Table des matières

[Les bâtiments, les plus gros consommateurs en énergie 3](#_Toc24126216)

[SMART GRID – Qu’est-ce c’est ? 4](#_Toc24126217)

[Données et nécessité de standard universel 4](#_Toc24126218)

[Réglementations et certiﬁcations pour l’efficacité énergétique 5](#_Toc24126219)

[Interopérabilité 6](#_Toc24126220)

[Notion de BUS 6](#_Toc24126221)

[Protocole BACnet 7](#_Toc24126222)

[Sécurité de BACnet 7](#_Toc24126223)

[Plateforme LonWorks 7](#_Toc24126224)

[SmartServer d’Echelon 8](#_Toc24126225)

[ModBus 8](#_Toc24126226)

[ModBus/TCP 8](#_Toc24126227)

[KNX 9](#_Toc24126228)

[Sécurité dans ZigBee 10](#_Toc24126229)

[Trust Center 10](#_Toc24126230)

[Z-Wave 10](#_Toc24126231)

[Sécurité 10](#_Toc24126232)

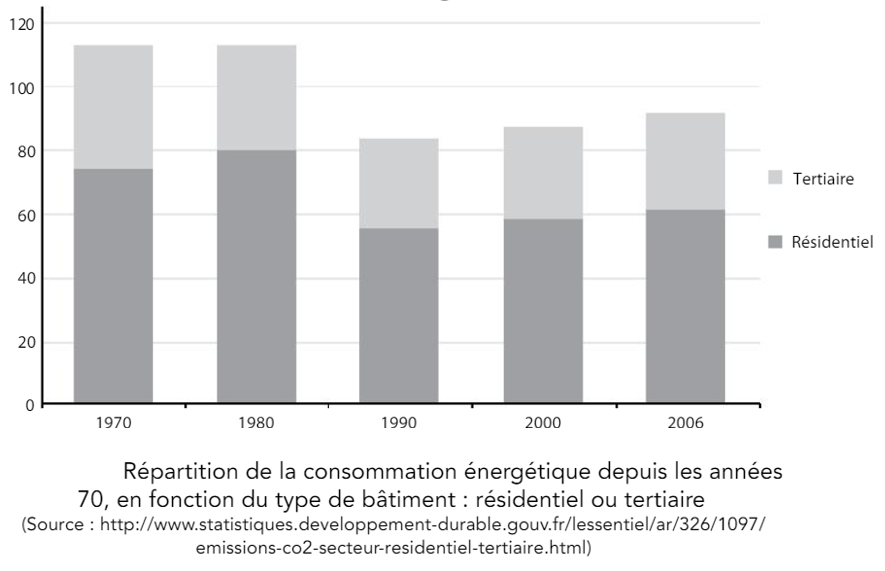
## Les bâtiments, les plus gros consommateurs en énergie

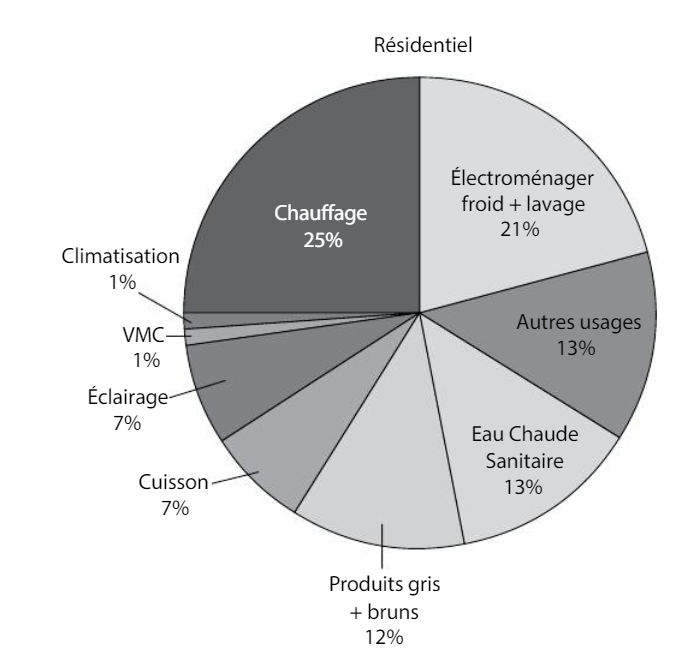
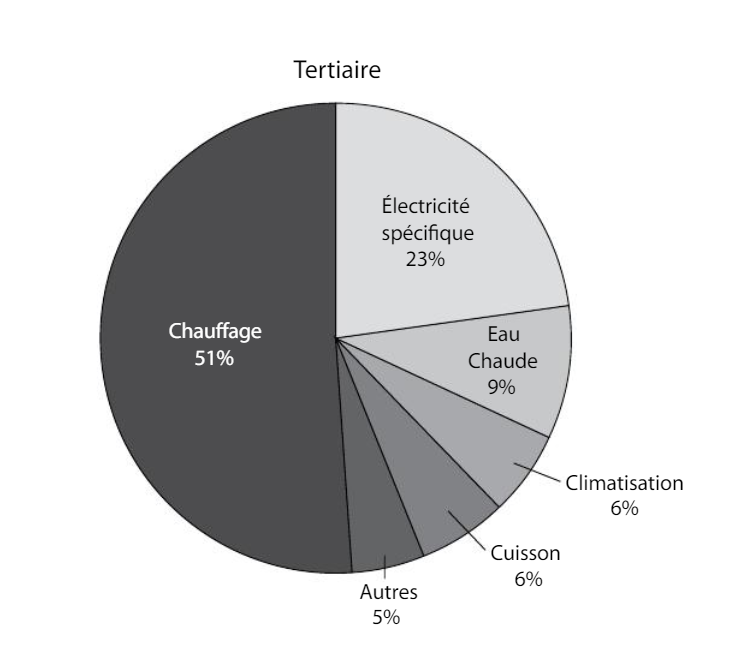
On parle de plus en plus d’économiser l’énergie. Même si cela semble simple, économiser l’énergie implique en réalité un ensemble colossal de connaissances et de techniques.

Le réchauffement climatique est une réalité. De nombreuses études l’ont montré, notre planète est en train de subir un changement climatique de grande ampleur dû en grande partie à l’activité humaine.

Le domaine du bâtiment, dans le résidentiel autant que dans le tertiaire, est particulièrement concerné par les émissions de gaz à effet de serre (GES)

Le secteur du bâtiment est responsable chaque année de 25% des émissions de CO2. De leur côté, les transports comptabilisent 28%, l’industrie 22% et l’agriculture/sylviculture 12%, 10% pour les autres secteurs. Sur l’ensemble des énergies consommées, 45,8% sont imputables au bâtiment, alors que l’industrie est responsable de 27,7%, les transports 23,9% et enfin 2,60% pour les autres secteurs. Les années 1990 ont vu une progression importante des émissions en CO2 dans le secteur du bâtiment, avec +22%, tandis que tous les autres secteurs, sauf le transport, ont vu une baisse significative.





Répartition de la consommation par poste entre résidentiel et tertiaire

## SMART GRID – Qu’est-ce c’est ?

Minimiser notre impact sur la planète nous commande de consommer moins d’énergie. Rendre nos bâtiments plus efficaces est indispensable et les initiatives donnent des résultats positifs, par exemple la réglementation thermique RT en la France.

La production d’énergie centralisée coûte très cher à transporter. Les infrastructures de transport coûtent également très cher à maintenir. En moyenne 30% de la facture d’électricité correspond au coût du transport de celle-ci. Les coûts d’investissement, d’entretien et de démantèlement des infrastructures ont des impacts très variables selon les pays, mais ont pour conclusion commune que l’avenir est dans la consommation locale de l’énergie.

L’énergie solaire fait peu à peu éclater ce modèle par un phénomène qui n’était pas anticipé lorsque les gouvernements ont incité à son développement: l’incapacité du réseau d’énergie, appelé Grid, à assimiler l’intermittence de la production. Que faire d’une production supérieure au besoin?

C’est là que la Grid trouve sa limite car elle n’est pas assez dynamique, pas assez smart.

Il va falloir équilibrer tout cela, consommer ce que l’on produit en temps réel et l’équilibrer à l’échelle d’une ville. Ce ne peut être que dynamique en raison de facteurs intermittents tels que l’ensoleillement, le vent ou les marées. Certains appareils consommateurs dans le bâtiment vont avoir besoin d’être mis en marche ou arrêtés par la grid car ils sont un élément de l’équilibre consommation/production.

Cette avancée majeure permettra également de faire disparaître les phénomènes de black-out puisque la grid pourra désactiver certaines charges et ainsi s’auto-délester pour éviter un effondrement total.

Le contrôle par la grid pose toutefois un problème de perte de confort: impossible par exemple d’accepter que le lave-vaisselle refuse de démarrer car le coût de l’énergie à ce moment n’est pas favorable. Il sera toujours possible de déroger à l’automatique et forcer le démarrage d’un appareil, mais l’utilisateur en paiera le surcoût.

Ces algorithmes et logiques ouvrent la voie à des systèmes d’optimisation sous des formes diverses tels que des boxes, ou des fonctions intégrées au smart building ou au smart home.

