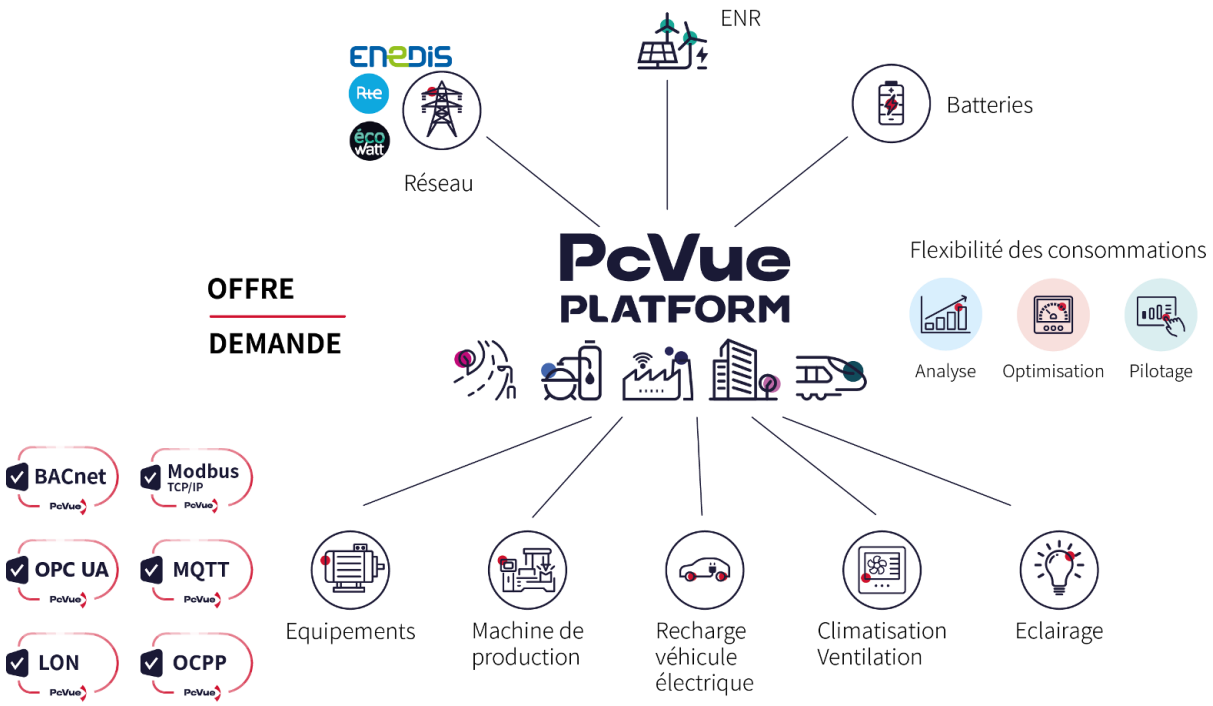
Un exemple inspirant pour le secteur de l'enseignement où les contraintes budgétaires et la complexité des usages reste un frein au passage à l'acte pour la maitrise des consommations énergétique, mais où les solutions existent.

SOBREN
l.fosse@sobren.fr
www.sobren.fr

EISOX
maxence.chotard@eisox.com
www.eisox.com

Marcq Institution
christophe.videlaine@marcq-institution.com
www.marcq-institution.com

Stratégie énergétique intelligente : les clés de la transition avec PcVue



Stratégie énergétique intelligente : les clés de la transition avec PcVue

Efficacité, flexibilité, cybersécurité : trois piliers indissociables d'une gestion moderne des bâtiments. Pour répondre à ces enjeux, une plateforme centralisée comme PcVue, joue un rôle essentiel en connectant, analysant et pilotant intelligemment les équipements sur l'ensemble de la chaine de production et de consommation.
La digitalisation, l'interopérabilité des systèmes et les nouvelles technologies telles que l'IA sont des éléments clés.

Interopérabilité complète

Une stratégie énergétique performante commence par une vue unifiée de tous les flux. Grâce à ses nombreux protocoles natifs, PcVue connecte aussi bien les sources d'énergie (réseau, photovoltaïque, batteries…) que les consommateurs (CVC, éclairages, Bornes de recharges…), pour un pilotage en temps réel.

Analyse et optimisation avec EmVue

EmVue, logiciel de la plateforme PcVue, transforme les données issues des compteurs en analyses concrètes. Il identifie les dérives, détecte les inefficacités, et aide à définir des actions ciblées. Pensé pour les experts en énergie, il reste accessible à tous : déploiement rapide, prise en main intuitive et résultats exploitables immédiatement.

Flexibilité et pilotage intelligent

PcVue permet d'anticiper les pics de consommation grâce à des scénarios intelligents intégrant météo, signaux tarifaires ou disponibilité des sources. L'IA embarquée apprends des évènements passés et pourra par exemple prédire des dépassements de seuils de consommation et ajuster le pilotage des équipements pour les éviter.

