B@TI-COM

Capteur d'informations utiles pour le bâtiment communicant et le Smartbuilding

N°97
08 avril 2016
Edition bimensuelle

SOMMAIRE

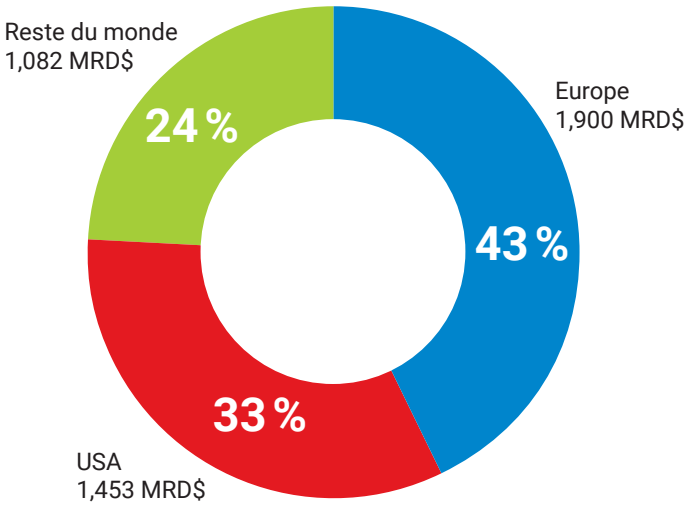
L'ACTU EN CHIFFRES

4,4 MRD$ Le marché global du Building Energy Management Systems (BEMS) estimé à 4,4 milliards de USD

D'après BSRIA le marché global des systèmes d'information énergétique (SIE) du bâtiment vaudra 4,4 milliards USD en 2016. Le plus gros contributeur est l'Europe (43%), dominé par l'Allemagne qui est confrontée à une règlementation environnementale exigeante et à des coûts de l'énergie élevés et provenant de régions instables. Le Royaume-Uni et les Pays-Bas sont aussi des marchés développés, ainsi que la Scandinavie. En France, l'électricité encore relativement peu chère met un frein à l'urgence de réaliser des économies d'énergie.

Source : BSRIA – avril 2016

Prévision du marché global « BEMS » 2016



À LA UNE !

La Cybersécurité des bâtiments communicants, plus qu'un défi, une nécessité !

Thème central de la journée Agor@lon organisée par Lonmark France en mars dernier, la cybersécurité va devenir un enjeux majeur à l'heure où le bâtiment devient communiquant et de plus en plus "intelligent". Ce choc de l'arrivée du monde de l'IT ouvert et web-communicant bouleverse les certitudes du monde de la GTB et de la supervision fermées et donc moins exposées aux nombreux problèmes que pourraient poser les cyber-attaques.

Peu de bâtiments communicants ont été envisagés en prenant en compte sérieusement l'aspect cybersécurité en particulier avec l'arrivée de l'IP et L'IoT, une connectivité filaire ou wireless accrue permettant des échanges de données entre des terminaux fixes ou mobiles et donc autant d'entrées possibles pour les hackers. Les attaques réussies sur les objets connectés sont légions et certains protocoles posent de véritables questions quand à leur sécurité par défaut. Car il faut bien considérer les systèmes GTB dont les supervisions comme complexes, hétérogènes et pour la plupart bâtis sur des standards sans mesure de sécurité.

Dans ce contexte, l'amélioration de la sécurité des réseaux dans le bâtiment est indispensable. Faut-il conserver deux réseaux séparés en isolant le réseau technique ou trouver des mesures efficaces sur un réseau mutualisé ?

En règle générale, la sécurité doit être intégrée dès le départ d'un projet de manière à évaluer les mesures nécessaires à prévoir sur le réseaux et ses différents objets (techniques ou services).

>> Suite

Suivez-nous sur :

La cybersécurité de la gestion technique du bâtiment est proche des systèmes industriels du type ICAS (Industrial Automation and Control Systems) qui se définissent comme un système numérique qui a pour objet une action ou une interaction sur les équipements physiques comme des capteurs ou des composants de pilotage. Progressivement les systèmes informatiques industriels ou les GTB sont devenus de plus en plus ouvert permettant le traitement à distance comme pour la télémaintenance par internet.

