

Sensibilisation à la norme ISA / IEC 62443

Formation sur étagère · 3 jours — 21 heures de formation

2025 – V1 | CABEXSI — Cabinet d'expertise en cybersécurité et systèmes d'information

1. Informations générales

INTITULÉ	Sensibilisation à la norme ISA / IEC 62443
TYPE DE FORMATION	Formation sur étagère
DURÉE	3 jours — 21 heures de formation
MODALITÉ	Présentiel sur site client — distanciel possible sur demande
PUBLIC VISÉ	Toute personne en entreprise souhaitant connaître la norme et en faire appliquer tout ou partie. Responsables de chaînes de production industrielles. Responsables sécurité (y compris IT) souhaitant comprendre les différences d'approche IT / OT. Responsables de la maintenance des systèmes d'information industriels.
PRÉREQUIS	Connaissances générales en systèmes d'information. Connaissances générales en sécurité des systèmes d'information. Une expérience en environnement industriel (OT / SCADA) est un plus.
RÉFÉRENT HANDICAP	Laurent Rousee — contact@cabexsi.com 06 22 56 29 17
TARIF	Sur devis — nous contacter : contact@cabexsi.com 06 22 56 29 17
FINANCEMENT	Potentiellement finançable par les OPCO selon les dispositifs en vigueur et les conditions propres à chaque organisme. CABEXSI vous accompagne dans le montage du dossier.

2. Objectifs pédagogiques

- Comprendre la norme ISA/IEC 62443 et sa structure
- Comprendre l'intérêt d'une norme spécifique aux IACS (Industrial Automation Control Systems)
- Comprendre la notion de Système de Management de la Cybersécurité (CSMS) et les processus associés
- Être capable d'initier une démarche de mise en conformité ISA/IEC 62443 dans son organisation

3. Compétences visées

- Capacité à comprendre les besoins de cybersécurité des systèmes industriels
- Capacité à comprendre les différentes phases (Plan, Do, Check, Act) d'un CSMS
- Capacité à cartographier les systèmes de contrôle et à les organiser en Zones et Conduits au sens de l'ISA/IEC 62443
- Capacité à définir une checklist pour identifier les écarts et démarrer une planification d'actions de remédiation
- Capacité à proposer des actions d'accompagnement en entreprise

- Capacité à expliquer la norme et ses conséquences en interne pour obtenir l'adhésion dans le plan de transformation correspondant

4. Méthodes et moyens pédagogiques

La formation est basée sur des méthodes participatives, explicatives et interrogatives, alternant apports théoriques et échanges d'expérience. La mise en pratique suit chaque séquence théorique. Le formateur ne passe pas à l'enseignement du module suivant tant que le précédent n'a pas été parfaitement compris et assimilé.

- Méthode pédagogique : expositive, participative et interrogative — alternance théorie / pratique
- Modalité : Présentiel sur site client — distanciel possible sur demande
- Matériel : écran, PC, salle de vidéoprojection, support PPTX
- Effectif recommandé : 4 à 12 participants
- En cas de session à distance, une assistance technique et pédagogique est assurée par visioconférence pendant toute la durée de la formation, avec un point de contact dédié : contact@cabexsi.com | 06 22 56 29 17

5. Évaluation des acquis

Au début et en fin de chaque module, un contrôle des connaissances vérifie que les principes et méthodes enseignés sont bien acquis avant de passer au module suivant.

- Quiz de positionnement en début de J1 (évaluation des acquis antérieurs)
- Contrôle des connaissances en fin de chaque module — le formateur ne passe au module suivant que lorsque le précédent est maîtrisé
- Exercice pratique J2 : partitionnement d'un cas industriel type en Zones et Conduits
- Synthèse finale J3 : restitution du comparatif normatif et construction d'un plan d'action
- Attestation de fin de formation remise à chaque participant à l'issue de la session

6. Indicateurs de résultats

Les indicateurs de résultats de cette action (taux de satisfaction, taux de réussite le cas échéant, effectifs formés) sont publiés et actualisés annuellement en ligne, et ne sont donc pas figés dans la présente fiche :

- Consultables sur www.cabexsi.com, rubrique Formation, en regard de chaque action
- Transmis sur demande au financeur (OPCO) et communiqués à l'entreprise cliente à l'issue de chaque session

7. Accessibilité handicap

Lors de l'entretien d'évaluation des besoins préalable à l'entrée en formation, la question de l'accessibilité liée à un handicap est systématiquement abordée. En cas de besoin identifié, le lieu, la durée, le déroulé et les supports pédagogiques peuvent être adaptés. Pour toute demande spécifique : contact@cabexsi.com | 06 22 56 29 17.

8. Modalités et délais d'accès

L'accès à la formation peut être initié par l'employeur, à l'initiative du salarié avec l'accord de ce dernier, ou à l'initiative propre du salarié. Pour chaque demande, une analyse des besoins est réalisée afin d'adapter et personnaliser le parcours, et permettre l'accueil des personnes présentant un handicap.

- Délai d'accès minimum : 1 mois avant le début de l'action, tenant compte des formalités administratives et financières
- Inscription et renseignements : contact@cabexsi.com | 06 22 56 29 17
- Convention de formation transmise et signée avant le démarrage de la session
- À l'issue de la formation, une attestation de fin de formation est remise à chaque participant

9. Programme — 3 jours / 21 heures

Chaque journée aborde les thématiques de manière interactive, sur base d'exemples et du contexte propre à l'entreprise. Les journées sont découpées en 2 demi-journées, avec une pause médiane.

Journée 1 — Fondamentaux de la norme ISA/IEC 62443

MATIN

- Présentation, objectifs de la formation
- Contexte business : menaces cyber sur les systèmes industriels, incidents majeurs
- Pourquoi une norme spécifique IACS — limites de l'approche IT classique en environnement OT
- Contenu de la norme ISA/IEC 62443 — structure générale des séries 1, 2, 3, 4
- Concepts fondamentaux : ISA-62443-1-1 — vocabulaire, modèles, politiques

APRÈS-MIDI

- Notion de CSMS (Cyber Security Management System)
- Première lecture commentée de la norme ISA-62443-2-1 (CSMS)
- Les processus du CSMS : évaluation des risques, mise en œuvre, surveillance
- Exercice : positionnement de votre organisation dans le référentiel

Journée 2 — Déploiement du CSMS et partitionnement en Zones et Conduits

MATIN

- Rappels J1 — questions ouvertes
- Monitoring et amélioration du CSMS
- Déploiement du CSMS — compréhension des étapes
- Identification des SuC (Systems under Consideration)
- Analyse de risque initiale

APRÈS-MIDI

- Partitionnement en Zones et Conduits — principes et règles
- Analyse de risque détaillée par zone
- Documentation et traçabilité requises
- Approbation des actions et validation de la démarche
- Exercice pratique : partitionnement d'un cas industriel type

Journée 3 — Niveaux de sécurité, sous-traitance et articulation normative

MATIN

- Rappels J2 — questions ouvertes
- Notion de niveaux de sécurité (SL — Security Levels) : SL cible, SL capacité, SL réalisé
- Contraintes de sécurité associées à chaque SL
- Structure des mesures de sécurité : ISA-62443-3-3 — les 7 fondements de sécurité (FR)

APRÈS-MIDI

- Gestion de la sous-traitance OT : exigences envers les intégrateurs et fournisseurs
- Comparatif avec les autres référentiels : ISO 27001, NIS 2, EBIOS RM
- Comment articuler ISA/IEC 62443 et ISO 27001 dans un programme cyber global
- Synthèse générale — construction du plan d'action individuel
- Questions / réponses finales — évaluation de la formation