

INTÉGRITÉ DES AUTOMATISMES DE SÉCURITÉ

SÉCURITÉ DU CONTROLE-COMMANDE : SIL-SCC

DUREE : 5 Jours

OBJECTIFS DU STAGE :

Pouvoir apporter la preuve qualitative et quantitative de la conformité au niveau SIL et un niveau de performance.
Comprendre et connaître les évolutions réglementaires et normatives relatives à la sécurité des machines et process industriels.

Connaître les avantages et inconvénients des différentes techniques et architectures utilisées et l'offre du marché.
Pouvoir concevoir, installer et maintenir des automatismes de sécurité sur des machines en suivant une démarche et une méthodologie respectueuse des normes et réglementations.

Etre capable d'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 :

Exposé des méthodes et outils s'appuyant sur les normes et réglementations.

Applications sur des exemples industriels.

Utilisation de vidéos, logiciels d'animation et de calculs.

Présentation de matériels et de logiciels.

Public : Ingénieurs, techniciens et toute autre personne participant à l'optimisation ou la conception d'un système automatisé de production.

PROGRAMME :

1. NOTIONS FONDAMENTALES ET VOCABULAIRE

Danger, risques et accident. Principe de sécurité intégrée.

Pannes aléatoires et systématiques et moyens de préventions.

Vocabulaire de la sûreté de fonctionnement (FMDSE, MTBF, MTTR, DC, PFD, PFH, HFT, SFF, CCF, SIF, SIL, PL, SIS, SRECS, ...).

Calcul de fiabilité, disponibilité et intégrité des systèmes.

Conflit sécurité / disponibilité

Enjeux dans le contexte Européen.

CADRE NORMATIF RELATIF A LA SECURITE INDUSTRIELLE

Le système normatif et les normes harmonisées

Principe et articulation des différents systèmes réglementaires et normatifs - synthèse.

Approches déterministes et probabilistes.

DEMARCHE D'INTEGRATION DE LA SECURITE MACHINE

Principe de conception sûre (ISO 12100, EN 292) / sécurité intrinsèque - protections - instructions.

Evaluation des risques humains et économiques - analyse et appréciation des risques (ISO 14121, ISO 13849, CEI 61508, CEI 62061).

Principes ergonomiques de conception des interfaces Homme / Machine.

Cahier des charges (clauses de sécurité et de disponibilité).

Les outils méthodologiques (AMDEC, HAZOP, arbre des défaillances, ...).

SYSTEMES DE COMMANDES DE SECURITE : SPECS - EXIGENCES

Sécurité des parties commandes et référentiels normatifs (ISO 13849).

EN 954 IEC 61 508, IEC 61 511, IEC 62 061).

Choix du référentiel suivant le domaine, la technologie, le niveau de conception e d'intégration.

Identification du niveau de sécurité requis (niveau SIL, niveau de performance et de 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, défaillances de mode commun, ...).

Etude de cas – analyse qualitative et quantitative.

Calcul et vérification du niveau SIL atteint.

CONCEPTION DES SYSTEMES DE COMMANDE DE SECURITE

Principes et techniques de sécurité (fiabilité, failsafe, tolérances aux pannes, diagnostic).

Actions et modes positifs électriques et mécaniques.

Composants de sécurité (relais, contacteurs, capteurs, détecteurs, inter verrouillage, actionneurs).

Types d'architectures redondantes : avantages et inconvénients (1001, 1002, 1002D, 2002, 2003, 1003, ...).

Techniques d'autocontrôle 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 (HONEYWALL, PILZ, INVESYS TRICONEX, SIEMENS, HIMA, YOKOGAWA, EMMERSON, ROCKWELL, SCNEIDER ...).

Réseaux de sécurité (Safety Bus, ProfiSafe, AS-I Safety, ...).

Principes et techniques utilisés dans les communications.