AVIS D' EXPERT

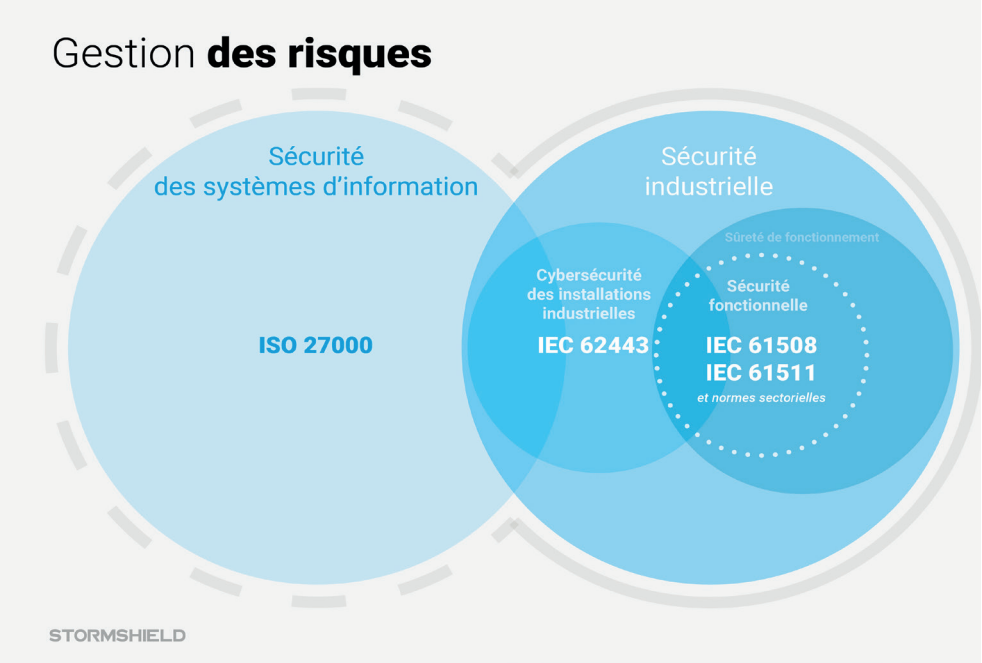
IEC 62443, LE STANDARD INCONTOURNABLE DE LA CYBERSÉCURITÉ INDUSTRIELLE

Vincent Nicaise
Responsable des partenariats et de l'écosystème industriels, Stormshield

Pendant longtemps, les risques cyber dans le monde industriel semblaient ne concerner que les secteurs sensibles, comme ceux de l'énergie ou du nucléaire. Mais des cyberattaques récentes ont démontré le contraire : peu importe la nature des réseaux opérationnels et de leurs champs d'application, ceux-ci peuvent à tout moment se retrouver exposés à des actes de malveillance informatique. D'autant plus avec la connectivité grandissante avec l'IT. Face à cette question de la cybersécurité des installations industrielles et des systèmes informatiques industriels, le standard IEC 62443 s'avère incontournable. Présentation.

UNE BASE COMMUNE POUR LA CYBERSÉCURITÉ INDUSTRIELLE

Dès 2007, les premiers référentiels spécifiques à la cybersécurité industrielle voient le jour, sous l'impulsion du comité 99 de l'ISA. Quelques années plus tard, la norme internationale IEC 62443 est née. Elle propose un cadre de cyberdéfense en profondeur des systèmes industriels, que ce soit ceux de la petite usine de production de chocolat du coin, ceux d'une station d'épuration ou ceux d'un réseau de transport. « *Une cyberattaque, même sur une petite entreprise qui fait du remplissage de boissons, peut provoquer un arrêt de production et par là même un impact financier lui-même potentiellement fatal pour l'entreprise* », explique **Khobeib Ben Boubaker**, Head of Industrial Security Business Line chez Stormshield.



Jusqu'alors il y avait d'un côté la sécurité des systèmes d'information (ISO 27000), et de l'autre la sécurité industrielle (sûreté de fonctionnement et sécurité fonctionnelle avec l'IEC 61508 et les normes sectorielles). La norme IEC 62443 sert désormais de liant à ces deux environnements qui, de fait, convergent de plus en plus. Elle constitue **un cercle vertueux au service d'une gestion du risque de cybersécurité des installations industrielles dans son ensemble.** Mais cette croisée des chemins entre l'OT et l'IT s'avère encore complexe. « *L'univers IT est très centré sur la confidentialité, l'intégrité : en cas de suspicion d'attaques, on aura tout de suite cette tendance à débrancher le système. En revanche, une usine, elle, a besoin de produire sans interruption et doit faire face aux risques humains comme environnementaux* », assure **Fabien Miquet**, Product and Solution Security Officer chez Siemens.

