

SÉCURITÉ & SÛRETÉ CYBERSÉCURITÉ SIL-SCC



Durée
30 h sur 5 jours
(hors temps de certification)

Horaires
lundi 13 h 30 - vendredi 12 h

Niveau d'acquis
Fondamentaux ★★☆☆

Nature des connaissances
Action d'acquisition des connaissances

Modalités d'évaluation
QCM, QUIZ

Participants
Mini : 2 - Maxi : 8

Responsable
Fabien CIUTAT

Formateur Principal
Fabien CIUTAT

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

**Formation disponible en
INTRA à la demande.**

Infos complémentaires

Formateur expert Sécurité.

À l'issue de la formation :
Remise d'une attestation
de formation avec
évaluation des acquis.

**Évaluation de la formation
par les stagiaires.**

**Les repas sur Arles vous
sont offerts.**

**Travaux dirigés
Études de cas**



Sécurité et Sûreté du Contrôle-Commande Industriel

Toute industrie (machine, manufacturier, système embarqué et process continu) doit intégrer les exigences de sécurité et sûreté dans le cycle de vie des systèmes de contrôle-commande.

Objectifs :

- Discuter de manière pertinente avec les différents acteurs de la sûreté et sécurité des procédés et des machines.
- Gérer la sécurité et sûreté du Contrôle-Commande industriel en suivant une démarche et une méthodologie respectueuse des normes, des réglementations et de l'état de l'art.
- Déterminer l'architecture optimale suivant les besoins, le SIL (Safety Integrity Level), et le SL (Security Level) requis.
- Valider en apportant la preuve qualitative et quantitative de la conformité au niveau de confiance (NC), niveau d'intégrité (SIL) ou niveau de performance (PL).
- Expliquer les avantages et inconvénients des différentes techniques et architectures utilisées et l'offre du marché.
- Intégrer des capteurs, automates de sécurité, actionneurs en respectant le niveau d'intégrité de sécurité (SIL) et le niveau de performance (PL) requis.

Méthode Pédagogique :

- Méthodes pédagogiques actives ajustées selon le niveau des participants.
- Méthodes inductives afin d'ancrer les principes de prévention et de sécurité intégrée.

Public :

- Tout professionnel souhaitant avoir une vision systémique des systèmes de sécurité industriels.

Prérequis :

- Avoir une expérience du milieu industriel.

Programme :

NOTIONS FONDAMENTALES ET VOCABULAIRE

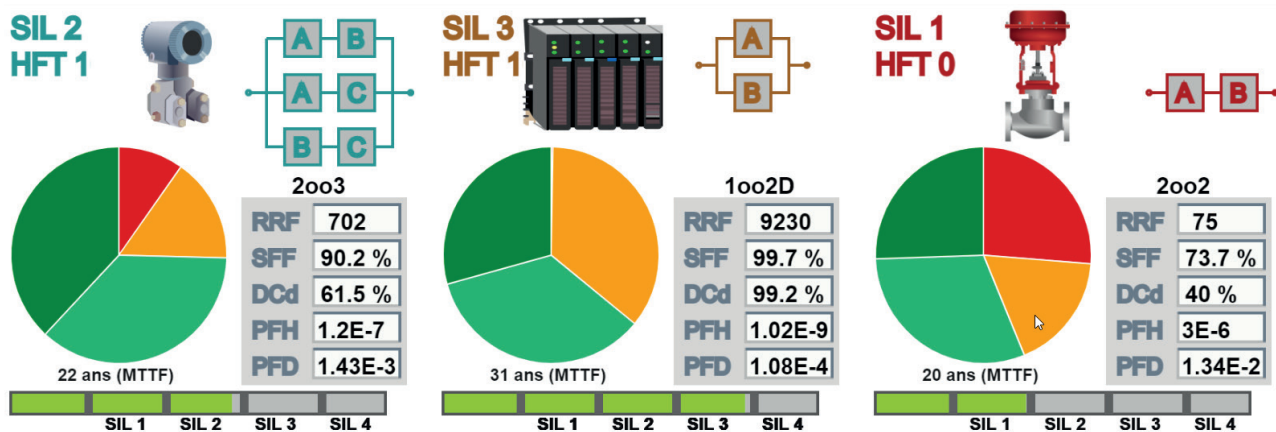
- Dangers, risques et accidents. Principe de sécurité intégrée, niveau d'intégrité, gestion des conflits sécurité / disponibilité / sûreté.
- Les différentes fonctions de sécurité et leur mode d'exploitation.
- Vocabulaire de la sûreté de fonctionnement (FMDSE, MTBF, MTTR, DC, PFD, PFH, HFT, SFF, CCF, SIF, SIL, PL, SIS, SRECS, etc).
- Calcul de fiabilité, disponibilité et intégrité des systèmes, identification et gestion des pannes aléatoires et systématiques.
- Enjeux dans le contexte européen et mondial.

