01

DATACENTERS

Cybersécurité : au-delà du périmètre

De la conception à l'exploitation d'un datacenter, en passant par sa réalisation, la cybersécurité fait corps avec la solution ABB Ability™ DataCenter Automation. L'offre du Groupe dédiée aux centres de données complète la protection périmétrique traditionnelle en sécurisant également les réseaux, serveurs et données.

Disposer en continu d'une alimentation électrique sûre et fiable est crucial pour les centres de données, qui s'appuient pour cela sur des alimentations sans interruption (ASI). Ces dernières garantissent la continuité de fonctionnement de l'infrastructure électrique, de la gestion technique du bâtiment (GTB) et des automatismes. L'intégration des technologies opérationnelles (OT) et informatiques (IT) améliore la fiabilité, le contrôle-commande et la performance des datacenters, mais les rend également plus que jamais vulnérables aux cyberattaques. Toute brèche dans l'accès aux données de ces infrastructures

—

Il y a une dizaine d'années, la sécurité d'un datacenter se résumait à la protection du périmètre physique et des données.

connectées les met à la merci d'acteurs malveillants : un cauchemar pour les exploitants, prêts à tout pour se protéger. Le marché mondial de la cybersécurité industrielle, qui englobe la sécurité des réseaux, le contrôle-commande industriel ainsi que les solutions logicielles et matérielles, devrait peser 24,41 milliards de dollars en 2023 [1].

Il y a une dizaine d'années, la cybersécurité d'un datacenter se résumait à la protection du périmètre des salles informatiques et des données hébergées. Le marché était dominé par les datacenters d'entreprise et les standards de communication industrielle prônant l'ouverture des systèmes d'automatisation n'étaient pas encore de mise. Le paysage a bien évolué depuis et ce qui semblait alors raisonnable s'avère aujourd'hui terriblement insuffisant : le déport des serveurs dans le cloud et l'interconnexion des automatismes augmentent le niveau d'exposition aux risques de cyberattaques. Protéger le périmètre et les données ne suffit pas à se prémunir des défaillances et pannes de grande ampleur [2].

ABB a une vision globale de la cybersécurité des datacenters, de la conception, du développement et du déploiement des systèmes de contrôle-commande et d'automatisation, jusqu'au moindre matériel électrique. Le Groupe s'appuie sur les meilleures pratiques, dictées tant par la normalisation internationale que par son expertise, pour mettre la cybersécurité au premier plan de son offre d'automatisation dédiée aux datacenters.

Numéro un mondial de la gestion d'actifs et du contrôle-commande distribué, avec 20 % de parts de marché [3], ABB est en position idéale pour fournir des systèmes d'automatisation fiables, sûrs, ouverts et interopérables. Repoussant toujours plus loin les limites de l'optimisation et de la disponibilité, la solution ABB Ability™ DataCenter Automation s'appuie sur ce puissant socle technologique pour s'adapter à tous les configurations : interne, externalisée ou mixte.

L'offre ABB de solutions « convergées » permet ainsi de piloter simultanément plusieurs systèmes du datacenter : GTB, commande et supervision électriques, gestion d'infrastructures (DCIM).

Cette plate-forme d'automatisation ouverte favorise l'échange de données entre systèmes, dispositifs, composants et applications, avec à la clé :

- une intégration plus rapide des outils de gestion du datacenter, y compris l'ajout automatisé d'actifs industriels dans les systèmes de surveillance ;
- une visualisation et une gestion des actifs physiques unifiées à l'échelle du datacenter, même multisite ;
- une automatisation de l'alimentation électrique et du refroidissement qui améliore l'optimisation continue et la disponibilité du centre.

La dure réalité de la menace cyber

Les menaces qui pèsent sur l'automatisation industrielle et l'infrastructure associée ne cessent d'augmenter et de se complexifier depuis dix ans [4]. Alors même que la communication entre automatismes et systèmes informatiques industriels multipliait les protocoles, matériels et logiciels, les réseaux étaient conçus dans un souci de performance, de fiabilité, de sécurité et de flexibilité, mais guère de protection des transmissions et des données. Aujourd'hui, ce « patrimoine informationnel », qui ne bénéficie que d'une défense périmétrique, est la première victime des cyberattaques et incidents de sécurité.

Les entreprises se heurtent à une double difficulté : d'une part exploiter les données des systèmes et procédés temps réel afin d'accroître l'interconnectivité et l'interopérabilité des différents automatismes, d'autre part intégrer les nouveaux systèmes à l'existant. Un panorama extra-périmétrique qui augmente naturellement le niveau des cybermenaces sur les centres de données.

