FÉDÉRATION FRANÇAISE
DES INTÉGRATEURS ÉLECTRICIENS

ALLIANCE NATIONALE
DES INTÉGRATEURS DE TECHNOLOGIES
CONNECTÉES, SÉCURISÉES ET PILOTÉES

NOTÉCO
LES NOTES ECONOMIQUES DE LA FFIE

Novembre 2021

n°30

LA PROTECTION DES SYSTÈMES DE GTB-GTC CONTRE LE RISQUE CYBER : UNE OFFRE COMPLÉMENTAIRE À PROPOSER

La commission économique de la FFIE et l'AniTEC ont souhaité se mobiliser sur le marché du pilotage securisé des bâtiments.

Fort de l'expertise de l'AniTEC sur la cybersécurité, cette note économique propose de renforcer l'offre des intégrateurs en mettant l'accent sur la protection des systèmes de pilotage.

En effet, sous l'impulsion du développement numérique, les bâtiments deviennent de plus en plus intelligents, nécessitant des installations techniques de pointe avec des systèmes de plus en plus complexes, mais aussi par le biais d'objets connectés.

Poussées par les décrets "Tertiaire et BACS", l'automatisation et la numérisation des bâtiments connaissent un nouvel essor.

Nous contacter : FFIE - 5 rue de l'Amiral Hamelin 75116 PARIS - Tél. 01 44 05 84 00 - ffie@ffie.fr

Le Décret BACS publié le 20 juillet 2020 signifie « Building Automation & Control Systems », le texte impose de mettre en place un système de régulation avant **le 1er janvier 2025** pour les bâtiments tertiaires non résidentiels disposant de systèmes assurant le chauffage ou la climatisation (ou une combinaison de ces deux postes avec la ventilation), d'une puissance supérieure à 290 kW.

Pour rappel, le décret « tertiaire » n°2019-771 du 23 juillet 2019, issu de l'application de l'article 175 de la loi ELAN, vise à réduire les consommations d'énergie finale dans les bâtiments à usage tertiaire ayant une surface de plancher ≥ 1000 m² de :

- 40% en 2030,
- 50% en 2040,
- 60% en 2050.

Les données à transmettre sur la plateforme OPERAT de l'ADEME dès septembre 2022 sont multiples :

- l'activité tertiaire exercée, surface de chaque bâtiment,
- consommations annuelles d'énergie,
- année de référence et les consommations associées,
- indicateurs d'intensité d'usage applicables aux activités hébergées,
- modulations du volume d'activité,
- consommations liées à la recharge des véhicules électriques.

I- GTB/GTC : DES SYSTÈMES DE PILOTAGE DU BÂTIMENT

- **L'essor des systèmes de GTB/GTC, atout incontournable pour réduire sa consommation d'énergie**

Les capteurs et actionneurs (les IoT au sens large et souvent regroupés sous le terme « smart grids ») pilotés par un système de gestion adapté à la structure immobilière, sont connus depuis plusieurs années sous les acronymes de GTB/GTC. Un système d'automatisation et de contrôle des bâtiments passe donc par l'installation de produits et de logiciels qui permettent d'assurer le suivi et le pilotage des consommations et des équipements du bâtiment.

A travers ces deux décrets, l'intégration des équipements et des systèmes de régulation et de Gestion technique du Bâtiment vont jouer un rôle fondamental dans l'atteinte de performance énergétique.

C'est l'opportunité pour le promoteur

de faire entrer le suivi de réduction de consommation dans une véritable politique d'Energie Management...

Celà permet de profiter de la mise en œuvre de ces solutions de gestion informatique pour le confort des occupants, usagers et pourquoi pas de la sécurité et de la sûreté.

En règle générale la **GTB,** parfois aussi appelée immotique dans le domaine tertiaire et industriel, permet de piloter les installations techniques telles que le chauffage, la ventilation, la climatisation, les installations de distribution d'électricité, d'éclairage ainsi que les installations de sécurité et de sûreté telles que la vidéo-surveillance, le contrôle d'accès.