CADRE RÉGLEMENTAIRE ET NORMATIF RELATIF À LA SÉCURITÉ INDUSTRIELLE

- Les directives européennes « Machine », « Seveso 3 », « ATEX », ANSSI, etc.
- Le système normatif et les normes harmonisées.
- Principe et articulation des différents Systèmes réglementaires et normatifs - synthèse.
- Mise en application de la directive « Machine » 2006/42.
- Approches déterministes et probabilistes.
- Directive SEVESO III, gestion des MMRI.
- Mesures de maîtrise des risques instrumentaux (MMRI), DT 93, note de doctrine.

DÉMARCHE D'INTÉGRATION DE LA SÉCURITÉ

- Principe de conception sûre (ISO 12100) / sécurité intrinsèque, protections, instructions.
- Évaluation des risques, analyse et appréciation des risques (ISO 14121, ISO 13849, CEI 61508, CEI 62061, CEI 61 511), Guide ANSSI, ISA 99, CEI 62443.
- Principes ergonomiques de conception des interfaces Homme / Machine.
- Cahier des charges (clauses de sécurité / sûreté et de disponibilité).
- Les outils méthodologiques (AMDEC, HAZOP, arbre des défaillances, etc).
- Identification du niveau de sécurité requis (niveau SIL, niveau de performance et catégorie) suivant les normes CEI 61511, CEI 62061 ou ISO 13849.



SYSTÈMES DE COMMANDE DE SÉCURITÉ – SRECS – SIS - EXIGENCES

- Sécurité des parties commandes et référentiels normatifs (ISO 13849, EN 954 IEC 61 508, IEC 61 511, IEC 62 061, IEC 62 061).
- Choix du référentiel suivant le domaine, la technologie, le niveau de conception et d'intégration.
- Identification du niveau de sécurité requis (niveau SIL, niveau de performance et catégorie) suivant les normes IEC 62 061 et ISO 13849.
- Exigences matérielles et organisationnelles en fonction du niveau de sécurité cible (architecture, crédibilité, fiabilité, taux de couverture, essais, défaillance de mode commun, etc).
- Étude de cas : Analyse qualitative et quantitative.
- Calcul et vérification du niveau SIL atteint.

CONCEPTION DES SYSTÈMES DE COMMANDE DE SÉCURITÉ

- Principes et techniques de sécurité (fiabilité, fail safe, tolérance aux pannes, diagnostic, sûreté, etc).
- Actions et modes positifs électriques et mécaniques.
- Composants de sécurité (relais, contacteurs, capteurs, détecteurs, interverrouillages, actionneurs, etc).
- Types d'architectures redondantes : avantages et inconvénients (1001, 1002, 1002D, 2002, 2003, 1003, etc).
- Techniques d'auto-contrôle et de diagnostic.
- Principe et câblage des blocs logiques de sécurité.
- Les automates programmables dédiés à la sécurité (APIdS).
- Principe et programmation des APIdS.
- Principes, architectures et différences par rapport à des API standards.
- Offres constructeurs (HONEYWELL, PILZ, INVENSYS TRICONEX, SIEMENS, HIMA, YOKOGAWA, EMERSON, JOKAB, ROCKWELL, SCHNEIDER).
- Réseaux de sécurité (SafetyBus, ProfiSafe, AS-I safety).
- Principes et techniques utilisés dans les communications.
- Techniques de sûreté, Cybersécurité, techniques de défense contre les attaques informatiques.