Cybersécurité des Systèmes Critiques – Quali-SIL-CYB

SIS-CYB

NOUVEAU STAGE

Quali-SIL INERIS

Le besoin de compétence en cybersécurité est un enjeu majeur des prochaines décennies industrielles. La maîtrise des cyber-risques doit permettre de tirer parti des perspectives qu'offre l'industrie 4.0. et préserver les installations critiques. Pourtant, peu d'entreprises disposent d'une stratégie de cybersécurité globale et à jour. Ce stage permet d'obtenir la certification Quali-SIL Cyber et de prolonger de 2 ans la certification Quali-SIL ING ou CIM.

Durée
25 h sur 4 jours

Horaires
mardi 9 h - vendred 12 h

Niveau d'acquis
Maitrise ★★★

Nature des connaissances
Perfectionnement des connaissances

Modalités d'évaluation
Quali-SIL Cyber ou FS-CYB

Certification obligatoire
Quali-SIL Cyber

Participants
Mini : 2 - Maxi : 12

Responsable
Fabien CIUTAT

Formateur Principal
Fabien CIUTAT

Dates, Prix & Certification
Consulter notre site internet : www.ira.eu

Formation disponible en INTRA à la demande.

Informations Complémentaires :

- *Formateur expert en Sécurité Fonctionnelle, Automatismes et réseaux industriels*
- *Certification des compétences : Modalité : dossier* + examen (QCM) durée 2 h. Certification de compétence QUALI-SIL-CYBER délivrée par INERIS (pour les personnes déjà certifiées Quali-SIL ING (voir stage SIS-ING) Certification valable 5 ans*
- *Les repas sur Arles vous sont offerts.*

**Dossier de candidature à remplir et à remettre avant l'entrée de stage*

Présentations & Démonstrations

Objectifs :

- Savoir intégrer les exigences de cybersécurité dans le management et les étapes du cycle de vie des Systèmes Instrumentés de Sécurité.
- Savoir identifier et analyser les risques de cybersécurité pour concevoir et maintenir des systèmes résilients aux menaces afin de préserver la sécurité des installations industrielles critiques.
- Etre capable de faire le lien avec tous les acteurs du cycle de vie et instaurer une démarche commune dans le domaine de la sécurité fonctionnelle.

Public :

- Responsables projet et leaders techniques (automaticiens, info. Indus., HSE, sécurité des procédés, BE, intégrateurs de SIS, direction de service technique) avec responsabilités dans cycle de vie de sécurité.
- Utilisateurs (propriétaires d'actifs) et les intégrateurs.

Méthode Pédagogique :

- Programme bâti sur le cycle de vie de la norme CEI 61511, incluant les exigences de cybersécurité.
- Intégration des exigences réglementaires (ANSSI) et normatives (CEI 62443) dans le cycle de vie de la sécurité fonctionnelle (CEI 61508, CEI 61511).
- Exercices de mise en pratique dans le prolongement de ceux des formations SIS-ING ou SIS-TECH (même procédé étudié sous l'angle cybersécurité).

Prérequis :

- Connaissances de base en cybersécurité ou avoir suivi le stage CYB – OT (p.118).
- Connaissances en sécurité fonctionnelle ou avoir suivi le stage SIS-ING (p.120) ou SIS-TECH (p.119).
- Être titulaire d'un certificat Quali-SIL ING ou CIM en cours de validité pour la certification Quali-SIL Cyb. Plus d'informations p.142

Programme :

CADRE ET VOCABULAIRE
- Rappels vocabulaire, définitions, notions fondamentales et spécificités des systèmes industriels de sécurité (IT/OT, CIA, Sécurité/Sûreté, etc.).
- Compréhension du cyberrisque (menaces, vulnérabilités, attaquants, propriétés CIA, etc.).
- Historique et actualités (dates clés, évolutions des menaces, CERT, etc.).
- Besoins de cybersécurité des systèmes de contrôle-commande industriels dédiés à la sécurité.

RÉGLEMENTATION, NORMES ET GUIDES DE REFERENCE
- Cadre réglementaire (LPM, directive NIS, arrêtés relatifs aux secteurs d'activité d'importance vitale, ICPE et OIV, etc.).
- Normes et guides (CEI 61 511 et série CEI 61508, ISO/CEI série 27 000, CEI 62 443, NIST, ANSSI, etc.).
- Principes & concepts fondamentaux et lignes directrices (SMS, défense en profondeur, etc.).

APPRECIATION DES RISQUES DE CYBERSECURITE
- Principe du cycle de vie, inventaire et cartographie.
- Evaluation initiale des risques de cybersécurité (High-Level Risk Assessment).
- Critères d'évaluation des risques, graphe des cyber-risques, probabilités d'attaque (menaces, attaquants, scénarios/vecteurs de menaces et vulnérabilités).
- Architecture et segmentation, identification et exigences relatives aux zones et conduits, détermination des SL-T (Sécurity Level Target), Identification des contre-mesures et facteurs de réduction du risque.

SPÉCIFICATIONS DES EXIGENCES DE CYBERSÉCURITÉ (CSRS)
- Fonctions essentielles, architectures et indépendances, contre-mesures compensatoires, etc.
- Spécifications des exigences fondamentales et SL-T, vecteur par zone et conduit.
- Exigences de contrôle d'identification et d'authentification (IAC), de Contrôle d'utilisation (UC), d'intégrité du système (SI), de confidentialité des données (DC), de Flux de données réduit (RDF), de réponse en temps réel aux événements (TRE), de disponibilité des ressources (RA).

CONCEPTION ET MISE EN OEUVRE DE LA CYBERSÉCURITÉ
- Certification produits, Niveau de cyber capabilité (SL-C), SAV fournisseur.
- Design préliminaire, évaluation des contre-mesures et moyens alternatifs de réduction des risques.
- Analyse et comparaison des architectures possibles et bonnes pratiques.
- Composants réseaux, conception détaillée, détails des zones et conduits, choix de protocoles de communication répondant aux exigences de sûreté et sécurité.

INSTALLATION, MISE EN SERVICE ET VALIDATION
- Tests d'intégration, PEN tests. FAT et SAT de cybersécurité et liaison avec la sécurité fonctionnelle.
- Pre-Startup Review – Audit de configuration.

EXPLOITATION ET MAINTENANCE
- Gestion des accès : sécurité physique, accès et communications non autorisés.
- Gestion des essais (bypass, Proof Test). Détection et contrôle des intrusions (IDS, IPS).
- Événements de menaces (plans de réponse aux incidents et de remédiation, PCA/PCS).
- Évaluation et métrique de cybersécurité.

INSPECTION – AUDIT – MOC – DÉCOMMISSIONING
- Veille sur les vulnérabilités (gestion des alertes, analyse des correctifs).
- Implémentation des mises à jour / correctifs - analyse d'impact sur l'intégrité (SIL) / requalification.
- Gestion de l'obsolescence (HW & SW plus supportés) et des mises au rebut.

SYSTÈME DE MANAGEMENT DE LA CYBERSÉCURITÉ
- Politique, planification, organisation, programme de sécurité (62443-2-1).
- SMC (modèle de maturité, processus, évaluation, vérification…).
- Sensibilisation et compétence du personnel.
- Formation, compétence, responsabilité et indépendance.