Elle contrôle à distance l'activité d'un site et supervise l'ensemble des équipements installés.

Afin de relier le système et l'utilisateur, l'interface "homme-machine" est assurée par un logiciel de supervision. Il assure la gestion et le suivi à distance des installations via les automates placés au sein des bâtiments et dispose d'une connexion internet.

En règle générale la **GTC**, quant à elle, contrôle toutes les installations techniques d'un seul lot ; par exemple, pour le lot électricité. La Gestion Technique Centralisée gère l'éclairage, la détection de présence, la consommation d'énergie électrique, la vidéoprotection et dans certains IGH (Immeubles de Grande Hauteur) la sûreté et parfois même la sécurité incendie.

- **Les systèmes de GTB/GTC, atouts incontournables pour optimiser le pilotage à distance**

En offrant la possibilité de contrôler différentes fonctions techniques, une GTB de nouvelle génération propose de réelles optimisations en venant renforcer :

- les économies d'énergies,
- la réduction des coûts d'exploitation,
- la diminution des coûts de maintenance,
- un suivi du bâtiment grâce à la gestion des installations techniques,
- l'amélioration du confort et du bien-être des occupants.

En effet, couplées avec des technologies additionnelles comme la maquette numérique 3D, voire d'un BIM - Building information modeling dédié, une GTB/GTC « hypervisée » avec des multi protocoles et une interface de télégestion multisites à distance, permet à une petite équipe de gérer un grand ensemble d'immeubles en intégrant les maintenances préventives et curatives.

Dans ce cas précis, les IoT implantés et la solution de gestion sont capables de générer des messages d'alertes et d'alarmes pour les techniciens du site. Cela permet également, via des interfaces de programmation, de s'implanter assez facilement sur des tablettes ou sur un smartphone dédié par le biais d'une application et d'un micro-logiciel de gestion.

- **Les systèmes de GTB/GTC, vers de nouveaux risques cyber qu'il faut prendre en compte**

Que la solution soit fermée et propriétaire ou ouverte multi systèmes et protocoles, les gains énergétiques et la réduction des coûts pour les promoteurs, bailleurs, propriétaires, amènent de nouveaux risques, qu'il est

indispensable de prendre en compte.

Ces nouveaux risques doivent être pris en compte par un intégrateur électricien expert du domaine numérique, (ou à défaut par un bureau d'étude spécialisé) qui aura un véritable rôle de conseil auprès du client final.

Un nouveau métier, un nouveau service réfléchi et travaillé par l'AniTEC appelé « l'Opérateur Local de Services Numériques ».

En effet depuis quelques années, le monde industriel et tertiaire fait l'objet d'attaques informatiques connues sous la thématique des rançongiciels.

II. Renforcement de l'offre GTB/GTC par une offre cyber sécurité

- **GTB/GTC et confiance numérique**

La prise en compte des cybermenaces entre de plus en plus dans les besoins exprimés des clients finaux.

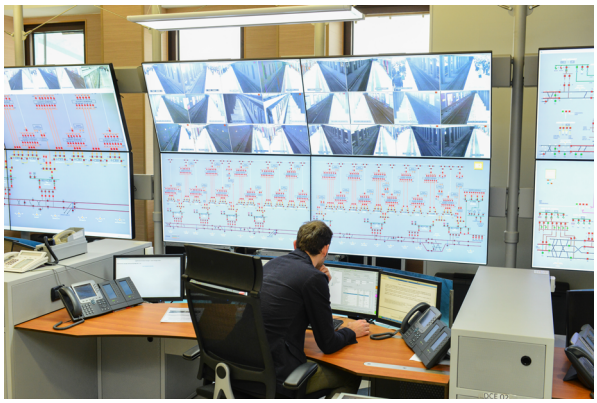
Ils expriment un besoin de protection pour une utilisation optimale et sécurisée des systèmes pilotés.

