SMART BUILDING : L'ESSENTIEL

Des automates programmables à l'intelligence artificielle

Jean-Pierre Arnaud

Editions
LE MONITEUR

Avant-propos

À la fin des années 1980, le terme « immeuble intelligent » devient un incontournable du marketing de la modernité : plusieurs sociétés se créent autour de l'idée d'une alliance des entreprises de la construction et de l'informatique[1]. Il ne s'agit pourtant, en ces débuts, que de vendre le principe d'un système de câblage universel et d'installer une pratique essentielle pour les industriels des réseaux et des télécommunications. C'est ainsi que les années 1990 ont vu une croissance d'immeubles que, à la faveur de la généralisation des micro-ordinateurs, on pouvait à bon droit qualifier de communicants ou de précâblés. La recherche d'une meilleure productivité tertiaire, grande affaire de ces années, a alors conduit à une forte structuration des systèmes d'information autour du câblage des bâtiments et des réseaux locaux : le premier bloc de l'immeuble intelligent, l'*Information Technology* (IT) recevait ainsi rapidement la forme qu'il prend encore aujourd'hui tout en ayant suivi la constante évolution des technologies qui le constituent.

La structuration d'ensemble des systèmes technologiques qu'abrite ou requiert le bâtiment n'était toutefois pas achevée. Les acteurs les plus inventifs s'aperçurent rapidement que l'on pouvait aller plus loin si l'on ne se limitait pas aux réseaux et si l'on s'intéressait aux autres technologies plus ou moins avancées déjà présentes dans le bâtiment. En profitant de l'ubiquité des terminaux de l'IT, on pouvait ainsi fournir de nouveaux services aux occupants comme aux gestionnaires pour maîtriser leur environnement, leur confort ou réaliser de substantielles économies. Il fallait pour cela interconnecter les différents systèmes gérant l'immeuble, au premier rang desquels la gestion technique centralisée (GTC) mais on pouvait aller plus loin avec le contrôle d'accès, la sécurité, etc. Le deuxième bloc, celui de l'*Operational Technology* (OT) recevait ainsi sa définition et le bâtiment n'était plus seulement un bâtiment connecté ou communicant, mais un bâtiment fournissant des services, soit un bâtiment intelligent ou encore un « *smart building* ».

Dans les années 1990, réaliser un tel objectif nécessitait un grand savoir-faire, faute de normes publiquement disponibles et de produits industriels : les ingénieries qui se sont engagées sur cette voie devaient convaincre de la faisabilité et le plus souvent réaliser des développements sur mesure pour faire dialoguer les systèmes de tous les fournisseurs.

Les années 1990 furent celles de la recherche d'une rationalisation de ce paysage fragmenté, mais ce ne fut qu'avec les années 2000 que le versant OT a trouvé une

(1) L'auteur de l'ouvrage est de ceux qui ont eu l'idée, dès 1987, de créer une filiale d'IBM et de Bouygues, IB2 Technologies se consacrant à la conception d'immeubles précâblés et qui devait très vite compléter son offre avec des prolongements multimédia, puis des services utilisateurs s'appuyant sur les GTC du marché et des conceptions de centres informatiques anticipant sur les *data centers* d'aujourd'hui.

structuration comparable à celle de l'IT et qu'il est possible de fournir une description cohérente d'un immeuble fournisseur de services.

La cohérence n'est toutefois pas synonyme de facilité car en intégrant des services extrêmement variés le concepteur d'un tel bâtiment doit coordonner le travail de corps de métiers très différents (de l'informatique aux aménageurs ou aux services de maintenance immobilière, par exemple) et se confronter à des technologies très diverses (des réseaux à la thermique, des automates aux bases de données…). Il faut alors une expertise dans les domaines spécifiques au projet (comme les réseaux de terrain), mais aussi dans les domaines applicatifs concernés (organisation des services de gestion et maintenance, thermique du bâtiment, éclairage, etc.).

Enfin, les années 2000 ont amené pléthores de solutions intégrées parmi lesquelles choisir. Le tout dans un contexte où des exigences nouvelles sont apparues pour lesquelles l'immeuble intelligent est clairement un élément clé, sinon décisif : impératif écologique ou télétravail entre autres. Si l'on ajoute à cela les technologies qui continuent à se renouveler (intelligence artificielle notamment) et les risques qu'on leur associe avec le lot de réglementations et de contraintes législatives qui en résultent, la tâche d'un chef de projet ou d'un maître d'œuvre peut paraître impossible.

On ne peut raisonnablement prétendre à une expertise sur l'ensemble des technologies, mais le pari de cet ouvrage est qu'il est possible de parvenir à une maîtrise suffisante pour faire des choix, en superviser la mise en place des différents systèmes, et définir une trajectoire pour un immeuble fournisseur de services en assurant une pérennité des investissements nécessaire à cette fin.