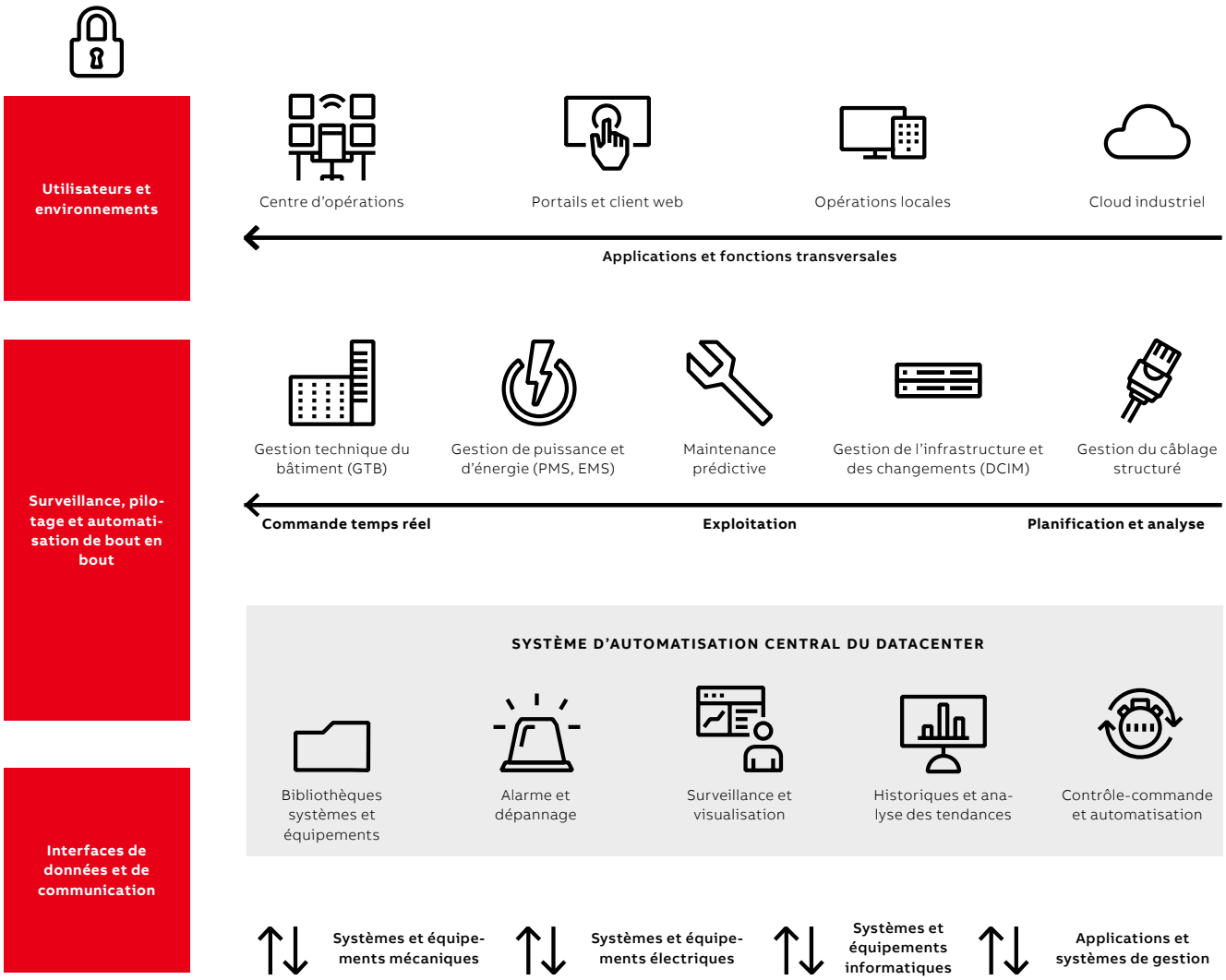
L'infrastructure électrique et le contrôle-commande sont complètement intégrés au cycle de vie des systèmes d'automatisation industrielle, de la conception et du développement au support client et aux évolutions, en passant par les essais et la mise en service. Les solutions globales de sécurité ABB permettent aux exploitants de datacenter d'identifier, d'atténuer et de gérer les cyber-risques. Elles suivent une démarche commune à toutes les

Madhav Kalia
ABB Data Center Automation Solutions
Singapour

madhav.kalia@sg.abb.com

Apala Ray
ABB Industrial Automation Process Industries
Bangalore (Inde)

apala.ray@in.abb.com



01

offres du Groupe embrassant les trois étapes de conception du produit, d'exécution du projet et d'exploitation du site.

