AYI NEDJIMI Consultants

IEC 62443 norme cybersécurité industrielle en pratique

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide pratique IEC 62443 : implémentation de la norme cybersécurité industrielle, Security Levels, zones et conduits, certification IACS en 2026.

Résumé exécutif

La norme IEC 62443 constitue le référentiel international de cybersécurité pour les systèmes d'automatisation et de contrôle industriels (IACS) et fournit un cadre structuré pour protéger les infrastructures critiques. Ce guide pratique décrypte ses quatre parties principales, les Security Levels allant de SL 1 contre les menaces accidentelles jusqu'à SL 4 contre les attaques étatiques, le concept fondamental de zones et conduits, et fournit une méthodologie de mise en conformité progressive adaptée aux réalités opérationnelles des sites industriels. De l'évaluation initiale des risques à la certification par des organismes accrédités, chaque étape est détaillée avec des exemples concrets d'implémentation sur des automates et des systèmes SCADA réels, permettant aux équipes de sécurité OT de structurer leur démarche de conformité de manière pragmatique et mesurable dans le temps.

Les systèmes d'automatisation et de contrôle industriels pilotent des processus physiques dont la compromission peut entraîner des conséquences catastrophiques : explosions, pollutions environnementales, interruptions de services essentiels ou pertes humaines. Face à la sophistication croissante des cyberattaques ciblant le secteur industriel, la norme IEC 62443 établit un cadre structuré et mesurable pour protéger ces systèmes critiques. Contrairement aux référentiels IT généralistes comme ISO 27001, la norme IEC 62443 prend en compte les contraintes spécifiques de l'environnement OT : priorité à la disponibilité et à la sûreté de fonctionnement, cycles de vie prolongés des équipements dépassant souvent vingt ans, protocoles propriétaires dépourvus de mécanismes de sécurité natifs, et impossibilité d'appliquer des correctifs sans fenêtre de maintenance planifiée. Cette spécificité fait de l'IEC 62443 la pierre angulaire de toute stratégie de cybersécurité industrielle sérieuse, désormais renforcée par les exigences de la directive européenne NIS 2 applicable aux opérateurs de services essentiels. Les retours d'expérience des incidents majeurs comme Stuxnet, Triton et l'attaque contre le réseau électrique ukrainien ont directement influencé les évolutions récentes de la norme, renforçant les exigences de vérification d'intégrité et de cloisonnement des systèmes instrumentés de sécurité au sein de l'architecture globale de protection.

Structure et parties de la norme IEC 62443

La norme **IEC 62443** se compose de quatre séries de documents couvrant l'ensemble du cycle de vie de la cybersécurité industrielle. La série 1 (General) définit les concepts, le vocabulaire et les modèles de référence. La série 2 (Policies & Procedures) adresse les exigences

organisationnelles pour l'exploitant du système. La série 3 (System) spécifie les exigences techniques au niveau du système intégré. La série 4 (Component) détaille les exigences de sécurité pour les composants individuels (automates, logiciels, dispositifs réseau).

La partie **IEC 62443-3-3** est la plus opérationnelle pour les architectes sécurité : elle définit les Foundational Requirements (FR) et les System Requirements (SR) que le système doit satisfaire pour atteindre un Security Level donné. Les sept FR couvrent l'identification et l'authentification (FR1), le contrôle d'utilisation (FR2), l'intégrité du système (FR3), la confidentialité des données (FR4), les flux de données restreints (FR5), la réponse aux événements (FR6) et la disponibilité des ressources (FR7). Chaque FR se décline en SR avec des niveaux d'exigence croissants, établissant un cadre directement alignable avec les pratiques de segmentation réseau et Zero Trust.

Comment déterminer les Security Levels adaptés ?

Le concept de **Security Level** (SL) constitue l'innovation majeure de la norme. Quatre niveaux définissent la résistance attendue face à des profils d'attaquants croissants. Le SL 1 protège contre les violations accidentelles ou non intentionnelles. Le SL 2 résiste aux attaques intentionnelles utilisant des moyens simples et des ressources limitées. Le SL 3 contre les attaques sophistiquées avec des moyens modérés et des connaissances spécifiques du système. Le SL 4, le plus exigeant, résiste aux attaques étatiques mobilisant des ressources étendues et une expertise avancée.

La norme distingue trois types de SL. Le *SL-T* (Target) représente le niveau de sécurité visé, déterminé par l'analyse de risque. Le *SL-C* (Capability) indique le niveau que les composants et le système peuvent atteindre par conception. Le SL-A (Achieved) mesure le niveau effectivement atteint après déploiement et configuration. L'écart entre SL-T et SL-C identifie les mesures compensatoires nécessaires, tandis que l'écart entre SL-T et SL-A révèle les vulnérabilités opérationnelles à traiter.