Cybersécurité intégrée et conformité

Interconnexion rime avec exposition. Face à la montée des cybermenaces, la sécurité devient un impératif. Les référentiels NIS2, IEC 62443, CSPN, CRA imposent des exigences strictes. ARC Informatique, intègre dans la plateforme PcVue des fonctions de cybersécurité telles que la gestion des accès, un chiffrement des flux (BACnet Secure Connect, OPC UA, TLS), et une supervision active des incidents. L'entreprise certifiée ISO 9001 et ISO 27001, applique ces standards garantissant un haut niveau de qualité et de sécurité à toutes les étapes de la conception à l'utilisation de ses solutions.

Mr François Fleche
Corporate marketing manager
f.fleche@arcinfo.com | www.pcvue.com

Consommation d'énergie AREE : Le suivi simplifié grâce à BACnet

Comment centraliser simplement le suivi énergétique d'un parc multi- sites composé d'automates industriels, de régulations embarquées hétérogènes et d'une production photovoltaïque hors norme sans remettre en cause l'existant ?

C'est la problématique à laquelle l'intégrateur SCS avec le logiciel AREE a su répondre.

Le BACnet : la solution

Face à la complexité de ses installations, le propriétaire du site aurait pu craindre un chantier invasif, long et coûteux. Au contraire, en choisissant l'intégrateur multi-marques SCS, il a pu continuer à se concentrer pleinement dans son domaine d'expertise (la supply-chain) pendant la mise en place de la solution.

La clé du succès ?

Assurer la convergence de l'ensemble des équipements autour d'un protocole, le BACnet. Et pour les équipements non-communicants, la transformation des protocoles ou la modernisation des installations aura impliqué le déploiement d'automates de marque Schneider Electric.

C'est là que la magie du logiciel AREE opère

En collectant les données directement à la source, au cœur de l'automate, et en limitant le recours à une chaîne d'équipements intermédiaires, AREE assure une fiabilité optimale tout en réduisant fortement les risques de panne.

C'est grâce à son driver BACnet que le logiciel déploie tout son potentiel et révèle son efficacité.

La détection de fuite d'eau facilement

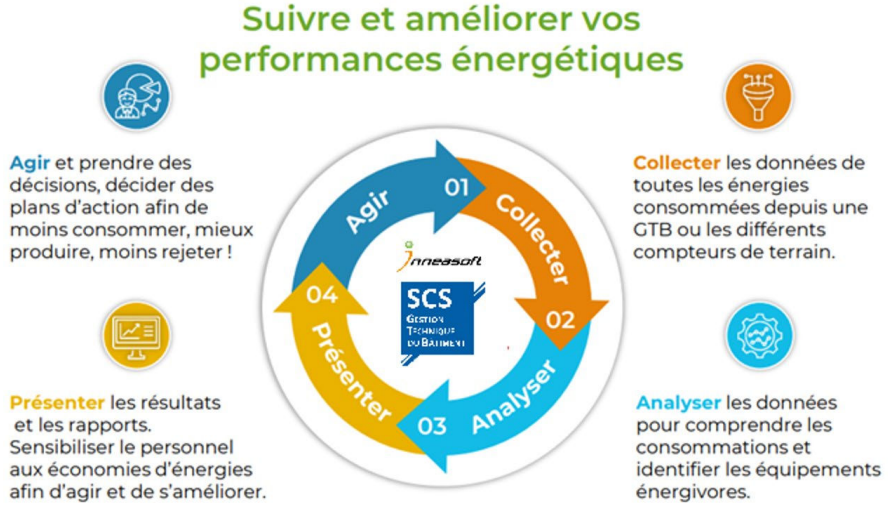
Il y a encore une dizaine d'années, détecter une fuite d'eau nécessitait de programmer manuellement chaque automate équipé d'un compteur, en surveillant l'évolution de l'index sur une période donnée. Une méthode efficace, certes, mais complexe à mettre en œuvre et à maintenir.

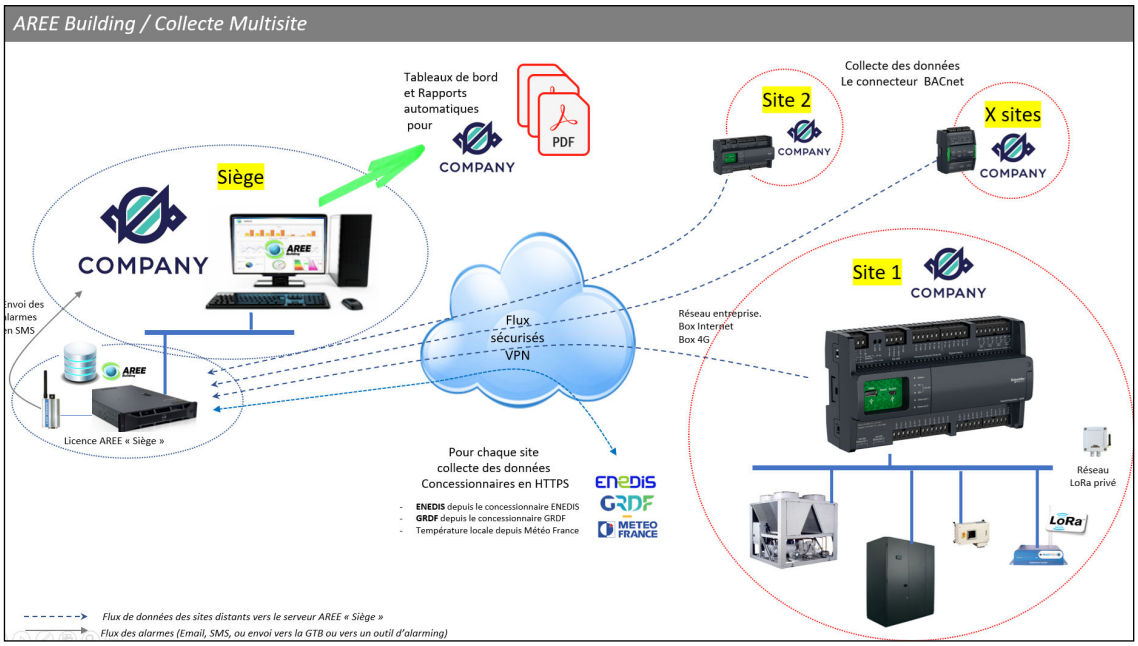
Aujourd'hui, AREE simplifie considérablement ce processus grâce à l'intégration, dans sa licence de base, d'un module dédié.

Ce dernier permet de définir des seuils instantanés (horaires, journaliers et/ou mensuels) facilement configurables et modifiables à tout moment par un utilisateur sans connaissance de programmation.

Une solution multisite

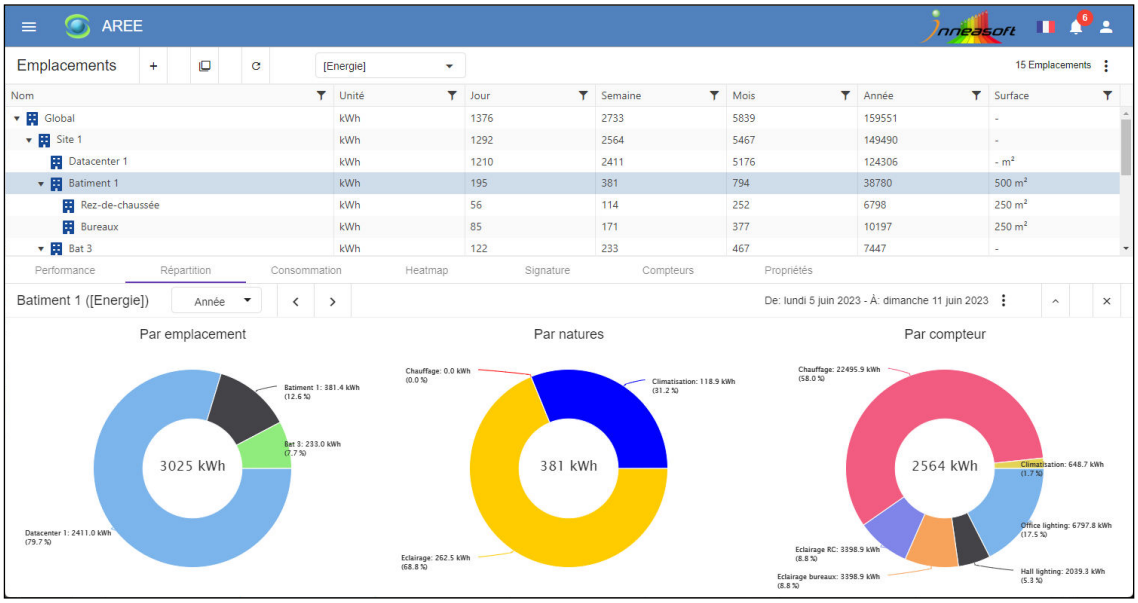
SPI Group : Créé en 1985, le groupe SPI apporte depuis plus de 30 ans sa vision industrielle et son expertise à ses clients. Le groupe apporte sa valeur ajoutée sur l'ensemble des métiers indispensables à la suppply chain. Conditionnement primaire et secondaire, mise en avant des produits, entreposage, préparation de commandes et pilotage des flux de transport.





Déploiement de la solution

L'architecture repose sur un principe simple : collecter les données de plusieurs sites à partir d'un point central, via les connecteurs disponibles dans le logiciel AREE Building.



Répartition multicritère

Les consommations peuvent être représentées à l'aide de différents types de graphiques permettant une lecture plus claire et comparative des données.

Avec SCS, vos installations évoluent à votre rythme : Satisfait du résultat obtenu sur son premier site, SPI Logistic a alors émis le souhait d'intégrer à la solution ses autres sites. Toutes les installations proposées par SCS sont évolutives dans le temps (la seule limite, c'est votre créativité).

La licence AREE Building est souple : elle permet l'extension facile du nombre de compteurs supervisés et l'installation sur site ou en Cloud Privé.

SPI Logistic en a fait l'expérience : après un premier déploiement réussi, un deuxième site a rejoint la plateforme… et d'autres suivront bientôt à travers toute la France. »

Nicolas Robin
Commercial Régulation & GTB |
Responsable Agence SCS Auvergne Rhône-Alpes
Nicolas.robin@s-c-s.fr | www.s-c-s.fr

Thierry Chenavas
Directeur Commercial | Co-gérant INNEASOFT
thierry.chenavas@inneasoft.com | www.inneasoft.com

Optimisez la cybersécurité de vos bâtiments grâce à BACnet/SC et à l'interopérabilité multimarques

Dans le cadre de son partenariat avec l'association BACnet France, AGILiCOM organise plusieurs ateliers en ligne consacrés à l'interopérabilité des équipements multimarques au sein des systèmes GTB/GTC, utilisant le protocole BACnet/SC. Ces événements ont permis de présenter des solutions innovantes pour améliorer la cybersécurité des bâtiments existants sans nécessiter un remplacement complet des installations.

L'interopérabilité multimarques représentée sur une maquette

Lors de ces ateliers, notre expert en réseaux industriels, Julien AUGER, s'appuie sur une maquette intégrant des équipements BACnet/IP et BACnet/SC de deux leaders du secteur, Siemens et Johnson Controls. Cette configuration permet d'illustrer de manière claire et détaillée comment ces deux systèmes peuvent fonctionner de manière harmonieuse, grâce à une interopérabilité fluide entre les équipements. À travers des démonstrations pratiques, Julien montre comment la mise à jour régulière des dispositifs et l'utilisation d'outils de configuration dédiés permettent de garantir non seulement la compatibilité des équipements, mais aussi une gestion optimale des infrastructures de bâtiments.

La gestion des certificats : un gage de sécurité

L'élément clé réside dans la gestion des certificats numériques, qui constitue le socle de la sécurité des communications entre équipements. En assurant une gestion stricte des certificats, BACnet/SC garantit une communication sécurisée et conforme aux standards les plus exigeants. Ce procédé est indispensable pour créer une interopérabilité fiable et sécurisée entre les systèmes de différentes marques, tout en répondant aux exigences de cybersécurité de plus en plus strictes dans le secteur.

Une innovation pour des bâtiments toujours plus sécurisés

Cette avancée technologique permet aux gestionnaires de bâtiments de moderniser leurs

installations sans devoir remplacer l'intégralité des équipements existants. BACnet/SC s'inscrit parfaitement dans cette logique en renforçant la cybersécurité des systèmes existants, tout en facilitant l'intégration de solutions multimarques. Ce protocole assure une protection renforcée contre les cybermenaces tout en offrant une interopérabilité avancée entre les équipements de différentes marques et versions de BACnet.

Testée et validée par AGILiCOM en partenariat avec BACnet France, cette approche constitue une étape majeure dans la modernisation sécurisée des bâtiments, offrant ainsi aux gestionnaires un moyen efficace de se conformer aux exigences de cybersécurité actuelles tout en optimisant la gestion de leurs infrastructures.

Sécurisez et optimisez votre GTB/GTC en formant vos équipes

Nouvelle formation BACnet chez AGILiCOM : BACnet/SC – Optimisez la cybersécurité de votre GTB/GTC. Les prochaines sessions auront lieu en décembre 2025.

Inscrivez-vous via le QR CODE et recevez le détail de la formation en ligne.

Vous pouvez également vous inscrire aux formations certifiées BACnet France :

- Présentation BACnet - 1j : permet d'acquérir les notions fondamentales pour communiquer sur vos projets avec vos interlocuteurs.
- BACnet Bureaux d'Etudes - 1j : centrée sur la maîtrise des points clés du réseau BACnet pour la conception et l'exploitation des projets multi-métiers GTB/GTC.
- BACnet Engineer - 2j : s'adresse aux intégrateurs et développeurs en présentant le standard BACnet. Cette formation aborde également des notions plus pointues telles que les outils et méthodes pour diagnostiquer un système BACnet via l'analyse des données du réseau.