L'intégrateur électricien doit donner confiance à son client, en venant proposer des garanties sur la confidentialité des systèmes et des capteurs, sur leur intégrité, leur disponibilité H24 et 365j/an. Il devra également proposer un contrat de maintenance pour assurer le suivi et l'entretien du système durant tout son cycle de vie. La cybersécurité opérationnelle devient un service additionnel !

La GTB doit intégrer la cybersécurité le plus en amont possible, le mieux est de l'envisager dès les technologies utilisées en tenant compte du besoin exprimé par le client.

La FFIE et l'AniTEC rappellent l'importance auprès des donneurs d'ordre, d'une véritable étape de conciliation et de travail concerté sur le choix des technologies, des produits, des systèmes, et d'une réflexion sur la protection des données et la cybersécurité.

Cet écosystème s'est encore agrandi récemment avec l'apparition de ce que l'on pourrait appeler les SmartSystems (SmartGrid, SmartCities, SmartWater....) qui étendent les technologies ICS (sécurité des technologies opérationnelles) et GTB à l'échelle d'une ville, d'une région ou d'un pays.... On ne parle plus de GTB-GTC mais de BOS « Building Operating Systems » et de centre de supervision urbain surdimensionné pour traiter la gestion urbaine en temps réel.



Alors que les ICS et GTB doivent traiter le sujet de la cybersécurité sur des installations qui n'ont pas été prévues pour cela, les SmartSystems grandiront avec cette nouvelle préoccupation de devoir faire face à une criminalité numérique et de l'impératif d'une stratégie commune à mettre en œuvre entre clients et intégrateurs pour optimiser et valoriser des systèmes de pilotages efficients.

- **Complémentarité entre « sûreté de fonctionnement » et « cybersécurité »**

Les pannes consécutives à la défaillance d'équipements, de capteurs, d'actionneurs sont bien connues et provoquent déjà des incidents.

Les spécialistes de la « sûreté de fonctionnement » (SDF) connaissent le sujet notamment dans le milieu industriel, les centres de production et de fabrication, mais la nouveauté provient des risques malveillants des cyberattaques.

Il faudrait donc que les bâtiments connectés de demain soient sécurisés pour ce tout ce qui concerne le numérique, la mécanique ou la maintenabilité des équipements, condition sine qua none

pour tendre vers une ville ou un territoire intelligents.

L'Opérateur Local de Services Numériques pourrait être ce facilitateur, cet expert « sûreté de fonctionnement » qui maintient, alerte et répare avant la contagion d'une cyberattaque.

> **➲ Conseil**
>
> Un intégrateur électricien spécialisé prendra en compte l'expression des besoins de son client et trouvera le produit ou système le plus résilient et sécurisé sur le marché.
>
> C'est une démarche « Intégrateur » comprise dans le devoir de conseil d'apporter au client le meilleur compromis prix/qualité/fiabilité pour répondre à un usage ou une finalité prédéterminé.

A noter depuis mai 2018 et l'entrée en vigueur du RGPD, un intégrateur électricien doit s'interroger sur l'intérêt du « Security by design », c'est-à-dire, d'interroger les fabricants, les développeurs, concepteurs distri-buteurs de produits de la prise en compte du RGPD et de la cybersécurité du produit ou du système dès la conception.

- **L'importance de la maintenance et de la mise à jour des systèmes pilotés**

Dans le cadre de la sûreté de fonctionnement, s'il parait peu crédible et probable que deux systèmes soient en panne en même temps, il est en revanche probable qu'un attaquant malveillant ait la volonté de prendre le contrôle simultanément de ces deux systèmes s'il en a la capacité technique.

La surface d'attaque peut être le capteur-actionneur installé, non sécurisé, mal paramétré ou programmé, un système d'exploitation caduque et obsolète qui n'a pas été mis à jour, un non-remplacement des mots de passe, mais aussi parfois une duplicité interne ...

Les menaces dans le monde cyber évoluent aussi rapidement que les technologies numériques.