Les défis de la sécurité

Alors que la cybermenace s'accentue et se diversifie, il convient de sécuriser réseaux, serveurs et données [2]. Ces mesures s'ajoutent à la protection périmétrique, qui défend non seulement les limites physiques du datacenter mais aussi l'infrastructure électrique et les commandes mécaniques ou électroniques.

La gestion de la sécurité d'une installation est indissociable d'une politique de rôles bien pensée, chaque collaborateur devant se voir attribuer les bonnes fonctions et autorisations.

Qui plus est, les protocoles industriels propriétaires n'intègrent souvent pas de mécanismes propres à sécuriser le contrôle-commande ou l'infrastructure électrique (authentification, contrôles d'intégrité, chiffrement, par exemple).

Protéger le réseau de communication et les données des attaques provenant d'un autre réseau est une tâche complexe qui fait appel, entre autres,

—

Alors que la cybermenace s'accentue et se diversifie, il convient de sécuriser réseaux, serveurs et données.

à la cryptographie. Le réseau doit par ailleurs disposer des dernières versions des correctifs de sécurité et listes de programmes malveillants (*malwares*). Enfin, en cas de catastrophe imprévue, des sauvegardes doivent garantir la reprise de l'activité. Les environnements virtuels, particulièrement complexes, exigent des solutions de surveillance à la hauteur. L'offre de cybersécurité d'ABB relève tous ces défis avec brio.

—
01 La solution ABB Ability™ DataCenter Automation permet d'automatiser tous les systèmes de commande électrique, mécanique et de gestion du bâtiment.

—
02 Architecture de référence de la solution cybersécurisée d'ABB pour les centres de données