Distributeur officiel INTESIS et LOYTEC

AGILiCOM propose une gamme complète de passerelles et d'interfaces de communication pour le marché du bâtiment afin d'interfacer les différents protocoles : GTB / GTC (LON, BACnet, KNX, M-Bus, ModBus…)

Besoin de vous former sur BACnet ?
Contactez-nous

AGILICOM
Réseau Gérance Industrielle

Julien Auger
Spécialiste Réseaux Industriels | +33 (0)2.47.76.10.20
j.auger@agilicom.fr | www.agilicom.fr

BACnet France lance son nouveau site web intégré à la présence web unifiée de la communauté BACnet mondiale

BACnet France a récemment dévoilé son site web remanié, désormais entièrement intégré à la présence web unifiée de la communauté BACnet mondiale. Cette consolidation de plusieurs plateformes en ligne s'inscrit dans un contexte important :

Il y a quelques années, BACnet International et BACnet Interest Group Europe (BIG EU) ont identifié un défi croissant dans le paysage numérique : les informations sur le protocole BACnet étaient dispersées sur différents sites Web, souvent incohérentes ou redondantes. Cette fragmentation compliquait la recherche d'informations claires et fiables.

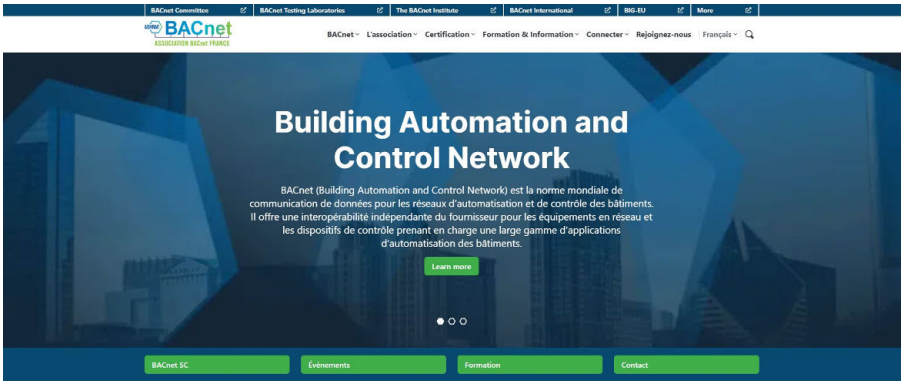
En réponse, BACnet International a mené une initiative visant à fusionner les principaux centres d'information en un cadre Web cohérent. En conséquence, la nouvelle plateforme unifiée englobe désormais :

- Le comité ASHRAE SSPC 135 (comité BACnet)
- BACnet International
- BACnet Interest Group Europe
- BACnet Testing Laboratories (BTL)
- Le BACnet Institute (TBI)

Le dernier ajout, BACnet France, renforce encore cette consolidation. Le site remanié offre :

- une structure et une navigation simplifiées et modernes,
- un contenu bilingue (français et anglais)
- une accessibilité améliorée, garantissant que les informations et les ressources de la communauté BACnet française sont facilement accessibles à un public international.

Dans l'ensemble, la plateforme mise à jour renforce la présence numérique de BACnet France et contribue à la visibilité et à l'accessibilité mondiales du protocole BACnet.



https://bacnetfrance.org/

En détail : nouvelles fonctionnalités du site web de BACnet France

- Navigation claire et complète : les visiteurs du site web peuvent facilement accéder à un large éventail d'informations, notamment les avantages de l'adhésion, la présentation de l'association, la certification BTL, les revues, les événements, et bien plus encore ! Les visiteurs peuvent également accéder à d'autres organisations BACnet au sein de la communauté mondiale BACnet.
- BACnet Secure Connect (BACnet/SC) : BACnet France offre une multitude d'informations sur BACnet/SC, notamment des formations, son projet de données sécurisées et du contenu exclusif pour les membres de BACnet France.
- Ressources pédagogiques : Approfondissez vos connaissances sur BACnet grâce aux articles de la revue BACnet France, aux études de cas, aux vidéos YouTube et aux modules de formation proposés en partenariat avec Agilicom.