Plutôt qu'une tentative illusoire de tout savoir sur tout, l'objectif des pages qui suivent est donc d'atteindre une connaissance suffisante pour guider les spécialistes de domaines très divers auxquels on fera appel, pour apprécier les limites des offres sur le marché et ainsi aboutir à une vision d'ensemble du souhaitable et du réalisable. Entre le savant qui sait tout sur (presque) rien et l'essayiste qui ne sait rien sur (presque) tout, on a tenté de se maintenir sur une ligne de crête qui permette au décideur de faire des choix lucides sans obérer l'avenir, et au stratège de définir une voie réaliste vers un futur souhaitable. Ce sera au lecteur de juger de la réussite de cette tentative car il serait inutile de dissimuler l'insatisfaction probable des spécialistes de chacun des domaines concernés. Un exposé théorique devient vite abscons lorsqu'on ne connaît pas les raisons qui ont amené à l'état de l'art actuel : même si un haut degré d'abstraction eût flatté l'universitaire, on a fait le choix de partir à chaque fois d'exemples simples, pour en extraire les concepts clés : cette approche m'a souvent conduit à faire l'historique d'une évolution qui explique les difficultés et parfois les impasses ou les incohérences auxquelles nous sommes confrontés aujourd'hui.

La lecture de cet ouvrage ne nécessite ainsi aucune connaissance préalable mais demande parfois l'effort de ne point reculer devant l'exposé un peu précis des technologies dont l'alliage permet la conception du bâtiment intelligent.

Cet ouvrage, comme un cahier des charges bien conçu, définira des objectifs avant de décrire les technologies et la méthode pour choisir solutions et intervenants.

Le premier chapitre, à partir d'un exemple simple universellement utilisé, le thermostat, permet d'extraire les concepts clés d'une régulation d'immeuble et explicite la nécessité d'un recours au numérique. Il tente d'approcher une définition de l'immeuble intelligent : approche et non définition catégorique car on y verra qu'une définition « *ex cathedra* » est impossible, voire peu souhaitable.

Les deux chapitres suivants sont les plus technologiques, et sans doute les plus difficiles. Ils mettent en place les notions essentielles d'une architecture réseau, en donnent les composantes et montrent la mise en œuvre dans les deux domaines clés : les technologies de l'information (IT) et celles des opérations (OT). Les premières visent la transmission de l'information, les systèmes de câblage et la structuration des réseaux locaux au bâtiment. Les secondes visent, en tenant compte des acquis de la première, les technologies de la régulation et du pilotage des services offerts. Le lecteur que rebutent les exposés techniques pourra esquiver en première lecture le plus gros de ces chapitres et se limiter aux paragraphes 3.4.5 et 3.4.6 : il y perdra toutefois l'essentiel des informations qui lui permettront une appréciation plus critique des technologies en présence, de leurs limites, avantages et incompatibilités. Il lui sera toujours possible d'y revenir quand la lecture de la suite l'aura familiarisé avec la terminologie nécessaire. Il pourra alors s'appuyer sur des connaissances plus complètes pour mieux évaluer la réelle valeur des innovations proposées par les différents acteurs.

Le chapitre 4 s'intéresse à la distinction entre systèmes fermés (ou « propriétaires ») et système ouverts, distinction cruciale pour l'évaluation de la pérennité de l'installation et pour une appréciation de la rentabilité des investissements réalisés.

Le chapitre 5 montre comment les technologies de l'OT, décrites comme elles sont apparues et donc de façon éparse au chapitre 3, ont été placées dans un cadre architectural qui a permis la définition d'un contexte réglementaire avec les décrets BACS et tertiaire en France. De ce cadre découle également la mise en place de labels et de référentiels utiles aux décideurs.

Le chapitre 6 montre comment l'IP, au-delà de son rôle de standard pour Internet, tend à devenir un standard pour l'ensemble des technologies numériques dans le bâtiment. En favorisant l'échange de données de plus en plus massives, en reposant sur la multiplication des objets connectés, il amène inéluctablement à un recours à l'intelligence artificielle (IA). On en approchera les limites et les conditions nécessaires, mais non suffisantes, pour une bonne intégration.

Le chapitre 7 s'intéresse à une conséquence de la montée en charge des communications numériques et du partage de données : les questions de cybersécurité deviennent aussi importantes pour l'OT que pour l'IT. On se demandera si le niveau de protection nécessaire en ce domaine est atteint et quelles sont les technologies à mobiliser pour faire face aux attaques.

Au-delà des techniques de sécurité, le chapitre 8 revient sur la gestion du risque dans un environnement plus conflictuel que jamais, et sur la dépendance aux technologies : des approches résilientes sont présentées.

Enfin, en conclusion, une approche de la définition et de la conduite du projet tenant compte des informations de l'ensemble des chapitres précédents est proposée. La connaissance des technologies actuelles permet également de tenter une sélection des évolutions les plus prometteuses : la *blockchain* et les *smart grids* sont de celles-ci et nécessiteront de nouveaux efforts de formation et d'information du public.

Bien que l'ensemble du texte soit destiné prioritairement au lecteur français, nombre de technologies et de concepts sont d'origine anglo-américaine : on leur a fait la place qui leur revenait, ainsi qu'aux exemples de réalisation, en privilégiant néanmoins l'existant et le disponible en France.

Plusieurs marques ou noms de produits sont mentionnés : dans ce domaine, il est d'ailleurs souvent difficile de les distinguer d'un standard ou d'une norme. On gardera néanmoins présent à l'esprit qu'il ne s'agit que d'exemples illustrant la réalité et la disponibilité des technologies présentées : ils aideront néanmoins à trouver le point de départ d'une recherche plus exhaustive et d'autant plus nécessaire que toute information de ce type devient obsolète dès le jour de sa communication.