« L'univers IT est très centré sur la confidentialité, l'intégrité : en cas de suspicion d'attaques, on aura tout de suite cette tendance à débrancher le système. En revanche, une usine, elle, a besoin de produire sans interruption et doit faire face aux risques humains comme environnementaux »

Fabien Miquet, Product and Solution Security Officer chez Siemens

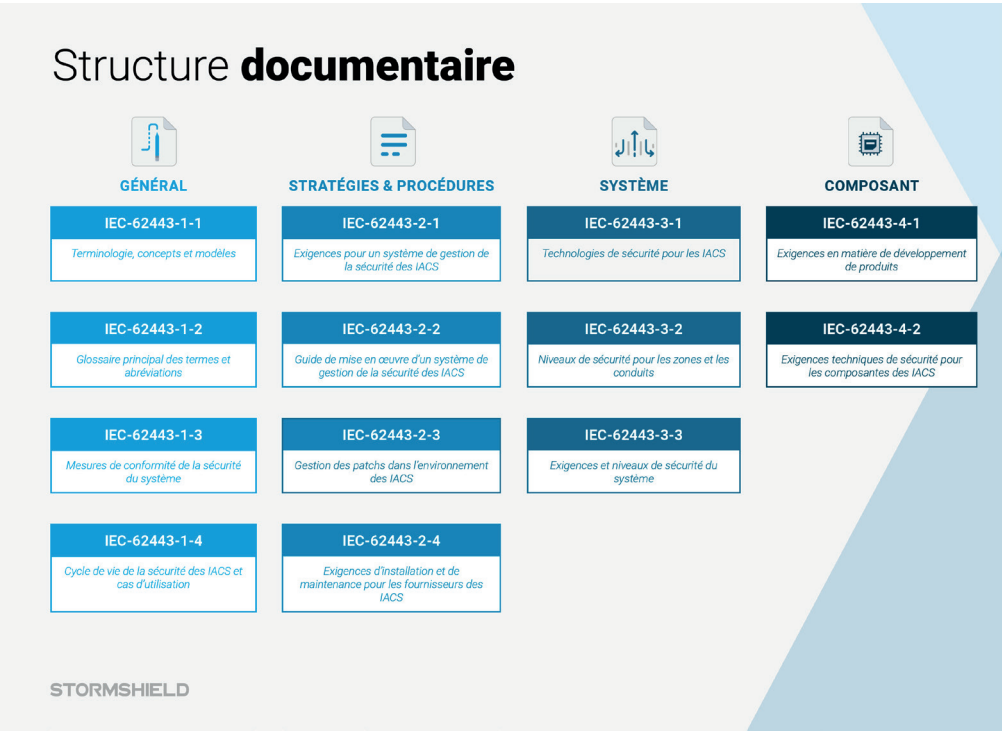
Mais la norme IEC 62443 est un ensemble de recommandations, elle ne s'impose pas aux industriels ni à leurs infrastructures critiques. Une flexibilité qui permet à la norme de s'adapter aux contextes et aux spécificités des installations critiques. « ***La norme IEC 62443 est une véritable référence pour la cybersécurité des installations industrielles, puisqu'elle sert de base commune.*** *Elle peut servir partiellement, selon les besoins, ou être complétée par une autre norme métier. Par exemple, l'IEC 61850 se réfère aux installations électriques, qui vont avoir une réalité opérationnelle différente dans une sous-station, dans un Smart Building, ou encore dans un établissement*

hospitalier », témoigne Khobeib Ben Boubaker. Cette norme semble donc nécessaire et structurante, d'autant plus que « *le monde industriel est très hétérogène de par la quantité de métiers qui le compose,* déclare **Anthony Di Prima**, Senior Manager chez Wavestone. *En fonction de si l'on appartient au monde de la chimie, de l'énergie, les composants et les systèmes diffèrent. La norme IEC 62443 porte en elle un projet d'harmonisation des bonnes pratiques cyber sur ce marché fragmenté et qui a pour habitude d'évoluer en système fermé. Ce standard permet d'évoluer vers plus d'interopérabilité et ce, avec une portée internationale* ».

IEC 62443, AU CŒUR DE LA BÊTE

La norme IEC 62443 est composée de plusieurs documents – pour publics avertis –, regroupés en quatre parties.

- **« General 62443-1 » :** ce premier volet regroupe les documents destinés au concepts généraux, à la terminologie et aux méthodes. Il définit notamment un glossaire ;
- **« Policies & procedures 62443-2 » :** ce second volet spécifie les mesures organisationnelles, et s'adresse aux exploitants et mainteneurs des solutions d'automatisation. Il contient également des recommandations dans le cadre des corrections et mises à jour des composants du système, en respectant les spécificités des infrastructures critiques industrielles (IEC-62443-2-3) ;
- **« System 62443-3 » :** ce troisième volet est dédié aux moyens opérationnels de sécurité des ICS *(Industrial Control Systems*), ou plutôt des IACS *(Industrial Automation and Control Systems)* – à ne pas confondre avec le SCADA, puisque la norme définit sa propre définition des infrastructures de contrôle-commande. Il fournit une évaluation actuelle des différents outils de cybersécurité, décrit la méthode et les moyens pour structurer leur architecture en zones et conduits et dresse un état des lieux des techniques de protection contre les cyberattaques. Il propose ainsi la segmentation des IACS par zones en fonction des niveaux de criticité des équipements (62443-3-2), tout en rappelant que ces zones pourront ensuite communiquer entre elles – que ce soit par clé USB, câble réseau ou encore liaison VPN. **Certainement le volet le plus intéressant puisqu'il présente les éléments d'une cyberdéfense en profondeur** ;
- **« Component 62443-4 » :** enfin, ce quatrième volet est destiné aux équipementiers de solutions de contrôle-commande : automates, éléments de supervision, stations d'ingénierie et autres équipements de commutation. Cette partie décrit d'une part les exigences de sécurité pour ces équipements et présente les bonnes pratiques de développement d'un produit.



« *L'IEC 62443 est la norme la plus complète du marché* : ***elle prend à la fois en compte la sécurité informatique pure et la sûreté de fonctionnement.*** *Elle est pragmatique. Dans les environnements industriels, contrairement aux environnements bureautiques, on ne peut pas mettre en œuvre de la cybersécurité si on ne prend pas en compte la sûreté de fonctionnement. C'est notamment pour cela que la norme IEC 62443 a vraiment du sens pour parler de la sécurité des systèmes informatiques industriels* », rappelle Khobeib Ben Boubaker. Pour chaque industrie, il est donc incontournable de définir les zones et conduits de son infrastructure, le niveau de risque pour chacune de ces zones et d'appliquer les mesures de sécurité associées telles que définies dans l'IEC 62443-3-3.

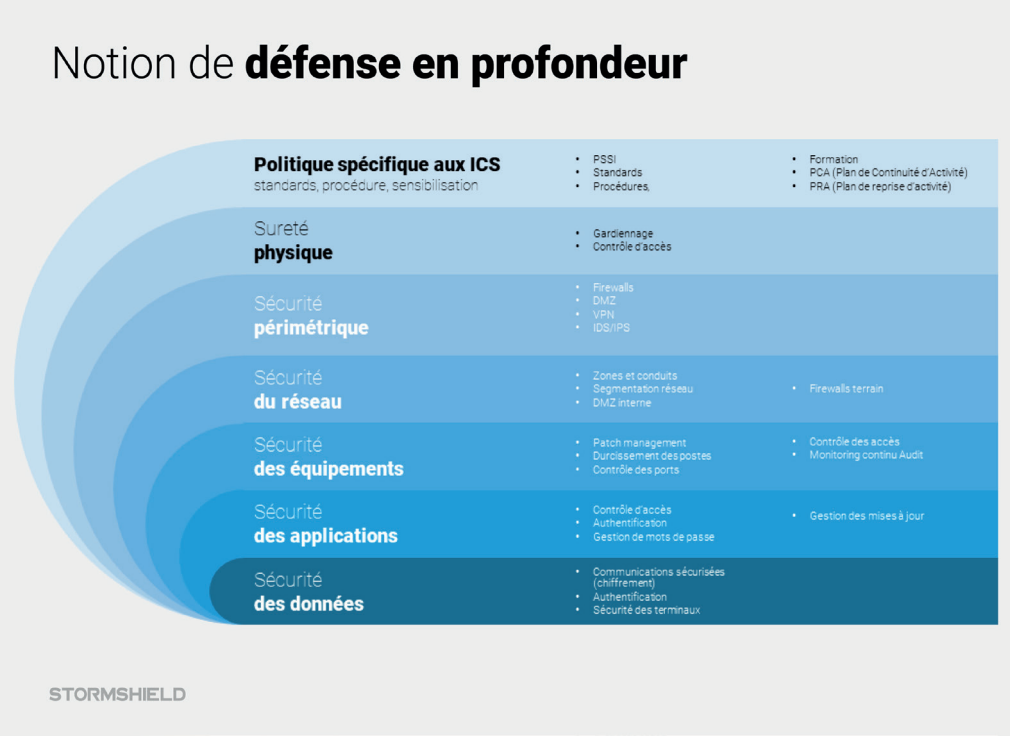
À cette répartition des zones, il convient d'appliquer les sept exigences fondamentales de la norme IEC 62443 :

- identifier et authentifier tous les utilisateurs (personnes, processus logiciels et appareils) avant d'autoriser l'accès à un système ;
- contrôler l'usage (faire respecter les privilèges attribués à un utilisateur authentifié) ;
- assurer l'intégrité des données, logiciels et équipements ;
- garantir la confidentialité des informations sur les flux de communication ainsi que dans les espace de stockage des données ;
- limiter les flux inutiles de données ;
- réagir aux attaques en informant l'autorité compétente dans les délais ;
- et garantir la résistance du système en cas d'attaque DDoS.