## Données et nécessité de standard universel

La grid parle au building jusqu’à l’appareil consommateur d’énergie, le building parle à la grid, les prévisions météo sont incluses dans l’équation, la production centralisée et les productions distribuées parlent à la grid. Tous doivent s’entendre sur un langage qui n’appartienne pas à un fabricant.

Un langage universel qui se limite à décrire la partie importante de la communication entre deux systèmes: la donnée.

Qu’elle soit température, variation, pourcentage il faut qu’elle utilise un format commun, ouvert et non propriétaire.

De nombreux protocoles de communication existent, ouverts ou non. Un moyen de transport de ces données universel est TCP/IP utilisé par tous les ordinateurs du monde, mais ce dernier ne décrit pas la forme de la donnée. En fait un format de donnée commun et ouvert existe et est utilisé par de nombreux protocoles de communication, par exemple KNX. Mais quels sont les produits disponibles qui utilisent ce format de donnée pour équiper les bâtiments aujourd’hui? C’est là que la sélection se réduit à Bacnet et KNX.

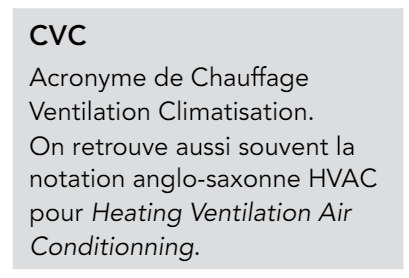
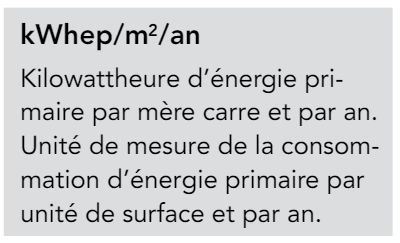
## Réglementations et certiﬁcations pour l’efficacité énergétique

En France, la réglementation thermique RT2012 a pour but de fixer une limite maximale à la consommation énergétique des bâtiments neufs pour le chauffage, la ventilation, la climatisation, la production d’eau chaude sanitaire ainsi que l’éclairage. La RT2012 actuellement en cours s’applique à tous les bâtiments neufs résidentiels ou non. Elle impose des contraintes relatives au traitement de la ventilation et des ponts thermiques. Elle impose des limites à la perméabilité à l’air, ainsi qu’aux tailles des ouvertures telles que fenêtres et baies vitrées. Elle encourage aussi le recours aux énergies renouvelables dans le but d’atteindre l’objectif des 20% d’énergies renouvelables d’ici à 2020. Cela prend la forme dans le résidentiel de l’imposition d’au moins une forme d’énergie renouvelable dans les constructions neuves (solaire thermique, solaire photovoltaïque, ballon d’eau chaude thermodynamique ou système de chauffage par énergie renouvelable telle que le bois).

L’objectif de la RT 2012 est que les habitations neuves consomment au maximum 50 kWhep/m2/an\*, qui est la consommation d’énergie primaire.

Les 3 exigences globales de la RT2012 sont:

* Objectif Bbiomax (besoin bioclimatique). Il s’agit d’un indicateur de la qualité de conception et d’isolation du bâtiment;
* Objectif Cmax (consommation). Définit les exigences de consommation maximale en énergie primaire, et ceci dans 5 domaines: chauffage, refroidissement, éclairage, eau chaude sanitaire, autres;
* Objectif de confort d’été: exigence sur la température intérieure atteinte au cours d’une suite de 5 jours chauds



La certication eu-bac (European Building Automation and Controls Association) a été créée en 2003 par 25 des plus grandes entreprises internationales spécialisées dans le secteur du contrôle et de la régulation des bâtiments. Le but de l’association est de trouver des solutions de contrôle des dépenses énergétiques, ainsi que la fabrication d’éléments d’automatisation permettant d’atteindre cet objectif. Un système de certification a été mis en place par l’association, certification permettant d’assurer l’efficacité énergétique des systèmes d’automatisation du bâtiment. La principale particularité tient au fait que cette certification tient compte non seulement de l’efficacité énergétique du bâtiment au moment de sa construction, mais également tout au long de sa vie, en tenant compte de la détérioration dans le temps des systèmes de régulation et de contrôle, impactant de ce fait leur performance énergétique.