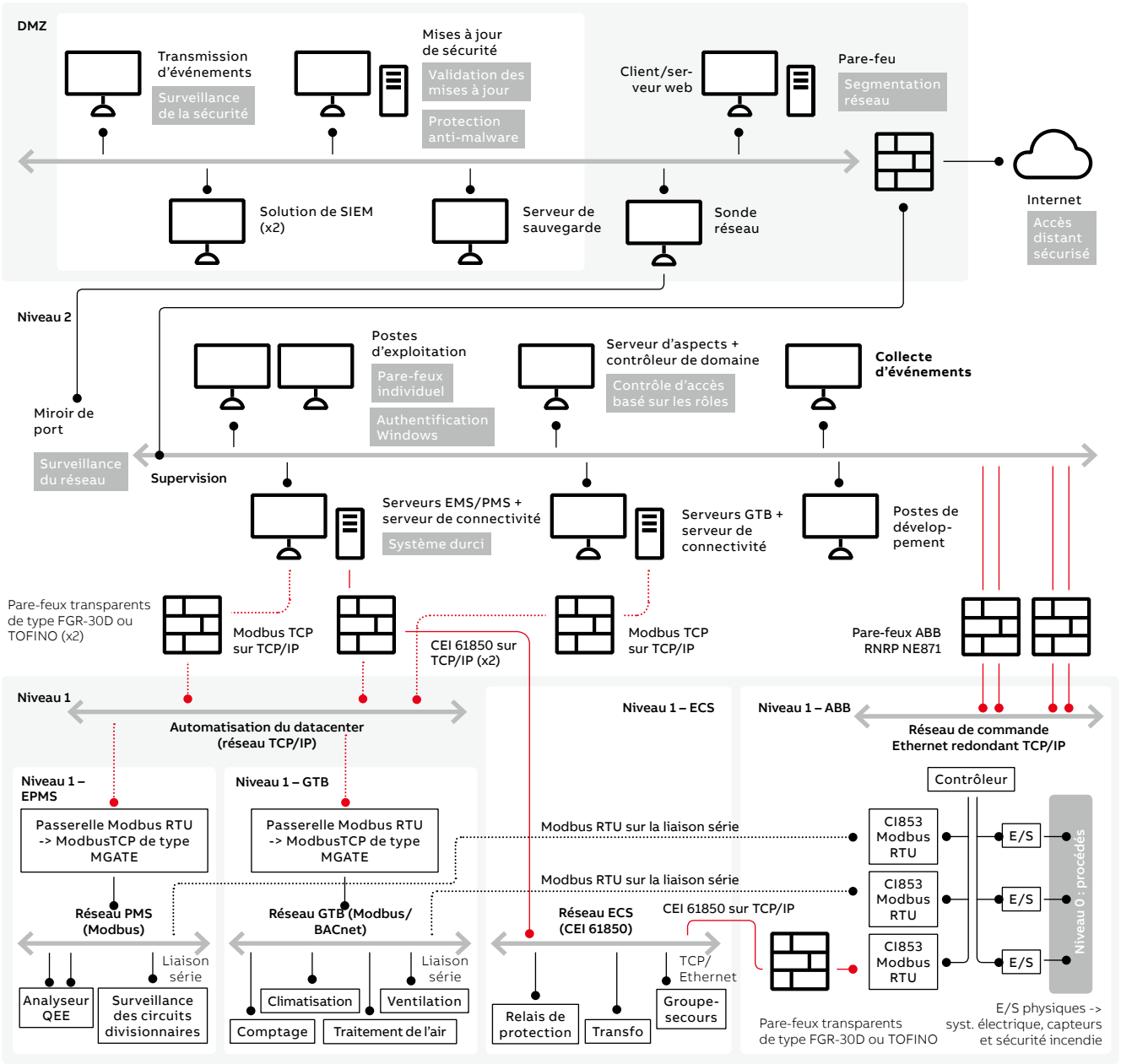
Cybersécurité ABB

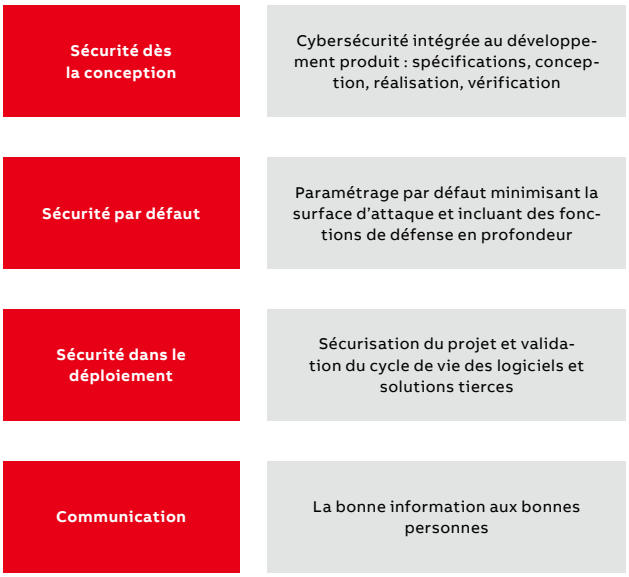
La suite logicielle ABB Ability™ DataCenter Automation regroupe des fonctions de gestion énergétique (EMS), de gestion technique du bâtiment (GTB) et de gestion automatisée de l'électricité (PMS) au sein d'un système de pilotage et de surveillance de l'infrastructure électrique ECMS →01 qui enregistre toutes les données à des fin de surveillance et de documentation. L'exploitant de datacenter peut ainsi développer, mettre en service, surveiller et piloter l'automatisation de son infrastructure.

Même si la technologie ne suffit évidemment pas pour supprimer le cyberrisque, la solution ABB soutient la démarche cybersécurité des clients du Groupe en leur donnant les moyens de déployer un système d'automatisation de datacenter doté des contrôles de sécurité *ad hoc*. Elle peut aussi constituer une architecture de référence, adaptable aux exigences de chaque projet, en concertation avec le client. Le Groupe place ainsi l'humain, le procédé et la technologie au cœur de sa stratégie de cyberdéfense renforcée.

Segmenter pour mieux sécuriser

Le système d'automatisation de datacenter ABB assigne à chaque composant un niveau spécifique du réseau →02. La segmentation, concept de sécurité très répandu, vise à mettre en place des pare-feux et des zones démilitarisées (DMZ) pour isoler les réseaux sécurisés. Appliqué à l'automatisation des datacenters, où les différents équipements d'un réseau interne possèdent des



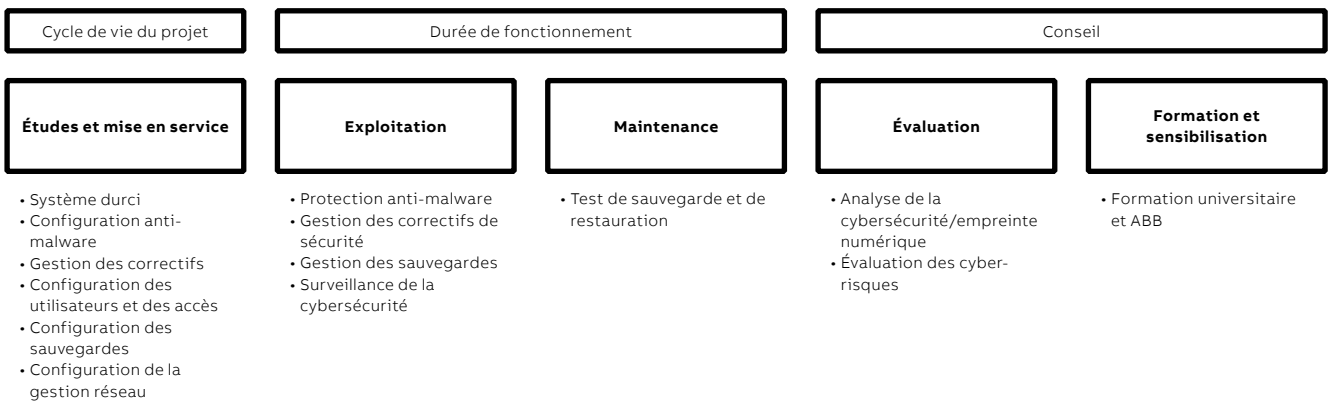


03

ABB propose une démarche sécurité bâtie sur le triptyque conception du produit, réalisation du projet et exploitation du site.

niveaux de sécurité variables, ce principe revient à diviser le réseau en zones pour renforcer le système. Au sein d'un même niveau, des pare-feux logiciels installés sur chaque ordinateur sécurisent la connectivité réseau ; les données ne peuvent accéder à un autre niveau qu'après avoir franchi un pare-feu matériel. La solution ABB assure l'authentification (utilisateur, appareils, logiciels), la gestion des autorisations et des comptes, la protection contre les codes malveillants, la segmentation du réseau et sa surveillance en continu pour parer aux cyberattaques. Elle englobe également la phase d'exploitation et de maintenance des automatismes, au moyen de contrôles de sécurité. Cette architecture en couches fait appel à des mécanismes différents selon le niveau concerné :

- Gestion des correctifs : sont déployées sur le serveur les mises à jour de sécurité validées par les éditeurs tiers (Microsoft, EXSi et Adobe). L'utilisateur a ainsi la garantie de toujours utiliser la dernière version du système de contrôle-commande ;
- Mise à jour fréquente des antivirus des serveurs ;
- Gestion des sauvegardes : documentation des procédures, test et conservation des sauvegardes dans un espace sécurisé hors ligne, afin d'éviter la perte de données en cas de défaillance ou de panne prolongée. La solution ABB prend en charge les applications de planification, de gestion et d'exécution régulière de la sauvegarde des données stockées sur les ordinateurs, serveurs ou autres équipements réseau, conformément au plan de continuité d'activité du client ;
- Durcissement du système : seuls les applications et services essentiels sont installés afin de diminuer la surface d'attaque. Des pare-feux sont déployés sur chaque poste et les mots de passe par défaut changés ;
- Gestion des comptes d'utilisateurs ainsi que des rôles et droits d'accès, élément clé de la cybersécurité ;
- Surveillance en continu des systèmes d'automatisation à partir des informations de sécurité et de la plate-forme de gestion des événements pour parer à toute nouvelle menace et intrusion quotidienne.



04

— 03 Les quatre composantes de la sécurité SD3+C.

— 04 ABB intègre la cybersécurité à toutes les étapes du cycle de vie d'un datacenter.

- Adhésion d'ABB au référentiel de sécurité SD3+C créé par Microsoft pour garantir et renforcer la sécurité de ses produits →03, selon quatre axes : réduire les défauts de jeunesse des nouveaux logiciels (vulnérabilités, failles de sécurité), accroître la résilience des configurations et installations par défaut, garantir un déploiement et une maintenance sécurisés, et enfin, promouvoir une communication responsable.

Maximiser la valeur

La cybersécurité est partie intégrante de la solution ABB Ability™ DataCenter Automation sur tout le cycle de vie : conception, exploitation, conseil et assistance →04. Les étapes d'étude et de mise en service permettent de configurer en une seule passe les mesures de protection, tandis que celle d'exploitation se caractérise par un renouvellement régulier des services de cybersécurité, tant en fonctionnement qu'en maintenance.