Cette évolution des technologies numériques devient d'ailleurs préoccupante car la vitesse de formation des personnels à cette adaptation continuelle est de plus en plus difficile à mettre en œuvre.

La maturité d'une technologie numérique peut être de quelques mois pour les IoT, son obsolescence de l'ordre de deux ou trois ans pour certains produits, systèmes ou protocoles. Des vulnérabilités sur les produits et technologies sont détectées quotidiennement pour ne pas dire journellement. Les outils des malveillants deviennent chaque jour plus énergiques et à la portée d'un nombre grandissant d'individus sur l'internet profond (Deep web) ou le Darknet.

Il nous faut parvenir à s'assurer que le numérique devienne un monde sûr pour les bâtiments intelligents et demain les territoires intelligents.

III. La cybersécurité, quand, comment, avec quels acteurs ?

Le sujet de la cybersécurité doit être abordé malgré un contexte de pression sur les coûts, le manque de ressources et de compétences.

Il est possible d'identifier des pistes à explorer en fonction du contexte du site, de son ou de ses environnements, de la cartographie des équipes, de l'existence ou non dans l'entreprise cliente d'un système de management.

Cette démarche sera facilitée si le client possède déjà un système de management de type qualité comme l'ISO 9001, ou d'un 14001 pour l'environnement.

A défaut, il faut trouver les bonnes proportions et le bon mode opératoire.

Pour ce faire, il convient de ne pas commettre l'erreur de vouloir appliquer brutalement des normes et guides de bonnes pratiques sans, au préalable, se les approprier et les adapter à ses besoins. Le risque étant de déployer des solutions inadaptées, aux coûts importants dont personne n'a le réel contrôle et pour une efficacité réduite.

Le résultat peut même mener à l'échec du projet !

L'AniTEC défend une position de mutualisation avec les donneurs d'ordres, avec des bureaux d'études spécialisés et partenaires, ainsi que des partenaires fabricants et ou concepteurs comprenant tout l'intérêt d'une démarche globale dans la cybersécurité.

- **Connaître et faire connaître au plus grand nombre les menaces sur les GTB/GTC et ICS**

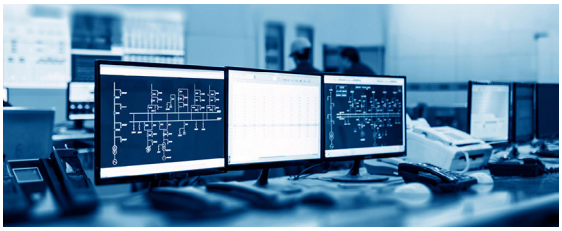
Les événements redoutés, les vulnérabilités ou failles et les modes opératoires sur les ICS et GTB/GTC sont multifactoriels. Les identifier, même à minima, est l'étape indispensable pour y faire face.

Réseaux sans fil : comment sécuriser les réseaux sans fil (WiFi, GSM, GPRS, etc.) ?
L'apparition de protocoles plus fiables (WPA2 pour le WiFi par exemple) laisse à penser que les risques d'attaques sont faibles.

Mais, si fiables soient-ils, ces protocoles doivent être implémentés et configurés correctement par les utilisateurs et mis à jour régulièrement.

Télégestion et Télémaintenance : les risques liés à la télémaintenance ne sont pas bénins même si des solutions comme les VPN apportent de la sécurité.

Le problème déjà évoqué des mauvaises implémentations et configurations rendra forcément la solution vulnérable. De plus, les mauvaises pratiques (connexions depuis des PC dont le niveau de sécurité est faible, mots de passe enregistrés dans le bureau de l'écran, etc.), sont hélas un grand classique. Pour maîtriser la télémaintenance, il faut d'une part maîtriser le canal de communication et d'autre part les équipements et utilisateurs « distants », ce qui est bien plus complexe, qu'il n'y paraît.