Pour répondre à la plupart de ces exigences de sécurité, « *le firewall est une des mesures de sécurité les plus appropriées. Pour autant, celui-ci doit être optimisé et durci physiquement. On ne peut pas déployer un firewall traditionnel dans une raffinerie ou dans un réseau d'eau car les contraintes physiques ne sont pas celles d'une salle informatique classique. Il faut qu'il puisse résister à des amplitudes de températures, à la poussière, à l'électromagnétisme* », explique **Simon Dansette**, Product Manager chez Stormshield.

UN PLAIDOYER POUR UNE CYBERDÉFENSE EN PROFONDEUR

Message fort et emblématique de la norme, le principe de défense en profondeur revient à sécuriser chaque sous-ensemble du système et s'oppose à la vision d'une sécurisation du système uniquement en périphérie. « ***La sécurité d'un système ne doit pas reposer sur une seule barrière,*** indique Fabien Miquet. *Et c'est pour cela que la norme IEC 62443 prône ce principe de défense en profondeur. Respecter ce standard est donc un gage de maturité en matière de cybersécurité.* »



Acteur engagé dans la protection des systèmes sensibles, Siemens a été l'un des premiers grands groupes à s'être référé à la norme IEC 62443 pour certifier ses processus de développement des produits d'automatisation et d'entraînement, y compris des logiciels industriels. « *La norme IEC 62443 est un des seuls standards qui permet à la fois de sécuriser au niveau industriel un produit mais aussi un ensemble de produits – un système, une solution – et même le process de développement de ce produit. Il est, de plus, reconnu de manière internationale et transverse dans le secteur industriel : idéal pour Siemens dont les activités couvrent aussi bien l'énergie, la santé, l'industrie pure (alimentation, boisson, etc.) et le bâtiment. Il s'est donc imposé logiquement,* continue Fabien Miquet. *Siemens a une trentaine d'usines certifiées IEC 62443. Nous croyons beaucoup en cette norme, au même titre que nos clients : idéal pour parler le même*

langage. »

Pour autant, **il ne faut pas oublier que le secteur industriel est complexe.** La plupart des usines manquent en effet de maturité en matière de cybersécurité, notamment à cause de systèmes mis en place pour de longues périodes (de 20 à 30 ans, voire encore davantage) et qui deviennent obsolètes. L'enjeu n'est donc pas de mettre en place des systèmes de cybersécurité pour les process des usines de demain, mais plutôt pour ceux liés aux usines d'aujourd'hui et d'hier. Changer ses machines, ses automates, reviendrait à dépenser des millions d'euros – que les entreprises n'ont pas forcément dans leurs finances à ce jour. Aujourd'hui, l'important est de mettre en œuvre un premier niveau de cybersécurité, avant qu'à terme, celle-ci ne s'impose comme une évidence dans la stratégie de développement de l'usine.

IEC 62443, UNE NORME EN CONSTANTE ÉVOLUTION

Si la rédaction de la norme IEC 62443 a débuté il y a quelques années, elle est toujours en cours. Cette norme est le fruit de groupes de travail de l'ISA (*International Society of Automation)*, ou plus précisément l'ISA GCA (*Global Cybersecurity Alliance*) sous l'égide de l'IEC (*International Electrotechnical Commission*). « *Comme les autres normes, la norme IEC 62443 doit continuer à se remettre en cause régulièrement, même dans son processus d'élaboration. Des mises à jour régulières sont nécessaires, surtout dans un environnement industriel. Un environnement et plus globalement une industrie 4.0 où de plus en plus d'objets communiquent vers l'extérieur, et où les sujets sensibles comme l'IIoT, le cloud ou encore le remote doivent être sans cesse réexaminés* », indique Anthony Di Prima. « *Plus il y aura de nouvelles fonctionnalités et de nouveaux modes de fonctionnement, plus la norme évoluera et avec elle son taux d'adoption : quantité d'appels d'offres, nationales ou internationales, se réfèrent désormais à la norme IEC 62443. On note une vraie évolution en ce sens depuis cinq ans* », souligne Khobeib Ben Boubaker.

De fait, **le développement de produits secure-by-design implique une réflexion de cybersécurité dès le début du processus.** « *Le schéma traditionnel de la conception du produit avant la question de la sécurité n'est plus de mise aujourd'hui. La cybersécurité n'est plus une option : elle est devenue une performance opérationnelle à part entière* », conclut Fabien Miquet.