Ces services, fruits de la longue expérience d'ABB, garantissent le respect des meilleures pratiques de cybersécurité conformes à la normalisation internationale. Ils poursuivent un quadruple objectif :

- Vérifier que les mises à jour ne perturbent pas le fonctionnement des infrastructures du centre ;
- Garantir une qualité de service constante et la présence de personnel qualifié ;
- Intégrer la cybersécurité à la totalité du cycle de développement des produits et solutions ABB ;
- Assurer la sécurité des solutions ABB tout au long de leur durée de vie.

Au plus près des besoins

Les exploitants de datacenters veulent sécuriser leurs réseaux, serveurs, données et périmètres, ainsi que l'infrastructure électrique et de commande. La segmentation, principe directeur de l'architecture de cybersécurité ABB, fait appel à des pare-feux qui surveillent et filtrent le trafic de données aux différents niveaux du réseau pour en améliorer la visibilité. La surveillance du réseau, qui permet de détecter les événements inhabituels, fait également partie de cet arsenal.

ABB a développé un modèle à trois niveaux pour gérer la cybersécurité des systèmes d'automatisation industrielle. À la base se trouvent des contrôles de sécurité organisationnelle et technique qui, correctement mis en place et actualisés, éliminent la majorité des menaces génériques. Le niveau 2 consiste à gérer, à entretenir, à compléter et à perfectionner ces mécanismes, quand le besoin s'en fait sentir. Enfin, le dernier niveau interface ces contrôles avec les services gérés de sécurité, par l'intermédiaire du centre d'opérations collaboratif ABB.

L'architecture de référence ABB contribue à une sécurité renforcée au niveau serveur, ainsi qu'à la mise à jour régulière des correctifs de sécurité et des bases de données de signatures des programmes malveillants. Le serveur de gestion des sauvegardes dans la DMZ suit les recommandations d'ABB en matière de plate-forme de sauvegarde et de restauration des données après incident. La sécurité des données du contrôle-commande et de l'infrastructure électrique est tout aussi vitale que celle du périmètre. Les données sécurisées, chiffrées et compressées transitent du point de collecte de données vers le serveur de journalisation, garantissant ainsi la sécurité des communications, tandis que le système d'automatisation surveille les événements sur le réseau. Enfin, ABB préconise une protection physique du datacenter lors du déploiement du système d'automatisation, afin d'assurer la sécurité périmétrique de l'infrastructure et du contrôle-commande.

— Les exploitants de datacenters peuvent compter sur ABB pour relever les enjeux de cybersécurité.

Pour complète qu'elle soit, cette architecture n'est pas l'alpha et l'oméga de la sécurité selon ABB. Le Groupe a conscience que l'adoption croissante du cloud alimente la menace cyber ; c'est pourquoi ses experts en sécurité informatique travaillent sur une solution de protection contre la falsification des données. Cette plate-forme sécurisée modulaire, qui repose sur un algorithme de chiffrement Rivest-Shamir-Adelman (RSA), garantit la sécurité d'un environnement informatique dans le cloud. Les exploitants de datacenters savent qu'ils peuvent compter sur ABB pour les aider à relever les enjeux de cybersécurité, aujourd'hui comme demain. •

— **Bibliographie**

[1] Market Research Future, *Industrial Cyber Security Market Worth 24.41 USD Billion By 2023 With 10.97 % CAGR*, disponible sur : https://www.marketresearchfuture.com/press-release/industrial-cyber-security-market, 28 septembre 2017 (consulté le 18 juin 2020).

[2] Howarth, F., *Architecting the security of the next-generation data center: Why security needs to be a key component early in the design phase*, livre blanc Bloor Research, disponible sur : https://www.bloorresearch.com/research/architecting-security-next-generation-data-centre, 9 août 2011 (consulté le 5 mai 2020).

[3] ABB, *Industry analyst ranks ABB #1 for distributed control systems globally*, disponible sur : https://new.abb.com/news/detail/9992/industry-analyst-ranks-abb-1-for-distributed-control-systems-globally, 6 novembre 2018 (consulté le 5 mai 2020).

[4] Ashford, W., « Cyber threat to industrial control systems highest yet », *Computer Weekly*, disponible sur : https://www.computerweekly.com/news/252436129/Cyber-threat-to-industrial-control-systems-highest-yet, 2 mars 2018 (consulté le 5 mai 2020).