IACS (Industrial Automation Control System) - Cyber-sécurité des Systèmes de Contrôle-Commande Industriel

CATEGORIE : C

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse :
- **INDUSTRIE**
- **INSTALLATION ET MAINTENANCE**
- **SUPPORT A L'ENTREPRISE**

Bien que la certification concerne plus particulièrement les professionnels de l'industries, elle touche également le transport, l'agriculture, la domotique, ... et tous les secteurs mettant en œuvre des systèmes opérationnels physiques (procédé, machine, véhicule, engins, ...) utilisant des automatismes et technologies numériques pour les piloter.

Code(s) NAF : **33.20C**
Code(s) NSF : **200**, **326**, **201**
Code(s) ROME : **I1102**, **H1208**, **H1206**, **I1302**
Formacode : **24454**

Date de création de la certification : **28/02/2017**
Mots clés : **Automatisme**, **informatique industrielle**, **contrôle-commande**, **Cybersécurité**

Identification

Identifiant : **3384**
Version du : **27/03/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **La sécurité des activités d'importance vitale**
- **Directive Network and Information Security (NIS)**

Non formalisé :
- **Guide pour une formation sur la cybersécurité des systèmes industriels**

Descriptif

Objectifs de l'habilitation/certification

Vérifier et valider les connaissances et les aptitudes des professionnels du contrôle-commande industriel à intégrer la prise en compte des risques de cybersécurité dans le cadre de leur activités professionnelle.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Certificat de qualification professionnelle Préventeur(trice) en cybersécurité des systèmes d'informations (CQPM)

Descriptif général des compétences constituant la certification

C1 - Intégrer une démarche de cyber sécurité durant les phases de conception, d'installation et de maintenance d'un système de contrôle-commande industriel.

C2 - Réaliser une évaluation des menaces de cyber attaque et des impacts (risque) afin d'identifier la criticité, le niveau de performance requis pour ce système.

C3 - Concevoir et exploiter des systèmes de contrôle commande, des

Public visé par la certification

- salariés
- demandeurs d'emploi

infrastructures réseaux de niveau 0/1 et 2 (CIM) suivant le niveau de performance requis et les contraintes opérationnelles et les menaces potentielles (cyber attaque).

Modalités générales

Modalités d'accès à cette certification

Avoir une expérience de trois années minimum dans le domaine du Contrôle-Commande Industriel et qui ne date pas de plus de 5 ans ;
Avoir suivi le cursus de formation Cybersécurité des systèmes industriels - OT,
Suivant les pré-requis (informatique, réseau, automatisme), trois cursus sont possibles :

Cursus automatisme :
Module ARC (Architecture des réseaux de communication) + AUT4 (IHM – supervision) + CYB

Cursus réseau
Module ARC + AUT5 (Pratique des communications industrielles) + CYB

Cursus informatique :
Module ARC + TCP-IP (maintenance et mise en œuvre des réseaux TCP-IP) + CYB

Chaque cursus se termine obligatoirement par la formation **CYB : Cybersécurité des Systèmes Industriels - OT**

Suivant le cursus la durée de la formation peut varier de 48h à 78h.

Liens avec le développement durable

niveau 2 : certifications et métiers pour lesquels des compétences évoluent en intégrant la dimension du développement durable

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

A travers son expérience, sa crédibilité et reconnaissance par le monde industriel, la certification « **IACS Cybersécurité des systèmes de contrôle-commande Industriel** » délivrée par **l'Institut de Régulation et d'Automatio**n apporte aux personnes **la reconnaissance objective de leurs compétences professionnelles** dans l'intégration des règles de l'art de sûreté contre les risques de cyberattaque.

Par la pertinence du référentiel métier et sa valorisation, le professionnel certifié pourra plus facilement faire évoluer son métier vers des activités à plus forte valeur, lui permettant une meilleure **employabilité et mobilité professionnelle nationale et internationale.**

Pour l'entité utilisatrice

La certification permet à l'entreprise de s'assurer que la personne dispose des compétences professionnelles à jour et pertinentes. Elle apporte une plus grande **confiance sur la capacité de leur personnel à accomplir des activités professionnelles conformément aux réglementations, aux règles de l'art et aux évolutions techniques et méthodologiques.**

Evaluation / certification

Pré-requis

Connaissances de base en informatique et réseau ou avoir suivi le stage ARC (architecture des réseaux de communication) ou le stage TCP-IP (Maintenance et mise en œuvre des réseaux TCP-IP).
Connaissances de base en systèmes de Contrôle-Commande et réseau ou avoir suivi le stage AUT4 (IHM - Supervision et Terminaux Opérateurs) ou le stage AUT5 (Pratique des Communications Industrielles (Industrial Automation Network).

Compétences évaluées

Les compétences évaluées (C1, C2, C3) se déclinent en différentes aptitudes et connaissances essentielles :

C1 - Intégrer une démarche de cyber sécurité durant les phases de conception, d'installation et de maintenance d'un système de contrôle-commande industriel.
- A1 — Mettre en œuvre une démarche et une méthodologie respectueuse des normes, des réglementations et de l'état de l'art.
- A2 — Veiller à ce que les moyens de défense soient adaptés à la menace et aux conséquences.
- A3 — Assurer la conformité du système de contrôle-commande aux normes et règlementation en termes cyber sécurité, de santé et sécurité au travail.
- A4 — Assurer une veille liée à la démarche de prévention en cybersécurité.

C2 - Réaliser une évaluation des menaces de cyber attaque et des impacts (risque) afin d'identifier la criticité, le niveau de performance requis pour ce système
- A5 — Identifier et évaluer les risques liés aux cyberattaques dans les différentes phases du cycle de vie de l'installation (conception, exploitation, maintenance et de démantèlement).
- A6 — Comprendre les démarches méthodologiques d'analyse des risques de cyberattaque adaptées.
- A7 — Choisir et utiliser une méthode adaptée suivant le domaine, la technologie, le niveau d'impact et l'organisation.
- A8 — Identifier le niveau d'assurance de sécurité requis (niveau SL, niveau de performance et catégorie).

C3 - Concevoir et exploiter des systèmes de contrôle commande, des infrastructures réseaux de niveau 0/1 et 2 (CIM) suivant le niveau de performance requis et les contraintes opérationnelles et les menaces potentielles (cyber attaque).
- A9 – Présenter et classer en termes de disponibilité et sécurité les différentes techniques et architectures utilisées et l'offre du marché.
- A10 – Participer à la conception ou exploitation d'une architecture optimale suivant les besoins opérationnels, les impératifs de SdF (SL et SIL requis).
- A11 - Apporter la preuve qualitative de la conformité au niveau SL (security Level) requis et à un niveau de performance.
- A12 – Intégrer et maintenir des appareils, capteurs, automates de sécurité, actionneurs en respectant les contraintes liées aux mesures anti-intrusion et cybersécurité.
- A13 – Analyser les attaques incidents et accidents, diagnostiquer et proposer des solutions techniques pertinentes en fonction des exigences et contraintes.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Centre(s) de passage/certification

- Institut de Régulation et Automation (IRA) - 23 chemin des moines - Arles

N/A

La validité est Temporaire

5 ans
Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Certificat de compétence professionnelle IRA - IACS

Plus d'informations

Statistiques

Nombre de personnes formées sur ce cursus, en 2016 : 24 , en 2017 : 42.

Nombres de certifications IACS déroulés* : 23 en 2016, 47 en 2017 (taux de réussite 58%)

* Il s'agit de certification IACS autres (Sécurité du contrôle-commande, régulation, instrumentation). Aucune certification IACS cybersécurité n'a été délivré ces deux premières années car la formation et les évaluations étaient encore en phase d'ajustement et de validation.

Autres sources d'information

Institut de Regulation et Automation

Cluster d'innovation Pédagogique et Numérique

Industrial Control System