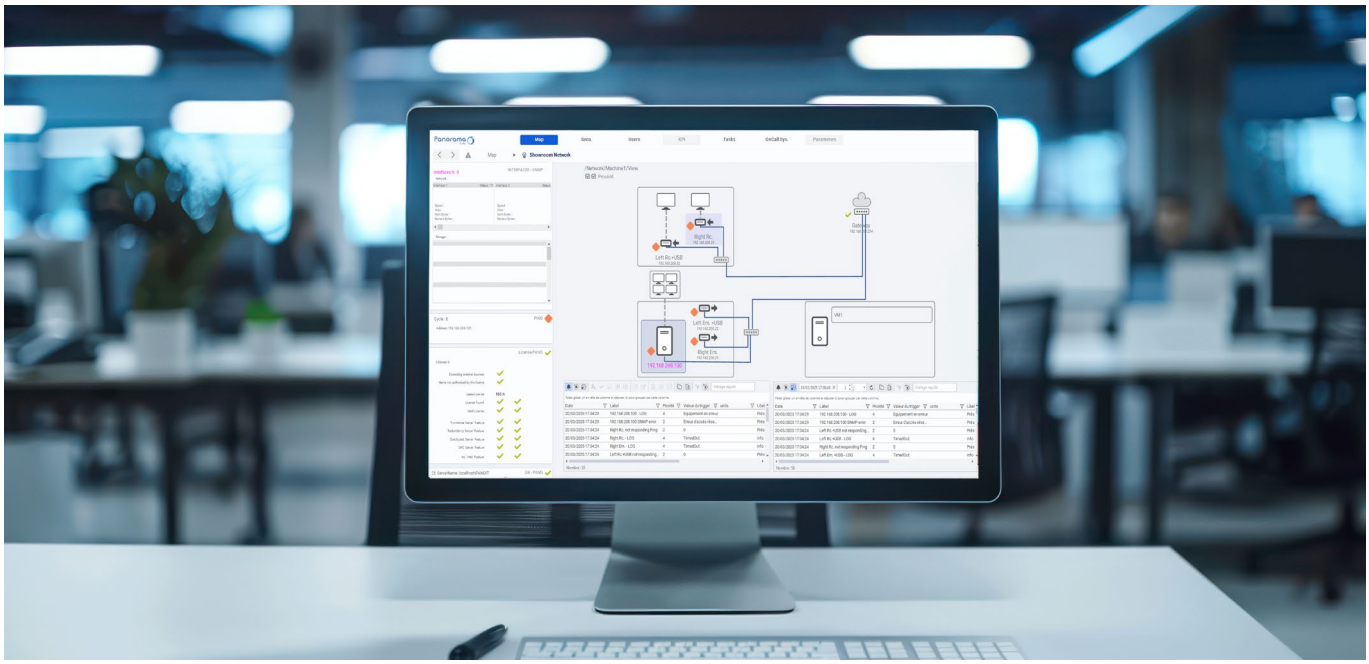
Conclusion

Le site web remanié de BACnet France, avec sa conception plus claire, son contenu bilingue et son alignement sur l'écosystème web BACnet plus large, marque une étape décisive vers l'accessibilité mondiale des informations relatives à BACnet. En regroupant des ressources complètes sous un même toit numérique cohérent, cette initiative renforce la transparence, l'efficacité et la collaboration internationale.

Mary Catherine Heard
Responsable Marketing et Communication | BACnet International
marycatherine@bacnetinternational.org | www.bacnetinternational.org

Hans Symanczik
Rédaction et publicité | TEMA Technologie Marketing AG
symanczik@tema.de | www.tema.de

BACnet/SC : Comprendre la norme dédiée à la sécurité des bâtiments



L'impact de cette norme pour les applications SCADA

Dans le domaine de la gestion technique des bâtiments (GTB), la sécurité et l'interopérabilité des systèmes sont cruciales. La norme BACnet Secure Connect (BACnet/SC) répond à ces défis en sécurisant les communications entre les divers appareils et systèmes de contrôle.

Avec l'augmentation des cybermenaces, il est devenu impératif de protéger les infrastructures critiques. Les applications SCADA développées avec Panorama Suite peuvent intégrer désormais cette norme, offrant ainsi aux utilisateurs une infrastructure plus sûre et efficace.

Cet article explore les aspects clés de BACnet/SC, son fonctionnement, et comment une solution comme Panorama Suite intègre cette norme.

Qu'est-ce que la norme BACnet/SC ?

Origine et développement

BACnet/SC est une extension du protocole BACnet, visant à renforcer la sécurité des communications. BACnet/SC ajoute une couche de sécurité supplémentaire, protégeant contre les cyberattaques et sécurisant les données échangées entre les appareils grâce à des certificats et des protocoles de chiffrement avancés. Cette extension est le résultat de plusieurs années de recherche et de développement pour répondre aux défis de sécurité émergents dans le domaine de la GTB.

Pour être compatible avec cette norme, la plateforme Panorama Suite a dû respecter deux standards:

- Intégrer un hub de sécurité dans son architecture
- Utiliser des protocoles de communication sécurisées

Fonctionnement d'un hub BACnet/SC

Un hub BACnet/SC sert d'interface centrale de communication entre les automates et les systèmes de supervision. Voici son rôle et son importance pour une infrastructure sécurisée :

- Interface de Communication : Le hub facilite la gestion et le contrôle des flux de données, assurant une communication fluide et sécurisée entre les différents composants du système. Ceci permet une intégration transparente et efficace.

- Redondance : Les hubs peuvent être configurés en mode redondant pour assurer une continuité de service, minimisant ainsi les risques de panne et garantissant une disponibilité constante. Cette fonctionnalité offre aux applications SCADA une flexibilité accrue et une fiabilité améliorée.

- Hub Non Fournis : Bien que Panorama Suite supporte les hubs BACnet/SC, ceux-ci ne sont pas fournis. Des constructeurs proposent des automates et logiciels spécifiquement conçus pour jouer ce rôle, offrant ainsi une gamme de solutions adaptées aux besoins spécifiques des utilisateurs.