Dans le monde industriel comme pour la GTB, les critères liés à la sureté de fonctionnement sont prioritaires par rapports à la confidentialité ou à la traçabilité. Ces systèmes ont des caractéristiques spécifiques qu'il faut prendre en compte dans la gestion des risques comme leur durée de vie plus longue. On prévoit en effet ces systèmes pour des dizaines d'années D'autre part, la continuité de service doit être la meilleure possible. Enfin la dépendance aux fournisseurs est forte car ils livrent la solution clé en main et souvent assortie d'une maintenance. Tous ces aspects influent fortement sur la gestion des risques et la manière de les sécuriser.

Les référentiels concernant la sécurité des systèmes informatiques sont très fournis et pas toujours d'une lecture facile. Pour identifier le référentiel le plus adapté, un guide sur l'initiation à la cybersécurité des systèmes informatiques industriels créé par le CLUSIF (club de la sécurité de l'information Français) est en téléchargement libre (www.clusif.asso.fr). Il répertorie et classe parmi plus de 50 documents, les 20 plus pertinents donnant ainsi une sélection lisible d'applications concrètes.

Par ailleurs, ce guide détaille les 5 phases clés pour envisager la cybersécurité des systèmes industriels :
• Réaliser un état des lieux et assimiler le fonctionnement
• Sensibiliser les décideurs sur les vulnérabilités informatiques induisant des risques
• Elaborer la politique de sécurité des systèmes informatiques
• Décliner la PSSI au niveau opérationnel
• Maintenir sous contrôle les cyber risques.

La démarche de cybersécurité est aussi liée à la responsabilité informatique d'un bâtiment. Aujourd'hui, l'intégration des exigences de sécurité dans le bâtiment est un facteur de coût nécessaire qui ne peut se résumer à l'aspect technologique auquel il faut ajouter le facteur organisationnel. La plupart des fournisseurs de sécurité viennent du monde de l'IT et doivent absolument comprendre le monde de la GTB-GTC.

Dans ce contexte des acteurs du marché ont signé, dès 2013, des protocoles de coopération dans la domaine de la cybersécurité des systèmes industriels à l'exemple de THALES et de SCHNEIDER ELECTRIC avec une approche de sécurité globale adaptée aux systèmes de contrôle pour apporter de nouvelles solutions en particulier sur le contrôle des bâtiments. Dans ce domaine, THALES est un centre de compétence regroupant près de 1500 experts. Cette division réalise des audits d'architecture et organisationnels ainsi que des tests d'intrusion qui permettent de matérialiser le risque et faire prendre conscience par exemple qu'un Firewall plus un élément de sécurité si il est mal ou pas configuré correctement.

Ceci pour suivre les étapes essentielles de sécurisation chez les opérateurs à savoir :
• Faire un point précis sur les équipements, logiciels et identification des zones à risque
• Définir, phaser et appliquer le plan de sécurité
• Maintenir un niveau de sécurité dans le temps

Dans bien des cas le bâtiment étant au cœur des réseaux intelligents (Smart Grids, Smart Cities, Transports,..), l'installation de produit de type diode (sortant mais pas entrant) est à privilégier pour limiter le risque d'attaque sans négliger la partie organisationnelle interne.

Au niveau européen des initiatives ont vue le jour comme : FUSE-IT (Facility Using Smart Energy & Information Technology) un projet de R&D soutenue par l'Union et centré sur le bâtiment et la sécurité en particulier sur les sites sensibles. Le programme vise à trouver les moyens d'assurer la sécurité et la sureté du bâtiment sans compromettre son efficacité. Les thèmes de recherches sont orientés entre autre sur la technologie radio, le domaine des capteurs basse consommation, l'IoT et sécurité des réseaux de capteurs ou encore le chiffrement sur plateforme à ressources contraintes.

Pour en savoir plus : www.fuseit.com

L'ANSSI (Agence nationale de la sécurité des systèmes d'information www.ssi.gouv.fr/) propose aussi des recommandations sur la cybersécurité applicables aux bâtiments.
L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information.