Security Level	Profil attaquant	Moyens	Exemple de contexte
SL 1	Non intentionnel	Accidentel	Erreur opérateur, malware générique
SL 2	Intentionnel basique	Limités, généraliste	Hacktiviste, insider mécontent
SL 3	Intentionnel avancé	Modérés, spécifique IACS	Cybercriminel organisé, APT opportuniste
SL 4	Étatique	Étendus, expertise OT	Groupe APT dédié, cyberarme

L'attaque Triton/TRISIS de 2017 contre une usine pétrochimique en Arabie Saoudite illustre la nécessité du SL 4 pour les systèmes instrumentés de sécurité (SIS). Les attaquants, attribués à un laboratoire de recherche étatique, ont développé un malware ciblant spécifiquement les contrôleurs Triconex de Schneider Electric, démontrant une connaissance approfondie des protocoles propriétaires et de l'architecture du système de sûreté. Seule une défense de niveau SL 4 aurait été appropriée pour ce type de système critique.

Méthodologie de mise en conformité IEC 62443

La mise en conformité suit un processus structuré en phases. La première phase consiste à réaliser un **inventaire exhaustif des actifs IACS** : automates, HMI, serveurs SCADA, commutateurs industriels, passerelles de protocole. Cet inventaire doit capturer les versions de firmware, les protocoles utilisés, les interconnexions réseau et les flux de données. Les outils de découverte passive comme ceux proposés par Nozomi Networks permettent cette cartographie sans perturber les processus industriels.

La deuxième phase est l'**analyse de risque** selon la méthodologie proposée dans l'IEC 62443-3-2. Elle combine l'évaluation des conséquences (impact sur la sûreté, l'environnement, la production) avec l'évaluation des menaces et des vulnérabilités pour déterminer le SL-T de chaque zone. Cette analyse doit impliquer les équipes OT, les responsables sûreté et les experts cybersécurité pour obtenir une vision complète des risques réels.

La troisième phase traduit les écarts entre SL-C et SL-T en plan de remédiation priorisé. Les mesures se répartissent entre contrôles techniques (segmentation, authentification, chiffrement), organisationnels (procédures, formation, gestion des accès) et compensatoires (surveillance renforcée quand un contrôle technique est impossible). L'approche de réponse aux incidents doit être intégrée dès cette phase de planification.

Mon avis : La certification IEC 62443 reste un objectif ambitieux que peu de sites industriels atteignent intégralement. L'approche pragmatique consiste à utiliser la norme comme grille de lecture et objectif d'amélioration continue plutôt que comme checklist binaire. Commencer par les zones les plus critiques (SIS, contrôle-commande primaire) et progresser méthodiquement vers les zones secondaires produit des résultats tangibles sans paralyser l'organisation.

Pourquoi les fabricants IACS doivent certifier leurs produits ?

La partie **IEC 62443-4-1** définit les exigences de cycle de vie de développement sécurisé pour les fabricants de composants IACS. Cette certification garantit que les automates, les logiciels SCADA et les équipements réseau industriels intègrent la sécurité dès la conception (Security by Design). Les fabricants certifiés appliquent des pratiques de modélisation des menaces, de revue de code sécurisé, de gestion des vulnérabilités et de tests de pénétration systématiques, conformément aux méthodologies de détection engineering.

La partie **IEC 62443-4-2** spécifie les exigences techniques de sécurité par type de composant : logiciel applicatif, dispositif embarqué, dispositif réseau et dispositif hôte. Chaque composant se voit attribuer un SL-C attestant de ses capacités de sécurité natives. Pour les exploitants, sélectionner des composants certifiés simplifie considérablement l'atteinte du SL-T : un automate certifié SL 3 réduit le besoin de mesures compensatoires coûteuses.

Vos fournisseurs d'automates et de SCADA disposent-ils d'une certification IEC 62443-4-1 pour leur processus de développement ?

Quelles synergies entre IEC 62443 et les autres référentiels ?

La norme IEC 62443 ne fonctionne pas en isolation. Son articulation avec **ISO 27001** est naturelle : le SMSI (Système de Management de la Sécurité de l'Information) couvre les aspects organisationnels tandis que l'IEC 62443 adresse les spécificités techniques OT. Un mapping entre les contrôles ISO 27001 Annexe A et les SR de l'IEC 62443-3-3 évite la redondance des efforts de conformité. La directive NIS 2 renforce cette convergence en exigeant des mesures de sécurité pour les réseaux et systèmes d'information des entités essentielles et importantes, incluant explicitement les systèmes industriels.