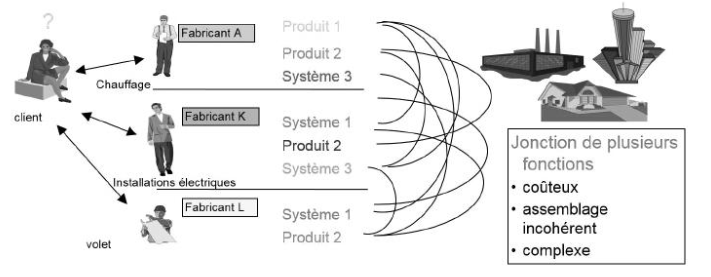
## Interopérabilité

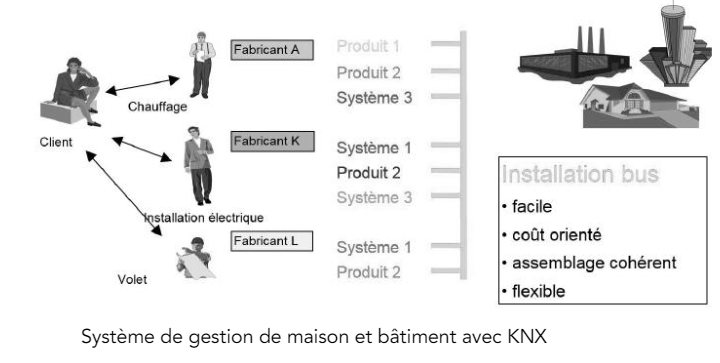
Autant dans le résidentiel que dans le tertiaire, le besoin d’interopérabilité se fait de plus en plus sentir.

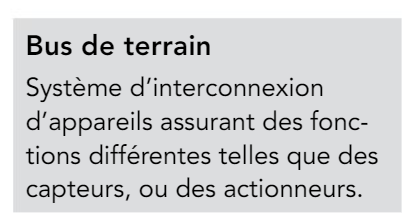
Qu’est-ce que l’interopérabilité? C’est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d’autres produits ou systèmes existants ou futurs et ce sans restriction d’accès ou de mise en œuvre.



## Notion de BUS







Les différentes technologies de bus de terrain ne sont pas facilement interchangeables. Les différences entre eux sont si profondes qu'elles ne peuvent pas être facilement connectées les unes aux autres.

## Protocole BACnet

BACnet (Data Communication Protocol for Building Automation and Control Network) est un protocole de communication de données pour la gestion technique de bâtiment (GTB). Contrairement à la plupart des autres protocoles, qui ont débuté par des implémentations propriétaires suivies de travaux de normalisation, BACnet a été développé dès le départ sous forme d’un protocole de commande et d’automation normalisé, indépendant, libre de droit et ouvert.

Le comité de normalisation était dirigé jusqu’en 2004 par des professeurs d’université, avec pour objectif d’harmoniser les types et formats de données, les primitives d’échange de données et les services applicatifs communs.

Plusieurs piles BACnet open-source sont disponibles, par exemple sur les sites http://bacsharp.sourceforge.net et http://bacnet.sourceforge.net. Le spectre des applications BACnet est très large: CVC (chauffage, ventilation et climatisation), éclairage, contrôle d’incendie et alarme, sécurité et GTB en général.

Avec LonWorks, BACnet est l’un des protocoles de commande et d’automation industriels les plus répandus, que de nombreux fournisseurs majeurs ont adopté pour leurs produits (Siemens Building Technologies, Johnson Controls, Inc., Teletrol Systems, IC, TAC, KMC Controls, American Auto-Matrix, Contemporary Controls Ltd, Reliable Controls).

### Sécurité de BACnet

Un dispositif BACnet A qui prend charge la sécurité peut demander une clé de session à un serveur en vue d’une communication future avec le dispositif B. Le serveur de clés génère une clé de session SKab et la transmet de façon sécurisée à A et à B (en la chiffrant avec les clés publiques de A et de B). BACnet met en place un chiffrement DES sur 56bits. Le dispositif A peut ensuite authentifier une transaction ultérieure avec B: A et B s’authentifient l’un et l’autre en échangeant des challenges (fondés sur des nombres aléatoires chiffrés à l’aide de la clé de session). Le message de challenge comprend l’identifiant (InvokeID) de la future transaction à authentifier. A peut également assurer la confidentialité de la future transaction en chiffrant les messages applicatifs correspondants à l’aide de la clé de session.

## Plateforme LonWorks

La suite de protocoles réseau LonWorks a été développée par Echelon Corpora-tion afin de répondre aux besoins des applications de contrôle et d’automation. Elle est à présent gérée par le groupe LonMark International.

À l’origine, la plate-forme LonWorks avait pour but de s’éloigner d’un modèle de commande centralisé propriétaire dans lequel un contrôleur central reçoit toutes les mesures fournies par des capteurs distants et envoie des commandes à des actionneurs distants. Pour supprimer le point individuel de défaillance que représente le contrôleur et améliorer l’efficacité et la puissance des systèmes de contrôle, la plateforme LonWorks définit un concept de «connexion», selon un modèle inscription/notification, qui permet aux appareils d’échanger directement des données.

Au niveau de la couche physique, la plateforme est compatible avec différents supports: paires torsadées, courants porteurs sur les lignes électriques, radio, fibre optique.

Les protocoles de la plateforme LonWorks sont parmi les plus employés dans la gestion technique de bâtiment. Echelon annonce plus de 90millions de dispositifs installés.

### SmartServer d’Echelon

Le SmartServer d’Echelon est une passerelle Internet et une plateforme logicielle locale (par exemple Edge Control Node) qui connecte LonWorks, ModBus, M-Bus et des E/S locales à d’autres dispositifs et réseaux, en plus de fournir une interface de services Web SOAP pour l’accès aux données et la configuration.

L’application DataServer permet de créer, de gérer, de supprimer et d’accéder à des points de données.

## ModBus

ModBus est une marque déposée par Modicon (groupe Schneider Electric), qui se charge également de l’actualisation de la norme.

ModBus est un protocole de messagerie de la couche application. Il apporte une communication client-serveur entre des dispositifs connectés au moyen de différents types de bus ou de réseaux.

En raison de sa simplicité, il est devenu depuis 1979 l’un des standards de fait pour les communications série à base de messages. ModBus fonctionne normalement au-dessus de liaisons RS232, RS442 point à point ou RS485 point à multipoint.

Les spécifications ModBus/TCP, publiées en 1999, définissent une couche liaison IP pour les trames ModBus. Les dispositifs ModBus communiquent selon un modèle maître-esclave: un appareil, le maître, peut initier des transactions, appelées requêtes, qui peuvent être destinées à des esclaves individuels ou à l’ensemble des esclaves. Les esclaves réalisent les actions précisées par la requête ou retournent au maître les données demandées.

### ModBus/TCP

Les spécifications de ModBus/TCP sont disponibles dans le document http://www.eecs.umich.edu/modbus/documents/Open\_ModbusTCP\_Standard.doc.

Grâce à ModBus/TCP, l’accès aux fonctionnalités de ModBus peut se faire au-dessus de TCP/IP. Chaque requête/réponse est envoyée au travers d’une connexion TCP établie entre le maître et l’esclave sur le port 502. Cette connexion peut être réutilisée pour plusieurs échanges requête/réponse.

## KNX

Association Konnex/KNX L’association Konnex (ou KNX) a été créée en 1999 par la fusion de trois associations européennes qui promouvaient le développement d’un habitat intelligent:

* BCI France (Batibus Club International) qui défendait le système Bâtibus;
* EIBA (European Installation Bus Association) qui proposait le système EIB;
* EHSA (European Home Systems Association), en Hollande, qui offrait le système EHS.

L’objectif de l’association KNX est de définir et d’offrir des services de certification pour la norme ouverte KNX, tout en proposant une prise en charge et une certification des systèmes Bâtibus,

EIB1 et EHS. Ses membres sont exclusivement des fabricants. En 2013, ils sont plus de 300, issus de 36 pays. On y trouve notamment ABB, Agilent, Bosch, Electrolux, Hager, Legrand, Merten, Moeller, Schneider, Siemens et de nombreux autres fournisseurs d’équipements domotiques et immotiques. KNX est probablement le premier écosystème au monde pour l’immotique, avec plus de 30000 partenaires travaillant dans 75 pays. La technologie KNX peut être employée gratuitement par les membres de l’association.

Il existe des spécifications pour des passerelles entre les réseaux BACnet (ISO484 annexe 5 H.5 correspondance KNX et BACnet, voir également le chapitre 4), DALI (commande d’éclairage) et KNX.

En 2013, une interface REST pour KNX a été ajoutée dans le cadre des spécifications ETSI M2M (ETSI TR 102966, section B.4). Elle facilite l’intégration des applications domotiques au bus KNX par l’intermédiaire d’une API REST indépendante du fournisseur. Une implémentation open-source de cette interface REST vers KNX/IP est disponible à l’adresse <http://cocoon.actility.com>.

L’architecture globale de KNX est une architecture décentralisée, avec des nœuds qui peuvent interagir sans passer par un contrôleur central. La pile de protocoles se fonde sur le modèle OSI, avec des couches session et présentation vides. Elle se fonde sur le travail initialement effectué pour EIB, qui est donc rétro compatible avec KNX. KNX normalise non seulement le protocole mais également le modèle de données pour la commutation, la commande d’éclairage lumineuse, la commande des stores, les valeurs entières et à virgule flottante, les pourcentages, le CVC, etc.

ZigBee

La norme 802.15.4 définit une technologie de couches physique et liaison optimisées pour les applications bas débit, avec un facteur d’utilisation cyclique faible. Toutefois, dans la pratique, les applications de capteur et de commande ont également besoin d’une couche de routage pour former un réseau maillé, ainsi que d’une syntaxe standard pour les messages de la couche application.

En 2002, plusieurs industriels ont décidé de former l’alliance ZigBee, avec pour objectif de développer les couches standard manquantes qui permettraient de créer un réseau maillé multifournisseur au-dessus des liaisons radio 802.15.4. Depuis cette date, l’alliance ZigBee a publié des spécifications pour des applications de domotique, de Smart Energy et de commande à distance.

### Sécurité dans ZigBee

Sécurité ZigBee et 802.15.4 Les réseaux ZigBee décident d’activer ou non la sécurité. Les dispositifs conformes à un profil d’application public doivent respecter les paramètres de sécurité de leur profil. Dans ZigBee, les services de sécurité se trouvent au niveau réseau (NWK) et au niveau application (APS).

### Trust Center

La distribution des clés n’est pas traitée dans la norme 802.15.4. Pour des questions de sécurité, ZigBee définit un Trust Center chargé de la distribution des clés et de la stratégie d’association.

## Z-Wave

Le protocole Z-Wave a été conçu par la société Zensys (www.zen-sys.com), basée aux États-Unis et au Danemark. Zensys est à présent une filiale de SIGMA Designs, qui fabrique des composants SoC (System on Chip) pour l’industrie du multimédia et du loisir. Zensys a commencé par proposer au marché, en 2001, un système de contrôle léger destiné aux consommateurs et a fait évoluer son produit vers un protocole réseau maillé complet pour les habitations mises en œuvre dans un SoC propriétaire. Z-Wave est rapidement devenu un protocole domotique très populaire, avec, en 2013, environ 900 produits référencés, proposés par plus de 250 fabricants. Les fonctionnalités de Z-Wave sont quasi équivalentes à celles de son concurrent ZigBee Home Automation. Mais le SoC Z-Wave étant disponible auprès d’un seul fournisseur, les problèmes d’interopérabilité entre les fabricants sont moindres car leurs produits sont souvent constitués de quelques composants externes autour de ce SoC et d’un boîtier en plastique. Par ailleurs, l’emploi du spectre inférieur au gigahertz ena fait un bon candidat au déploiement dans les bâtiments en béton, notamment en Europe.

Les fabricants d’équipement d’origine (OEM, Original Equipment Manufacturer) qui utilisent le protocole sont regroupés au sein de l’alliance Z-Wave (www.z-waveal-liance.org), dont l’objectif est de promouvoir les produits et d’organiser les forums pour développeurs et les événements de tests d’interopérabilité («Unplugfest»). Les produits Z-Wave sont certifiés par l’alliance Z-Wave à l’aide d’outils fournis par SIGMA. Ils permettent de vérifier les fonctionnalités de gestion du réseau et d’évaluer le taux d’erreur de communication (CER, Communication Error Rate) avec différentes distances. La dernière version du SoC Z-Wave date d’octobre 2013 et porte la référence SD-3502. SIGMA l’a également nommée «Z-Wave nouvelle génération (next-gen)».

### Sécurité

Dans un réseau Z-Wave, la sécurité est facultative et implémentée à l’aide des commandes de la classe Security Command. Lorsque la sécurité est présente, par exemple pour les serrures des portes, elle se fonde sur une clé secrète de niveau réseau créée au démarrage par le contrôleur principal. Cette clé est utilisée pour chiffrer les commandes sécurisées par encapsulation (security encapsulated secure command. Un dispositif qui souhaite envoyer une telle commande à un autre commence par demander un nonce au Node ID cible (au travers d’un échange de message Nonce get/Nonce report). La valeur de ce nonce, ainsi qu’un vecteur d’initialisation source généré, sont inclus dans la commande sûre de sécurité encapsulée, ce qui évite les problèmes de rejeu. Un code d’authentification du message est également ajouté afin d’éviter les manipulations. Puisque le Node ID destination est passé en clair dans une trame singlecast standard, les messages sécurisés peuvent être routés au travers de nœuds non sûrs. Une solution AES 128 est employée pour l’authentification (code d’authentification du message fondé sur un hachage Davies-Meyer) et le chiffrement. Si les premières générations de SoC Z-Wave demandaient une implémentation logicielle (d’où le peu de fournisseurs offrant la sécurité), la sécurité est aujourd’hui prise en charge de façon matérielle dans les SoC de nouvelle génération. La clé secrète du réseau est distribuée au cours de l’installation initiale: juste après l’inclusion d’un nœud sécurisé, le contrôleur principal envoie des commandes de sécurité encapsulées Key Set à ce nœud en utilisant une clé temporaire (uniquement des zéros).

## La gestion technique du bâtiment, superviseurs et hyperviseurs

Une GTB n’est pas uniquement une télécommande permettant de visualiser les états d’un bâtiment ou de les contrôler. Cela va beaucoup plus loin. Elle est par exemple capable de comprendre les différents protocoles présents, de discuter avec les uns et les autres, et bien entendu de servir d’interface ou de passerelle si vous préférez entre les uns et les autres. Elle peut se présenter soit sous la forme d’un logiciel à installer sur une machine, soit sur un système d’exploitation dédié tel que Windows, soit sur un système open source du type Linux. De plus en plus de superviseurs à l’heure actuelle tournent sur ce dernier type de plateforme.

Le superviseur peut également se trouver embarqué dans des machines de type automate, dans lesquels on va trouver, en plus de la partie logicielle, une partie hardware constituée par exemple d’entrées/sorties binaire, analogiques et digitales. Ce genre de plateforme est en général relativement limité en termes de puissance et de capacité de stockage des données. Elle utilise des systèmes d’exploitation embarqués en versions allégées tels que Windows CE. D’autres utilisent encore des versions modifiées de Linux.

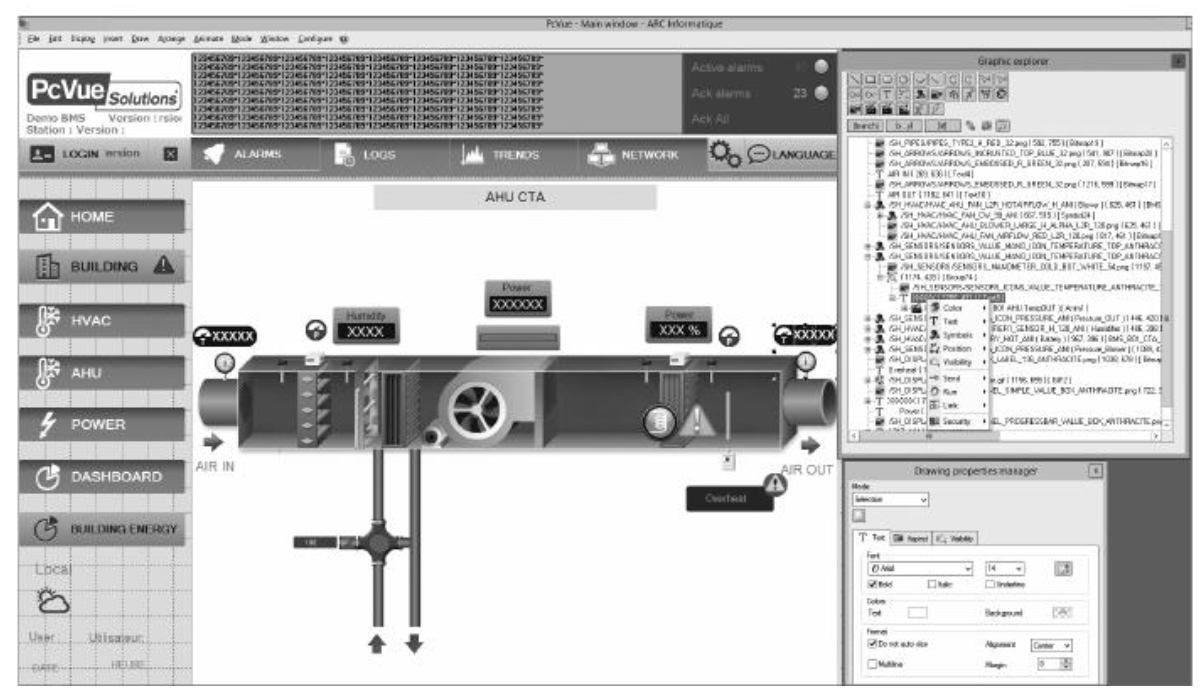
### Collecte de données

Un superviseur par définition est capable de stocker de la donnée. En fonction des capacités de stockage du disque dur et de la quantité de données qu’il stocke en permanence, il est capable de stocker plusieurs années.

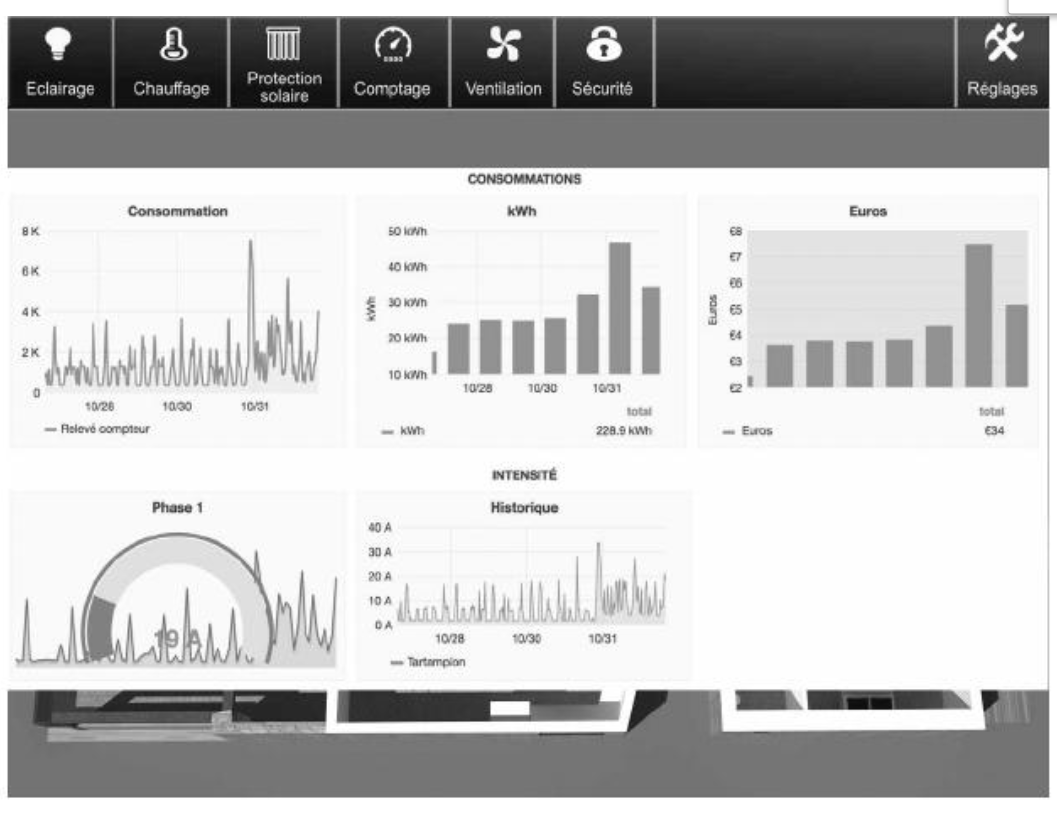
### Interface utilisateur

Les interfaces utilisateur, ce que l’utilisateur voit sur son écran et lui permet d’interagir avec l’installation, ont beaucoup évolué ces dernières années. Alors que dans le tertiaire les visualisations restent relativement techniques, à l’ergonomie limitée et esthétiquement très sommaire, on assiste cependant à une évolution vers des interfaces utilisateur au design plus recherché, et avec une ergonomie qui s’améliore de plus en plus. À l’heure actuelle, les interfaces web sont de plus en plus utilisées.





### Tableaux de bord énergétiques



### Surveillance d’installation

Le superviseur peut être utilisé dans le cadre de la surveillance des installations. Il peut par exemple vérifier que les différents périphériques supervisés sont bien présents et répondent à des requêtes envoyées toutes les x minutes. Ils peuvent également envoyer des alertes visuelles (texto, email, notification push) aux utilisateurs concernés par ces alertes dans les cas où une intervention humaine rapide est requise.

### Accès à distance sécurisé

Un accès à distance sécurisé ne se fait pas uniquement à travers un superviseur. Un simple tunnel VPN\* permet d’accéder de manière simple et sécurisée à une installation distante, sans avoir besoin du moindre ordinateur sur place. En revanche, l’accès à certains logiciels présents uniquement sur la machine de supervision ne pourra pas forcément se faire de la même façon.

### Hyperviseurs pour supervision multisite

L’hypervision consiste à superviser plusieurs sites pouvant être très éloignés les uns des autres à partir d’une interface utilisateur unique et commune.

### Multiprotocole

Un des principaux intérêts des superviseurs est leur capacité à intégrer d’origine la gestion de plusieurs protocoles de communication, ou de protocoles de bus de terrain. Que ce soit du RS485, du RS232, de l’IP ou encore KNX, M-Bus, Modbus ou Bacnet, de nombreux superviseurs supportent ces protocoles, et ont été développés pour être interopérables avec eux. L’intérêt est que le superviseur peut alors servir de «passerelle» entre 2 ou plusieurs autres protocoles. On évite alors l’achat de passerelles de communication spécifiques, puisque c’est le superviseur qui les gère.