À propos de l'auteur

Jean-Pierre Arnaud a commencé sa carrière dans la recherche en télécommunications au laboratoire européen d'IBM à La Gaude. Chargé de l'introduction en France des réseaux locaux et du premier système de câblage d'établissement, il en dirige les équipes marketing. Son travail l'amène ainsi à s'intéresser au domaine en émergence que l'on appelle alors le bâtiment intelligent : il fait ainsi partie de ceux qui créeront la société IB2 Technologies, première dans le domaine dès 1987.

Ces expériences l'ayant sensibilisé aux problèmes de formation posés par les nouvelles technologies, il devient titulaire de la chaire de Réseaux au Cnam (Conservatoire national des Arts et Métiers). Dans ce cadre, il participera à la création d'un Institut de la Transformation Numérique des entreprises (avec le Cigref – Club informatique des grandes entreprises françaises) ainsi qu'à celle de programmes portant sur la cybersécurité.

Il est également consultant auprès de grandes entreprises et institutions ce qui lui permet de participer à de nombreux projets dans des secteurs divers : des équipementiers (Alcatel, Nortel, Cisco…), des fournisseurs et éditeurs de contenus (TF1, Presse quotidienne régionale…), des opérateurs (Bouygues Télécom, 9 Telecom…), des utilisateurs (universités, collectivités territoriales, sièges sociaux…).

Auteur de nombreux articles dans des publications professionnelles, son travail est reconnu par plusieurs distinctions (chevalier dans l'ordre national du Mérite, officier dans l'ordre des Palmes académiques), il est ingénieur de l'ENST (École nationale supérieure des télécommunications), docteur es lettres et diplômé de l'IAE (Institut d'administration des entreprises).

CHAPITRE 1

L'immeuble « intelligent » ou smart building : de quoi s'agit-il ?

En parcourant un *smart building*, on doit avoir l'impression qu'il comprend les besoins avant même qu'ils ne soient exprimés et que chaque composant est connecté et travaille de concert avec les autres pour optimiser confort, sécurité et efficacité. Comme le feraient des entités vivantes, dynamiques et réactives.

Commençons par étudier un automatisme des plus simples pour mettre en évidence les composantes sous-jacentes des technologies nécessaires au bon fonctionnement d'un immeuble intelligent.

En en recensant les limites, les imperfections et les contraintes, nous pourrons aussi comprendre comment les surpasser et pourquoi l'interconnexion et la communication entre les technologies s'est avérée indispensable et que leur présence dans l'immeuble est le signe distinctif qui caractérise l'immeuble intelligent aujourd'hui.

1.1 Un peu de mécanique…

Le chauffage voire le confort thermique représentent le premier poste de dépense énergétique du bâtiment, il est donc naturel de se tourner vers le dispositif qui permet de le contrôler tout en gardant un niveau de confort acceptable.

Un **thermostat** a pour objectif de maintenir une température stable dans l'environnement qui l'accueille, et d'éviter les consommations inutiles. Dans sa version la plus élémentaire, on peut songer au thermostat équipant un corps de chauffe (convecteur, par exemple) et l'activant ou le désactivant pour maintenir une température approximativement constante.

En décrire sa constitution et son fonctionnement va nous permettre de mieux comprendre et les briques de base qu'il faudra reprendre dans le contexte plus

général de la gestion technique des bâtiments (GTB), puis à plus grande échelle du *smart building*.

Dans le cas d'un corps de chauffe électrique, la régulation la plus simple sera réalisée en coupant son alimentation lorsque la température requise est atteinte.

Le **thermostat bilame** est fréquemment utilisé. Son fonctionnement est basé sur l'expansion et la contraction de deux lames métalliques de coefficients de dilatation thermique différents. Ces lames sont soudées ensemble, ce qui fait qu'elles se courbent dans des directions opposées lorsque la température change.

Lorsque la température autour du thermostat change, les métaux des deux lames se dilatent ou se contractent différemment en raison de leurs coefficients de dilatation thermique distincts. Par conséquent, les lames se déforment et se courbent dans des directions opposées.

Cette déformation des lames provoque un mouvement mécanique, généralement utilisé pour ouvrir ou fermer le circuit électrique. Lorsque la température baisse en dessous du réglage du thermostat, les lames se courbent dans un sens, ce qui peut actionner un contact électrique pour activer le chauffage (fig. 1.1). Lorsque la température atteint la valeur désirée, les lames se courbent dans l'autre sens, ce qui coupe l'alimentation électrique au chauffage.

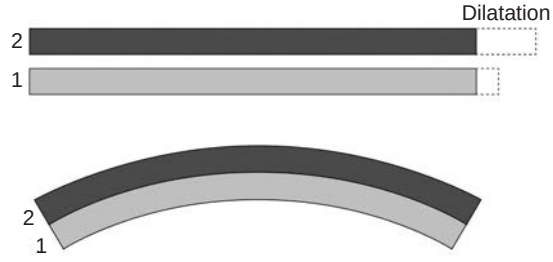

Fig. 1.1 – Effet de la dilatation thermique
(source : Kanthal Thermostatic_Bimetallic Handbook)

Sur la base de ce principe, il est aisé de construire un thermostat pilotant l'alimentation d'un radiateur électrique (fig. 1.2).

Ce thermostat souffre néanmoins d'un inconvénient majeur : la température à laquelle se ferme le contact est fixée par la structure physique du bilame et non par une consigne donnée par l'utilisateur, il est donc approprié à la construction d'un disjoncteur thermique, mais non à celle d'un thermostat régulant le chauffage.

Pour le rendre réglable, il faut lui adjoindre un cadran. Situé sur le boîtier de l'appareil, il peut être gradué en degrés Celsius ou Fahrenheit. En le tournant dans le sens horaire ou antihoraire, l'utilisateur sélectionne une température de consigne.

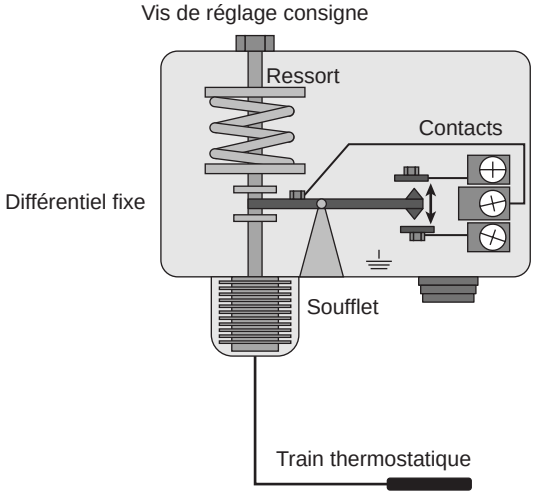

Fig. 1.4 – Thermostat à bulbe
(source : ABC clim)

1.2 Des blocs fonctionnels

Procédons à une analyse conceptuelle des fonctions réalisées dans ce thermostat pourtant très simple. On y distinguera :
– Une saisie de **l'information** température : le bulbe, le train thermostatique, la conception même du bilame capture cette information. Cette fonction de capture sera généralisée dans l'immeuble intelligent et on parlera donc de **capteurs** qui auront cette mission, quelle que soit la technologie utilisée, laquelle ne nous intéressera plus par la suite en tant que telle. On parlera de sonde thermique pour la température, mais bien d'autres informations pourront être saisies par le capteur : présence, mouvement, humidité, compteurs, pression… À un certain niveau d'abstraction, par exemple dans le standard BACnet, les objets du monde physique seront représentés par un ensemble de données (température actuelle, température de consigne, plage de variation pour un thermostat) qui définiront l'objet virtuel dont aura connaissance le personnel, le logiciel, le système, l'algorithme, ou de futures entités qui nous restent à imaginer !
– En fonction de **la consigne**, le thermostat activera le corps de chauffe en permettant son alimentation. Plus généralement, celui qui active sera désigné sous le nom d'**actionneur**.

Dans notre exemple, capteur et actionneur sont intégrés en un seul ensemble, mais rien ne l'impose et, dans un bâtiment moderne, ils seront fréquemment dissociés pour des fonctionnements plus sophistiqués tenant compte, par exemple, d'un capteur de la température extérieure.

Dans d'autres domaines comme la sécurité et le contrôle des accès, cela peut impliquer un capteur détectant une présence et envoyant cette information à un centre sécurité, provoquant une alarme, ainsi qu'une commande d'éclairage de la zone concernée.

La régulation de la température s'opère à l'aide d'une consigne liée à une action mécanique ponctuelle. Cette constitution, très fruste, ne convient pas dès que l'on s'intéresse à un bâtiment où l'on voudrait agir depuis un local de gestion, voire à distance pour la gestion d'un parc. Il faudra alors rassembler les informations nécessaires à la prise de décision et à la gestion, et intégrer ce que l'on appelle une **gestion centralisée du bâtiment** ou **gestion technique centralisée** (GTC).

Si les capteurs et actionneurs sont interconnectés en réseau, certaines actions peuvent être effectuées sans faire intervenir le personnel de maintenance, lequel n'interviendra que pour modifier les consignes ou pour gérer des exceptions. L'ensemble n'étant plus centralisé, il sera alors désigné sous le terme générique de **gestion technique du bâtiment** (GTB).

Le thermostat mécanique décrit précédemment n'est pas en mesure de fournir ces informations puisque son fonctionnement est purement local et que les thermostats fonctionnent indépendamment les uns des autres.

Il sera donc nécessaire de placer l'ensemble des capteurs et actionneurs sous le contrôle d'une **supervision** qui assurera le fonctionnement et informera les responsables de l'état du bâtiment tel que reflété par les capteurs. Si, par le passé, on avait recours à des tableaux de pilotage calqués sur les postes de commande des sites industriels, la fonction est aujourd'hui assurée par un logiciel de supervision.

REMARQUE

Sur le modèle des systèmes d'exploitation d'ordinateurs (*Operating Systems,* OS), on ira jusqu'à parler de *Building Operating System* (BOS) : nous y reviendrons dans la suite cet ouvrage.

À partir d'une analyse quasi phénoménologique d'un dispositif simple, nous avons donc été conduits à distinguer les grands blocs fonctionnels nécessaires à la conception d'un immeuble « intelligent » :
– des **capteurs** saisissant des informations de toute nature allant en se diversifiant au fur et à mesure de la découverte des besoins des utilisateurs et des gestionnaires ;
– des **actionneurs** pilotant les dispositifs mis en place ;
– un ou des **réseaux** permettant de gérer les flux d'information entre capteurs, actionneurs et logiciels surtout s'ils sont mis en place dans des locaux différents et distants parfois de plusieurs centaines de mètres ou plus.
– un ou des **logiciels** automatisant la prise de décision et permettant l'information et l'intervention pertinente des personnels.