Le framework **NIST CSF** (Cybersecurity Framework) offre une vue complémentaire orientée fonctions (Identify, Protect, Detect, Respond, Recover). L'IEC 62443 se concentre davantage sur les exigences techniques spécifiques aux IACS. Les organisations matures utilisent le NIST CSF comme cadre de gouvernance global et l'IEC 62443 comme référentiel technique détaillé pour leurs systèmes industriels. Le référentiel ISA/IEC 62443 bénéficie de mises à jour régulières intégrant les retours d'expérience du terrain. Le mapping précis entre ces référentiels permet aux organisations certifiées ISO 27001 de capitaliser sur leur système de management existant et de l'étendre aux spécificités OT sans duplication d'effort. Les contrôles organisationnels comme la gestion des identités, la sensibilisation du personnel et la gestion des fournisseurs se transposent directement, tandis que les contrôles techniques nécessitent une adaptation aux protocoles et équipements industriels spécifiques.

Le cadre **MITRE ATT&CK for ICS** complète l'approche normative par une perspective offensive, documentant les tactiques et techniques réellement utilisées par les groupes de menaces ciblant les systèmes industriels. L'alignement entre les SR de l'IEC 62443-3-3 et les mitigations ATT&CK for ICS renforce la pertinence opérationnelle des contrôles déployés en les corrélant aux menaces actives observées sur le terrain.

Faut-il viser la certification ou la conformité partielle ?

La certification formelle IEC 62443, délivrée par des organismes accrédités comme TÜV ou Exida, apporte une validation externe de la posture de sécurité. Pour les *opérateurs d'importance vitale* (OIV) et les entités essentielles au sens de NIS 2, cette certification devient un avantage compétitif voire une exigence contractuelle. Les secteurs de l'énergie, du nucléaire et des transports sont les premiers concernés par cette démarche de certification intégrale.

Pour les organisations disposant de ressources limitées, une **conformité progressive** ciblée sur les zones à plus fort enjeu offre un retour sur investissement immédiat. L'approche recommandée commence par un assessment initial basé sur l'IEC 62443-2-1, identifie les quick wins (segmentation basique, durcissement des accès par défaut, suppression des mots de passe constructeur), puis établit une feuille de route pluriannuelle vers la conformité complète. Les outils de MITRE ATT&CK pour ICS facilitent la priorisation des contrôles en fonction des techniques d'attaque les plus fréquentes contre les systèmes industriels.

À retenir : L'IEC 62443 structure la cybersécurité industrielle autour de quatre piliers : la gouvernance (série 2), l'architecture système (série 3), la sécurité des composants (série 4) et les concepts fondamentaux (série 1). Les Security Levels permettent d'adapter les exigences au

profil de menace réel de chaque zone. La mise en conformité progressive, débutant par les systèmes les plus critiques, représente l'approche la plus pragmatique pour la majorité des organisations industrielles.

Sources et références : CISA ICS · ANSSI

Comment planifier les audits de conformité IEC 62443 ?

La planification des audits de conformité IEC 62443 requiert une coordination étroite avec les équipes de production pour minimiser l'impact sur les opérations. Les audits se décomposent en trois phases distinctes. La phase documentaire vérifie l'existence et la cohérence des politiques de sécurité, des procédures de gestion des accès, des plans de réponse aux incidents et des registres de gestion des changements. Cette phase peut se dérouler sans accès aux systèmes OT et constitue un point de départ accessible pour les organisations débutant leur parcours de conformité.

La phase technique évalue la conformité des configurations des équipements réseau, des automates et des systèmes de supervision par rapport aux exigences des Security Levels cibles. Les auditeurs vérifient le durcissement des systèmes d'exploitation, la robustesse des mécanismes d'authentification, la configuration des pare-feu industriels et l'efficacité de la segmentation réseau. Cette phase nécessite un accès contrôlé aux systèmes OT, idéalement planifié pendant les arrêts de maintenance programmés pour éviter tout risque sur la production. Les résultats alimentent directement le processus de disaster recovery et continuité d'activité industrielle.

La phase de validation opérationnelle teste l'efficacité des mesures de sécurité face à des scénarios d'attaque réalistes. Des exercices de type tabletop simulent des incidents cyber affectant les systèmes de contrôle, évaluant la capacité des équipes à détecter, contenir et remédier aux menaces. Les résultats de ces trois phases convergent vers un rapport d'évaluation global identifiant les écarts par rapport au SL-T et proposant un plan de remédiation priorisé avec des échéances réalistes alignées sur les cycles de maintenance industriels et les budgets disponibles.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr