

Mettre en œuvre une démarche de cybersécurité appliquée aux systèmes industriels selon les normes IEC 62443

RS7742 · RS · Publiée

L'essentiel

Code(s) NSF	326m, 326p, 200t
Formacode(s)	31006, 24491, 31045, 73054
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

BUREAU VERITAS EXPLOITATION · SIRET : 79018467501787

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification vise à permettre aux professionnels de la cybersécurité IT et aux professionnels du monde industriel d'acquérir les compétences nécessaires pour sécuriser les systèmes de contrôle-commande industriels (OT/IACS) en appliquant la norme internationale IEC 62443.

Face aux enjeux croissants de la cybersécurité industrielle dans le contexte de l'Industrie 4.0 et du renforcement des exigences réglementaires européennes, cette certification permet aux professionnels d'acquérir une compétence complémentaire stratégique pour : Analyser et évaluer les risques spécifiques aux environnements industriels (contraintes de disponibilité, sûreté, protocoles OT) ; Concevoir et mettre en œuvre des architectures de cybersécurité adaptées aux systèmes industriels ; Déployer un système de management de la cybersécurité industrielle (CSMS) conforme aux standards internationaux ; Piloter la sécurité tout au long du cycle de vie des installations industrielles. Cette certification répond aux besoins exprimés par les industriels qui exigent de plus en plus la maîtrise de la norme IEC 62443 auprès de leurs équipes internes et de leurs fournisseurs, garantissant ainsi un niveau de sécurité robuste face à l'évolution des menaces cyber.

COMPÉTENCES ATTESTÉES

Analyser le contexte de cybersécurité des systèmes de contrôle-commande industriels en identifiant les menaces, vulnérabilités et contraintes spécifiques aux environnements industriels OT par rapport aux environnements informatiques IT afin de déterminer les écarts de sécurité entre ces deux univers en s'appuyant sur les typologies d'attaques historiques et les architectures industrielles normalisées.

Concevoir l'architecture de cybersécurité d'un système industriel en appliquant les principes de segmentation réseau (découpage en zones et conduits sécurisés) et de défense en profondeur conformément à la norme IEC 62443-1-1 et 3-2 afin de réduire la surface d'attaque et atteindre le niveau de sécurité cible en utilisant les architectures de référence normalisées (modèle ISA-95) et en intégrant les contraintes opérationnelles de disponibilité et de sûreté.

Évaluer les risques de cybersécurité des installations industrielles en identifiant les actifs critiques (équipements, systèmes, données), en hiérarchisant les menaces et vulnérabilités, et en déterminant les niveaux de sécurité cibles conformément à la norme IEC 62443-3-2 afin d'élaborer un plan de traitement des risques adapté au contexte industriel en utilisant une méthodologie d'analyse de risque structurée.

Spécifier les exigences de cybersécurité des systèmes et composants industriels en sélectionnant les exigences techniques appropriées parmi les 7 familles d'exigences proposées par les normes IEC 62443-3-3 et 62443-4-2 afin de garantir la cohérence de la sécurité du système jusqu'au niveau des composants en fonction du SL-T, des risques

identifiés et en réduisant l'impact environnemental des solutions déployées par l'optimisation des ressources et la minimisation des équipements obsolètes.

Mettre en œuvre un Système de Management de la Cybersécurité Industrielle en déployant les exigences organisationnelles de la norme IEC 62443-2-1 afin d'assurer une gestion continue et structurée de la cybersécurité incluant les personnes en situation de handicap dans les dispositifs de formation et de sensibilisation en s'appuyant sur le modèle de maturité.

Formaliser les exigences de cybersécurité dans les relations contractuelles entre les acteurs industriels (propriétaire d'actifs, fournisseur de produits, fournisseur de services, intégrateur système) en élaborant des documents de contractualisation (appel d'offres, cahier des charges, spécifications techniques de sécurité) conformes à la norme IEC 62443-2-4 afin de clarifier les responsabilités, garantir la conformité des prestations et sécuriser la chaîne d'approvisionnement.

Intégrer les exigences de cybersécurité dans le cycle de développement des produits et systèmes industriels en appliquant les 8 pratiques du développement sécurisées couvrant exigences de la norme IEC 62443-4-1 afin de garantir la sécurité dès la conception et tout au long du cycle de vie en réduisant l'impact environnemental des solutions déployées par l'optimisation des ressources, la minimisation des équipements obsolètes et la réduction des déplacements grâce à des outils de télémaintenance sécurisés.

Piloter la surveillance et la gestion continue des risques de cybersécurité industrielle en déployant des processus de gestion des incidents, de gestion des correctifs (mises à jour de sécurité), de contrôle d'accès et de protection des données conformément aux exigences de la norme IEC 62443 afin de maintenir le niveau de sécurité requis tout au long du cycle de vie des installations en appliquant les principes de santé et sécurité au travail lors des interventions sur les systèmes industriels et en assurant la traçabilité et l'amélioration continue du dispositif.

Secteur d'activité et type d'emploi

RÉGLEMENTATIONS D'ACTIVITÉ

La cybersécurité industrielle s'inscrit aujourd'hui dans un environnement réglementaire et normatif particulièrement structurant, qui impacte directement les activités des organisations industrielles ainsi que les pratiques professionnelles des acteurs intervenant sur les systèmes industriels.

La certification prend explicitement en compte ce cadre réglementaire [1] et vise à en permettre la mise en œuvre opérationnelle.

[1] La directive NIS 2 ; La transposition de NIS 2 dans le cadre de la SRI 2 ; Le RGPD ; La Cyber Resilience Act (CRA) ; Le règlement DORA ; La norme internationale IEC 62443 ; La norme Internationale ISO / IEC 27001 : 2022 ; Le nouveau règlement machine (UE) 2023/1230

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Connaissance du fonctionnement managérial et organisationnel d'une structure et connaissance de base en sécurité de l'information et des systèmes industriels (validé par un questionnaire)

PRÉREQUIS À LA VALIDATION

Avoir suivi le parcours de formation de 35 heures (5 jours) sur la cybersécurité des installations industrielles IEC 62443

Avoir validé l'examen de connaissances avec un score minimum de 70/100 : Format : QCM de 100 questions (70 questions QCM + 30 questions sur mini-études de cas) - Durée : 2 heures - Cet examen valide les connaissances théoriques nécessaires avant d'accéder à l'évaluation certificative des compétences professionnelles

COMPOSITION DU JURY — FORMATION CONTINUE

Le jury de certification est ainsi composé de 2 personnes extérieures à Bureau Veritas : 2 professionnels justifiant d'au moins trois ans d'expérience en tant que professionnels de la cybersécurité et maîtrisant les normes IEC 62443 ; Externes à BVE ; Sans lien avec les candidats.

Base légale

Date de décision

30/09/2026

Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/09/2029
Date de dernière délivrance possible	30/03/2030

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	81	—	—	—
2024	24	—	—	—

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://formation.bureauveritas.fr/formation/cybersecurite/securite-industrielle/cybersecurite-des-installations-industrielles-iec-62443#sd>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/7742/>