Prenons maintenant l'exemple d'un capteur détectant une présence pour appréhender la complexité des réseaux, de leur câblage et de leur nécessaire flexibilité.

Dans un système orienté commande, un capteur est relié directement à une ampoule d'éclairage (fig. 1.5).

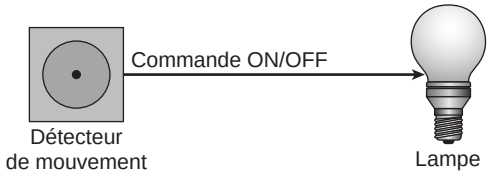

Fig. 1.5 – Système orienté commande (maître/esclave)

Dans cette approche, typique d'une orientation maître (le détecteur) - esclave (la lampe), la décision d'extinction ou d'allumage de la lampe est prise par le **détecteur**. Suivant ce modèle, chacune des lampes du bâtiment devra alors être connectée à son détecteur. On imagine aisément le volume de câblage, la complexité qui en résulte, et le coût, proportionnel au nombre d'équipements.

On peut aussi vouloir utiliser cette commande pour une autre fonction : par exemple, la sécurité des accès. Il faudra alors modifier le détecteur pour qu'il envoie la même information à la lampe et à l'alerte sécurité (fig. 1.6). Cet ajout engendrera forcément des coûts en multipliant les interconnexions.

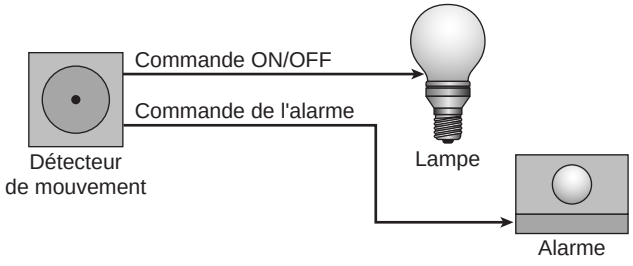

Fig. 1.6 – Système orienté commande : diffuser l'information

1.3 Des données

Semblable en cela à un organisme vivant, et dûment protégé par son enveloppe, le bâtiment n'a jamais été coupé de l'apport des fluides qui lui sont essentiels : **air**, **énergie** (gaz, chauffage ou électricité), **eau**. Comme nous l'avons vu, une bonne part des principes architecturaux visent à assurer la distribution de ces trois fluides essentiels à son « maintien en vie ».

Absorbant et rejetant les fluides après usage et traitement, le bâtiment est semblable en cela à un corps animal : pas plus que celui-ci il ne peut se passer d'un cerveau et

d'un système nerveux, et c'est sans doute en cela que peut se justifier la notion d'un bâtiment « intelligent ».

Ce que traite le cerveau et ce que distribue le système nerveux, c'est le quatrième fluide l'immeuble : **la donnée**.

En y regardant de plus près, on a distingué le système périphérique constitué des capteurs et actionneurs reliés entre eux par les « nerfs » du réseau de terrain. Le système central, supporté par la couche logicielle, collectera les données pour information et prise de décision puis communiquera *via* des connexions directes avec les réseaux de terrains ou indirectement *via* les organes effecteurs que sont les automates et stations intermédiaires (fig. 1.7).

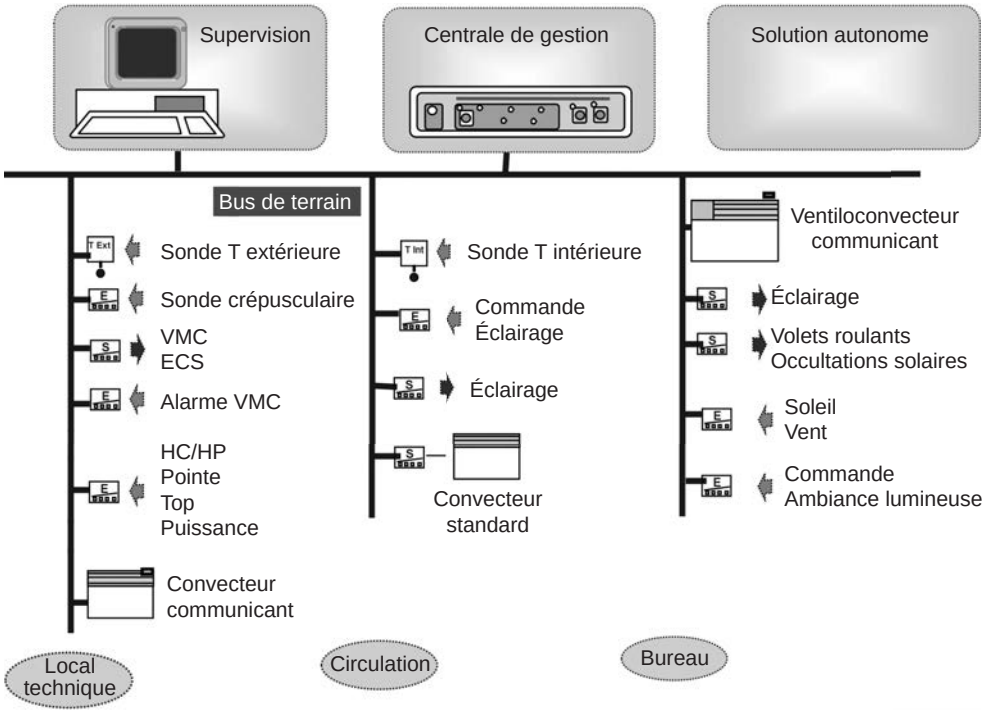

Fig. 1.7 – Système de gestion du bâtiment : une vue simplifiée

En allant au plus simple l'organisation de ce système nerveux pourra donc incorporer des organes effecteurs comme une centrale de gestion, des organes sensitifs comme un logiciel de supervision, et des terminaisons sensibles (capteurs) et motrices (actionneurs). Dans une perspective de rénovation, on aura aussi à prendre en compte les éventuels systèmes autonomes qui ne contrôlent que des fonctions spécifiques du bâtiment.