Communication sécurisée par certificat

- Exécution sur TLS : Les communications sont sécurisées via le protocole TLS (Transport Layer Security), garantissant un chiffrement de bout en bout. Cela signifie que toutes les données échangées entre les appareils sont protégées contre les interceptions et les manipulations, assurant ainsi une confidentialité et une intégrité optimales.

- Connexion Chiffrée : Chaque connexion est authentifiée et chiffrée, protégeant les données contre les accès non autorisés. Les systèmes de supervision assurent que toutes les communications sont sécurisées via ces connexions chiffrées, offrant ainsi une protection robuste contre les cybermenaces.

Explicitons le fonctionnement de cette norme de façon plus graphique, avec quelques schémas.

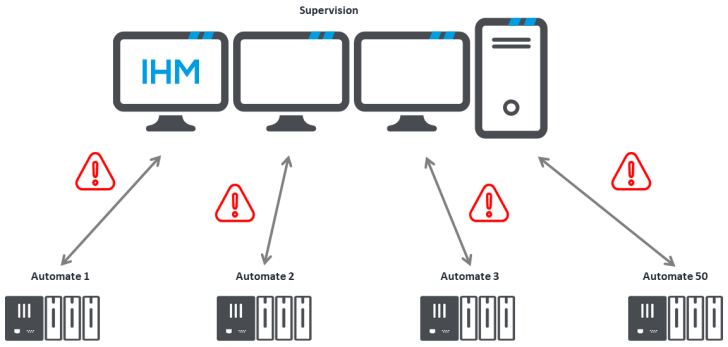
La norme BACnet/SC, une force pour vos infrastructures

L'adoption de BACnet/SC apporte des avantages significatifs pour la GTB. Voici pourquoi cette norme est cruciale :

Infrastructure BACnet d'une application SCADA sans BACnet/SC

Sans BACnet/SC, les automates sont exposés directement, augmentant les risques de sécurité.

Les communications non chiffrées sont vulnérables aux interceptions et aux cyberattaques, ce qui peut compromettre la sécurité et la fiabilité des systèmes de GTB.

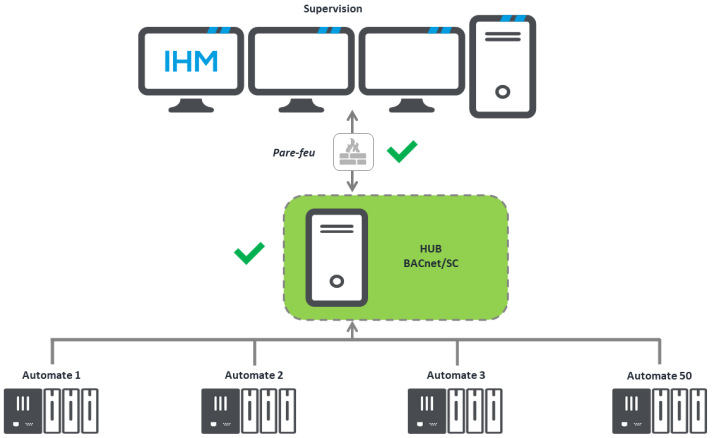


Infrastructure BACnet d'une application SCADA sans BACnet/SC

Infrastructure BACnet d'une application Panorama avec BACnet/SC

Avec BACnet/SC, les automates sont protégés derrière des systèmes de sécurité, réduisant le nombre de flux directs et simplifiant la gestion des communications.

Les applications SCADA intègrent cette configuration pour une gestion optimisée, offrant ainsi une solution complète et sécurisée pour la GTB.



Infrastructure BACnet d'une application Panorama avec BACnet/SC

BACnet/SC, une évolution essentielle pour la sécurisation des communications

En conclusion, BACnet/SC est une évolution essentielle pour la sécurisation des communications dans les systèmes de GTB. Avec des plateformes comme Panorama Suite, qui intègre cette norme, les utilisateurs bénéficient d'une intégration transparente et sécurisée, optimisant ainsi la performance et la sécurité de leur supervision, et donc de leurs infrastructures. CODRA se positionne comme un interlocuteur de choix pour une gestion technique des bâtiments plus sûre et efficace, répondant aux besoins croissants de sécurité et d'interopérabilité dans un monde de plus en plus connecté.