Web services : l'emploi des Web services dans les composants commence à se généraliser. Les contrôleurs, les SCADA[1], voire les capteurs et actionneurs intelligents, qu'ils soient industriels ou tertiaires, embarquent des serveurs Web. Pratiques à utiliser et standards, peu d'entre eux offrent un niveau de sécurité acceptable. Pourtant, les rendre plus sécurisés n'est pas nécessairement complexe ni plus consommateur en ressources. Cela vient légitimer l'importance d'une contractualisation avec l'intégrateur électricien « Opérateur Local de Services Numériques ».

Les systèmes accessibles sur Internet : les ICS et GTB connectés à Internet avec un niveau de protection nul ou faible sont malheureusement coutumiers. Dans de nombreux cas, il s'agit souvent de « petites installations » (gestion CVC du bâtiment, gestion des fluides en dehors de l'informationnel, etc.) mais les impacts, en cas d'incident, peuvent être conséquents pour leurs propriétaires (augmentation exponentielle de la température dans une salle blanche ...)

1 Supervisory Control and Data Acquisition (système de supervision industrielle qui traite en temps réel un grand nombre de mesures et controle à distance les installations)

De telles pratiques sont très fortement déconseillées.

Consoles de programmation et de maintenance déportées : elles sont une porte d'entrée délaissée et si elles contiennent des codes sources, c'est une menace véritable si elles sont mal maîtrisés ou sécurisés.

- **Analyse de risques et bonnes pratiques**

Cette exigence est déjà connue des intégrateurs électriciens habitués aux systèmes complexes et au traitement des données de masse dans la vidéoprotection et le contrôle d'accès au travers de l'article 35 du RGPD.

L'analyse de risques est régulièrement présentée comme le point de départ de toute démarche projet pour le client final disposant d'un DPO (Délégué à la protection des données) et nos entreprises. Il est en effet important d'adapter les mesures qui seront déployées aux risques identifiés, de ne pas en oublier et de ne pas les surestimer. Parfois longue, cette étape est indispensable.

Il est parfois tentant de se contenter d'appliquer quelques bonnes pratiques émanant de livres blancs de fabricants ou de guides généralistes d'organismes publics. Si certaines sont réalisables rapidement au travers de canevas réflexes et scénarisés, sans recourir à une analyse de risque complète, seule cette dernière permet d'avoir une réelle vision des moyens à mettre en œuvre face à l'importance du système à protéger.

Pour conclure, il convient de valoriser la cybersécurité et non de l'aborder comme une contrainte supplémentaire.

Cette offre de cybersécurité est un facteur contributif de performance et une source de réduction des coûts intelligente pour des projets en GTB-GTC efficients et sécurisés.

A titre d'exemple et de gain d'efficacité, il est conseillé par exemple de :

- **gérer les mots de passe et privilèges** des utilisateurs de manière centralisée si celle-ci est bien protégée et non plus individuellement,
- **renforcer la robustesse des systèmes et la productivité** en empêchant une modification d'un programme automate des stations GTB secondaires ou écrans d'application laissés dans des locaux non sécurisés, souvent dans les projets multisites,
- **contrôler l'intégrité et l'authenticité des applications installées** au travers d'une gestion intelligente des droits d'accès, contribue à réduire les risques de mauvaises manipulations (volontaires ou accidentelles),
- **cloisonner les réseaux :** utiliser des logiciels peu liés à d'autres briques de logiciels,
- **réaliser une cartographie des flux**.

Ces quelques exemples d'actions pourront faciliter, par la suite, la gestion de l'obsolescence, prendre les meilleurs arbitrages pour ce qui concerne la télégestion, réfléchir à une implémentation par brique pour les systèmes de sûreté ou la sécurité incendie.

C'est tout l'intérêt d'une démarche globale et d'une analyse des risques menées en concertation qui permettront la réussite du projet du bâtiment intelligent.

Ces pistes sont bien évidemment à étudier au cas par cas mais montrent que l'approche cybersécurité peut être un vecteur d'efficacité pour le bâtiment du futur.