compréhension des données, ontologies permettant la liaison des données, complétude, règles sémantiques assurant la cohérence (des unités employées, des attributs de chaque donnée…), etc. L'objectif, identique à celui du SI, est d'assurer une vue globale du bâtiment, de ses caractéristiques matérielles et immatérielles et évitant les « silos » d'information non communicants et incompatibles entre eux. Il a fallu des décennies aux SI avant de parvenir à la maturité, bien malin qui saurait dire combien de temps il faudra au BIS pour parvenir au même résultat.

La **démarche BIM** est une évolution naturelle des outils de la construction : on fait des plans (numériques), on construit puis on implante les équipements. La nouveauté apportée par le BIM est d'adjoindre aux plans toutes les données pertinentes (identification de locaux, circulation des divers réseaux, points de connexions…). Le tout est consolidé en un ensemble de données structurées, mémoire du bâtiment numérisé. La gestion du pilotage et de l'automatisation est alors simplifiée et se borne à connecter les informations reçues en temps réel au dispositif identifiés sur le BIM. Ceci est d'autant plus facile que les données sont dotées, dans la maquette BIM, d'une « ontologie » : typage des données et de leurs relations décrites dans un langage partagé et connu de tous les fournisseurs et intervenants. La démarche est inverse de celle qui part du logiciel d'exploitation : décrite précédemment (voir § 3.5), elle consiste à implanter les capteurs/actionneurs, le logiciel et à lancer celui-ci qui envoie des trames d'interrogation pour recenser les objets connectés et ce n'est qu'à la fin que l'on positionne l'ensemble du dispositif sur un fond de plan (voir § 3.4).

La démarche BIM peut donc être considérée comme plus proche d'un processus constructif :

$$\text{Plan} \rightarrow \text{implantation} \rightarrow \text{communication}$$

La démarche GTB se présentant comme un processus basé sur le réseau :

$$\text{Implantation} \rightarrow \text{communication} \rightarrow \text{plan}$$

Reste qu'il faut assurer la compréhension par le logiciel des données issues des différents composants. Une ontologie standardisée et reconnue de tous assurerait cette compréhension : nous n'en sommes pas (encore ?) là, même si plusieurs propositions visent cet objectif. Le problème est bien connu des ingénieurs en système d'information : plutôt que le logiciel de gestion de données soit équipé d'autant d'interfaces logicielles qu'il y a de sources de données, Ils ont forgé la notion de « middleware » (logiciel du milieu). Au lieu de s'adresser directement au logiciel de gestion, les sources de données envoient celles-ci au seul middleware qui les traduit en les envoyant au logiciel de traitement. Celui-ci n'a plus besoin de traduire les données qui le sont par le middleware, chaque source de données n'ayant, de son côté, à connaître qu'un seul format, celui du middleware.

La diversité des formats des données du bâtiment autorise à penser que le concept de middleware y est également intéressant.

Les informations collectées sur le bâtiment pour son exploitation sont source de valeur et les laisser inexploitées représenterait une perte dommageable, surtout quand l'on considère la durée de vie du bâti et qu'on la rapporte à celle, incomparablement plus courte, des équipements numériques qui les collectent et les conservent.

Qu'il s'agisse de les consolider au sein d'un BIS puis de les exploiter, ou d'aller les chercher sur les différents systèmes dont elles sont issues, un logiciel, de portée plus large que celle de la GTB ou BACS est nécessaire. D'où l'émergence depuis 2015 d'un nouvel acronyme, le **BOS** (*Building Operating System*). Il est destiné à consolider l'ensemble des logiciels du bâtiment, y compris certains de ceux du SI – on peut penser à un logiciel de réservation de salles : il est intéressant de remarquer que la société française créatrice du terme (Spinalcom) présentait son logiciel Spinalcore comme un middleware avant de le requalifier en BOS.

La démarche BIM est naturelle et est avantageuse pour la documentation, la maintenance et l'évolutivité. Le parc immobilier étant essentiellement composé de bâtiment existant, on peut se demander s'il est nécessaire d'entreprendre une reprise des plans existants pour les mettre au niveau BIM pour bénéficier de tous ces avantages. Une ontologie peut être créée en s'appuyant sur les plans – qui seront nécessaires et existent le plus souvent. Elle sera basée sur une hiérarchie structurée, par exemple :

Bâtiment → étage → local ou bureau → composants

Un middleware assurant la communication entre les composants et le logiciel. Nombre d'éditeurs de logiciel GTB (Siemens ou Honeywell par exemple) en proposent, en complément, un middleware. Cette approche, quoique simplifiée, permet souvent d'atteindre des résultats comparables à ceux obtenus avec une approche intégralement BIM, faute d'une ontologie BIM universellement acceptée par tous les fournisseurs, même si plusieurs initiatives sont actuellement en cours d'élaboration sans qu'aucune d'entre elles puisse aujourd'hui prétendre à une maturité dominante sur le marché. On peut citer SBOnto (*Smart Building Ontology*), BOT (*Building Topology Ontology*) proposée par le consortium WEB W3C ou le projet open source Haystack.