Charles Tabath
Chef de Projet – Marketing Produit chez CODRA
c.tabath@codra.fr | www.codra.fr

Date	Lieu	Événement	Contact
2024-2025			
30.09.-01.10.2025	Paris, Porte de Versailles	IBS – Intelligent Building Systems	www.ibs-event.com
15.-16.10.2025	ExCel, Londres, UK	BIG-EU au Smart Buildings Show 2025	www.smartbuildingsshow.com
10.02.2026	Paris, Carrousel du Louvre	EnerJ-meeting Journée de l'efficacité énergétique et environnementale du bâtiment	www.enerj-meeting.com
08.-13.03.2026	Francfort-sur-le-Main, Allemagne	BACnet Joint Booth au Light+Building 2026	www.light-building.messefrankfurt.com/frankfurt/de.html
Novembre 2026	Paris, Porte de Versailles	IBS – Intelligent Building Systems	www.ibs-event.com
15.-19.03.2027	Francfort-sur-le-Main, Allemagne	ISH – Salon International du CVC + Eau	www.ish.messefrankfurt.com/frankfurt/en.html

BACnet France Journal

ASHRAE BACnet ASSOCIATION BACnet FRANCE

Présentation du numéro 19 – Novembre 2026

Thème principal : la cybersécurité avec BACnet SC
Date limite d'enregistrement : Juin 2026

Date de parution : Novembre 2026

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 (Siemens)
Vice-Présidents :
Lucien River (Kieback&Peter),
Nicolas Cheyroux (Johnson Controls)
Trésorier :
Jean-Yves Bois (Agilicom)
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.

METZ CONNECT

We realize ideas

Routeurs BACnet/IP et BACnet/SC – Sécurité des données avec Secure Connect

IP

Routage entre les réseaux BACnet/IP, BACnet Ethernet et BACnet MS/TP

SC

Routeur utilisable comme Nœud BACnet/SC

Connexion rapide des appareils

RS485 TCP Alimentation électrique

Isolation galvanique triple

Serveur Web intégré

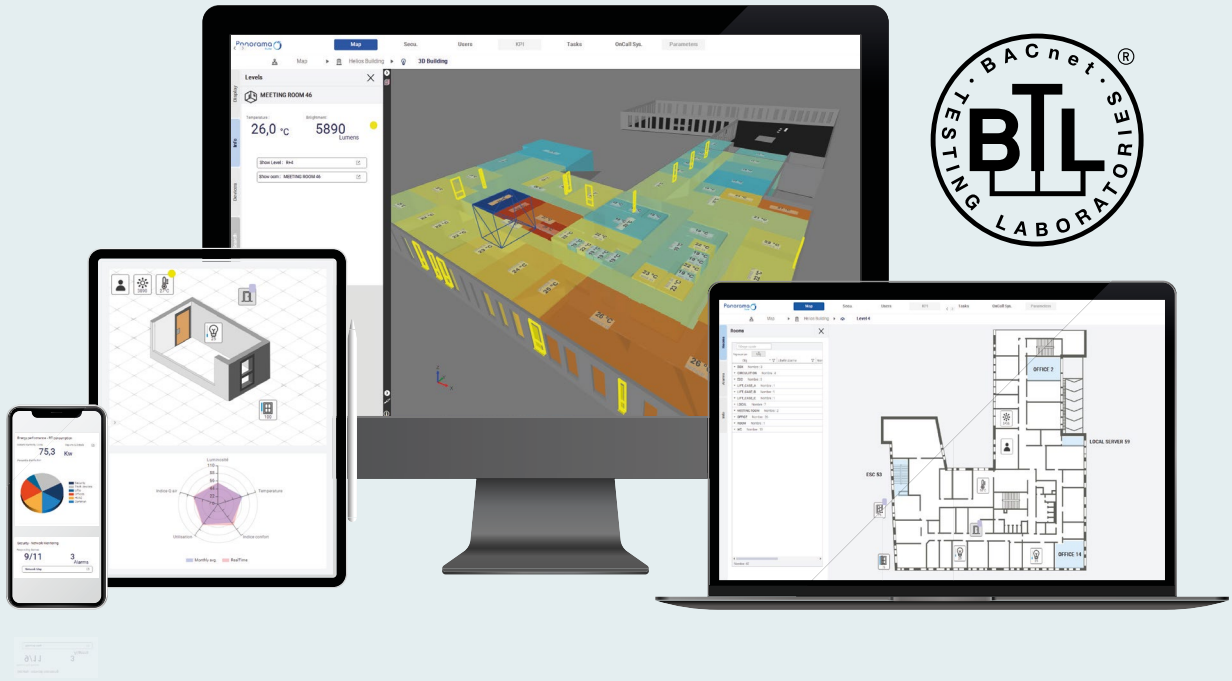
Configuration intuitive

www.metz-connect.com

Panorama Suite

Comment assurer le pilotage énergétique de vos bâtiments tertiaires ?

CODRA propose la plateforme Panorama Suite pour superviser et optimiser les consommations de vos bâtiments



- S'interfacer avec les différents systèmes techniques et métiers
- Suivre et analyser les données énergétiques
- Ajuster en temps réel la consommation des bâtiments
- Détecter les anomalies et alerter les exploitants

Installer une GTB/GTC Panorama, c'est optimiser les performances énergétiques de vos installations.

CODRA

Contactez-nous 01 60 92 34 34
www.codra.net panorama@codra.fr