En 2025, cette pluie d'acronymes alimente les colloques sur les bâtiments intelligents. Si jumeau numérique et BIM sont largement adoptés au plan international, BIS et BOS, bien que l'acronyme soit de langue anglaise, sont d'origine française et il est encore trop tôt pour affirmer qu'ils seront repris internationalement.

CHAPITRE 7

L'impact des crises et les risques du XXIe siècle

De multiples crises ont affecté un siècle de plus en plus incertain, certaines ont eu un impact positif sur notre secteur, d'autres ont eu un effet négatif. Essayons de profiter du premier, en limitant l'effet du second.

7.1 Crise énergétique, crise sanitaire, crise climatique : une nouvelle génération de labels

Depuis le XXe siècle, de multiples crises énergétiques ont provoqué une hausse des coûts d'approvisionnement (choc pétrolier et guerre en Ukraine notamment).

La crise climatique, et la prise de conscience de la part importante du secteur du bâtiment dans les émissions de gaz à effet de serre (plus de 20 % selon le ministère de l'écologie en France) ont amené les pouvoirs publics à offrir des aides financières à la mise en place des systèmes de GTB, et à définir ou favoriser des labels d'excellence environnementale qui dynamisent la demande.

La crise sanitaire liée au Covid a également joué un rôle en renforçant l'usage du télétravail et en en amenant à une prise de conscience de l'importance du contrôle de la qualité de l'air. Les BACS ne répondent pas à eux seuls à ces enjeux – les matériaux de construction ou les systèmes de ventilation par exemple sont cruciaux –, mais ils contribuent positivement à la résolution des problèmes soulevés. Nombre de bâtiments intelligents recherchent, et souvent obtiennent, la certification par des labels environnementaux, parmi lesquels on peut citer :

– En France le label HQE (Haute Qualité Environnementale) est attribué par CERQUAL et Certivea. La certification peut être attribuée dans d'autres pays.

– LEED (*Leadership in Energy and Environmental Design*) a été créé par le U.S. Green Building Council (USGBC) en 1998. En 2024, on compterait, selon

l'USGBC, 111 397 projets LEED certifiés dans le monde, dont 268 projets en France. (source : https://www.usgbc.org/projects).
– BREEAM créé en 1990 par le Building Research Establishment au Royaume-Uni, BREEAM est l'une des premières méthodes d'évaluation de la durabilité des bâtiments. Plusieurs centaines de milliers de bâtiments seraient certifiées dans le monde.

Ces certifications sont surtout centrées sur la performance énergétique et les services aux usagers. Centré sur la santé physique et mentale des usagers, on peut également mentionner :
– WELL développée en 2014 par l'IWBI (International WELL Building Institute) qui prend en compte qualité de l'air, de l'eau, confort acoustique, environnements qui soutiennent la santé mentale et le bien-être émotionnel… Selon l'IWBI, il y aurait dans le monde 13 059 projets certifiés, dont 119 en France (source : https://account.wellcertified.com/directories/projects/).

Les méthodologies adoptées pour l'attribution des labels sont presque routinières : fourniture des documents de conception ou de réalisation, évaluation au regard des critères et attribution d'une note d'ensemble ou d'un niveau de qualité par une moyenne pondérée sur les différents critères.

7.2 Géopolitique et criminalité : questions de cybersécurité

Il y a fort longtemps, l'attention des professionnels aurait pu être attirée par deux incidents :
– En 2013 Fazio Mechanical Services, prestataire de services chargé de la maintenance des systèmes de chauffage de Target (plus grosse entreprise de distribution aux USA), s'est fait voler les identifiants d'accès au réseau de Target par une classique attaque cyber de *phishing*. Une fois les identifiants récupérés, les attaquants ont accédé au réseau interne de Target. Ils ont exploité des failles dans la segmentation réseau, ce qui leur a permis de se déplacer latéralement jusqu'aux systèmes de point de vente. Environ 40 millions de cartes bancaires et les données personnelles de 70 millions de clients ont été compromises. On estime que Target a subi des pertes directes et indirectes, estimées à plus de 162 millions de dollars pour les indemnisations, la mise à jour des systèmes et la gestion de la crise.
– En 2017, un rançongiciel (ransomware) a neutralisé le système de sécurité du Romantik Seehotel Jägerwirt, établissement quatre étoiles situé dans les Alpes autrichiennes. Cette attaque a désactivé le dispositif de clés électroniques, empêchant les vacanciers d'entrer ou de sortir de leur chambre. Cette attaque perpétrée à plusieurs reprises, a amené la direction à payer la rançon exigée et même semble-t-il, à désactiver le système électronique et son pilotage pour le remplacer par des clés classiques.

Dans les deux cas, des prescriptions de cybersécurité, aujourd'hui usuelles, n'avaient pas été respectées : contrôle d'accès aux applications et entre les réseaux, voire isolation physique entre réseaux assurant des fonctions sans relations entre elles, chiffrement des communications sensibles, protection antivirus, etc.

La cybercriminalité est aujourd'hui un phénomène reconnu et en expansion constante. Les délinquants bénéficient de l'accès par Internet aux systèmes et de véritables « kits » d'attaque de faible coût et sont faciles à se procurer sur des magasins du « dark web ». Même organisés en véritables associations mafieuses, les malfaiteurs n'ont toutefois que des moyens limités comparés à ceux des états qui luttent et répriment leurs agissements : plus inquiétant toutefois, dans un paysage marqué en 2025 par une conflictualité jamais vue, il apparaît clairement que certains états cherchant à déstabiliser les institutions d'un autre pays mettent leurs importants moyens au service d'attaques de plus en plus sophistiquées.

Nous sommes entrés néanmoins dans une ère de conflictualité telle que les états protecteurs se transforment parfois en agresseurs dotés de moyens sans commune mesure avec ceux des délinquants.

Ces phénomènes ont pris une telle importance que l'état français a établi avec l'ANSSI (Agence nationale de la sécurité des systèmes d'information) une liste d'OIV (Opérateurs d'importance vitale), organisations et entreprises ayant des activités importantes pour la Nation (information, alimentation, gestion de l'eau, nucléaire, établissements de santé, etc.). Ces OIV doivent, en particulier, mettre en place des systèmes de sécurité, segmenter leurs réseaux, ou limiter les accès à leurs systèmes.

L'attaque sur Target aurait pu être évitée si l'entreprise avait respecté une règle de bon sens énoncée dans l'arrêté du 17 avril 2023 relatif aux établissements hospitaliers :

« *L'opérateur d'importance vitale procède au cloisonnement de ses systèmes d'information d'importance vitale (SIIV) afin de limiter la propagation des attaques informatiques au sein de ses systèmes ou ses sous-systèmes. Il respecte les règles suivantes :*
– chaque SIIV est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes d'information de l'opérateur et des systèmes d'information de tiers ; »

Les attaques contre les smarts buildings se sont développées depuis les premières alertes des années 2010 et une étude Kaspersky de 2019 avançait déjà le chiffre de 37,8 % d'entre eux victimes d'une attaque en 2019.

Or le bâtiment est une ressource vitale pour l'entreprise et/ou les personnes qu'il abrite et ses systèmes d'information (GTB, BOS ou logiciels de pilotage spécifiques) doivent être protégés au même titre que les SIIV d'organisations critiques aux yeux de l'état. Ceci concerne principalement les trois niveaux technologiques que nous y avons distingués : le logiciel, les réseaux de terrain, les objets pilotés.

Table des matières

SMART BUILDING : L'ESSENTIEL

Les *smart buildings* (ou bâtiments intelligents) ne sont plus un concept d'avenir : ils transforment déjà la manière de concevoir, gérer et exploiter les bâtiments. Ils offrent une multitude de services aux usagers ainsi qu'aux gestionnaires, tout en contribuant à la transition énergétique : contrôle des consommations (éclairage, chauffage, climatisation…), réduction des coûts d'énergie et de l'empreinte carbone, confort des occupants (qualité de l'air…), sécurité (contrôle d'accès biométrique, systèmes d'alerte incendie ou intrusion…), maintenance prédictive.

Mais intégrer ces innovations suppose de maîtriser une chaîne complexe de savoir-faire, de l'informatique à la thermique, des réseaux à la maintenance immobilière... Cela nécessite la coordination de métiers variés, et impose de comprendre les technologies de l'information (IT, OT, IoT, IP, GTC, GTB…) ainsi que les contraintes liées au bâtiment.

Cet ouvrage propose une **vision d'ensemble** du bâtiment intelligent, à la fois structurelle et matérielle, en aidant à :
– distinguer le souhaitable du réalisable ;
– définir un cahier des charges pertinent ;
– communiquer efficacement avec les spécialistes ;
– évaluer les offres du marché et leurs limites.

Au fil des chapitres, sont ainsi abordés :
– les principes essentiels des architectures de réseaux et des technologies numériques appliquées au bâtiment ;
– le contexte réglementaire international et français (RE2020, décret BACS, labels et référentiels) ;
– les enjeux croissants de cybersécurité et de l'intelligence artificielle, désormais aussi cruciaux pour l'exploitation technique (OT) que pour les systèmes informatiques (IT).

Un **guide indispensable** pour comprendre comment faire du bâtiment intelligent un bâtiment efficient, pérenne, respectueux de l'environnement, et flexible.

Destiné aux maîtres d'ouvrage, maîtres d'œuvre et acteurs du BTP, cet ouvrage offre une lecture accessible et structurée pour appréhender les mutations du secteur. Il vise à favoriser une compréhension concrète du terrain et à accompagner les professionnels dans la mise en œuvre de bâtiments performants, durables et évolutifs.

Jean-Pierre Arnaud a été professeur (titulaire de la chaire Réseaux) au Conservatoire national des Arts et Métiers (Cnam). Dès 1987, il a cocréé IB2 Technologies, filiale d'IBM et de Bouygues, se consacrant à la conception de bâtiments intelligents aujourd'hui appelés *smart buildings*. Il a également été expert auprès d'organismes de normalisation (Afnor, CCITT).

Sommaire

ISBN 978-2-281-14831-2

9 782281 148312

EDITIONS LE MONITEUR