

Note Méthodologique : Robots et Automatisation en Sécurité des Machines

Synthèse structurée de la démarche et des étapes de réalisation de la mission.

Contexte & finalité de la méthodologie

- Automatisation: concilier performance, continuité d'activité et prévention des dommages.
- Approche systématique: dangers → exigences → fonctions de sécurité → surveillance opérationnelle.
- Couvrir robots industriels/collaboratifs, commande, arrêts d'urgence, verrouillages, scanners.
- Finalité: prioriser, arbitrer et déployer des solutions reproductibles, ancrées dans les pratiques.
- Alignement clé: analyse de risques, PL/SIL, distances/temps de réponse, gestion des accès.

Point clé : Dimensionner les distances selon EN ISO 13855 avec temps d'arrêt mesurés et viser a minima PL d / SIL 2 pour prévenir le contact dangereux (EN ISO 13849-1, IEC 62061).

Objectifs de la mission

- Réduire les événements redoutés sans pénaliser la productivité.
 - Formaliser les critères de décision et définir des zones maîtrisées.
 - Outiller la supervision des fonctions de sécurité et la conduite du changement (incluant maintenance/équipes de nuit).
 - Obtenir un référentiel commun, des distances objectivées, des essais documentés et une traçabilité claire.
 - Déployer des listes de contrôle: fonctionnelle, organisation, technique, terrain.
 - Gouvernance: viser au minimum PL d ou SIL 2 pour les fonctions critiques, avec justification de tout écart.
-

Périmètre / livrables attendus

- Cadrage: périmètre de la cellule, modes de marche, interfaces, responsabilités.
 - Matrice risques-fonctions avec niveaux cibles PL/SIL.
 - Dossier de conception: capteurs-logique-actionneurs, redondance, diagnostic, IHM, scénarios d'arrêt.
 - Protocoles d'essais, rapports de validation, dossier technique et traçabilité.
 - Procédures d'accès/consignation, consignes visuelles, habilitations modes restreints.
 - Indicateurs d'exploitation (déclenchements, causes, temps de redémarrage) et plan de revues.
-

Démarche méthodologique (étapes)

Étape	Activités clés	Livrables / résultats
1. Cadrage et périmètre	Délimiter cellule, modes et interfaces; cartographier flux; recenser mouvements/énergies et accès.	Périmètre et responsabilités clarifiés.
2. Analyse des risques & exigences	Estimer risques; définir distances mini; cibler PL/SIL; matrice risques–fonctions.	Spécifications fonctionnelles sécurité.
3. Conception technique	Choisir composants certifiés; paramétrer STO/SLS/SS1; intégrer ergonomie et maintenabilité.	Dossier de conception et schémas.
4. Validation & essais	Plans d'essais; tests déclenchement/temps d'arrêt; diagnostic défauts; by-pass autorisés.	Protocoles, rapports, dossier technique.
5. Mise en service & consignes	Paramétrages finaux; procédures d'accès/consignation; profils utilisateurs; clés/sélecteurs; affichages.	Installation opérationnelle et habilitations.
6. Suivi & amélioration	Indicateurs; revues; analyse défauts; ajustements; MAJ analyses après changements.	Bilan de performance et plan d'actions.

Étape 1 – Cadrage et périmètre

- Actions: définir limites, modes, interfaces; cartographier flux; recenser mouvements/vitesses/énergies et accès.
- Résultat: livrable de périmètre et responsabilités.
- Vigilance: ne pas omettre un mode manuel local ou by-pass de maintenance.

Étape 2 – Analyse des risques et exigences fonctionnelles

- Actions: estimer gravité/fréquence/évitement; positionner distances; fixer PL/SIL cibles; matrice risques–fonctions.
- Résultat: exigences fonctionnelles de sécurité alignées avec l'automatisme.
- Vigilance: sur/sous-dimensionnement PL → coûts ou risque résiduel non maîtrisé.

Étape 3 – Conception des solutions techniques

- Actions: choisir composants certifiés; définir câblage/paramètres (STO, SLS, SS1); prévoir ergonomie et disponibilité.
- Résultat: dossier de conception (redondance, diagnostic, IHM, scénarios d'arrêt).
- Vigilance: ne pas confondre arrêt d'urgence et arrêt opérationnel; éviter contournements.

Étape 4 – Validation, essais et documentation

- Actions: piloter plans d'essais; tester déclenchements/temps d'arrêt; diagnostiquer défauts; vérifier by-pass autorisés.
- Résultat: protocoles, rapports d'essais, dossier technique avec traçabilité.
- Vigilance: non-reproductibilité des temps d'arrêt = doute sur distances atteintes.

Étape 5 – Mise en service, consignes et modes spéciaux

- Actions: finaliser paramétrages; structurer accès/consignation/retour auto; sécuriser profils utilisateurs, clés/sélecteurs; afficher consignes.
- Résultat: exploitation sûre avec habilitations et vitesses limitées validées.

- Vigilance: dérive des pratiques (équipes de nuit), prêt de badges; contrôler de façon réaliste et tracer.

Étape 6 – Suivi de performance et amélioration

- Actions: mettre en place indicateurs (déclenchements, causes, temps de redémarrage); tenir des revues; ajuster temporisations/distances.
- Résultat: bilans périodiques, capitalisation des retours d'expérience, MAJ des analyses de risques.
- Vigilance: toute modification méca/logicielle ⇒ réévaluation et gouvernance du changement.

Rôles & responsabilités (client / consultant)

Consultant

- Cadrer périmètre, flux, hypothèses; formaliser responsabilités.
- Structurer la matrice risques–fonctions et fixer les niveaux cibles PL/SIL.
- Concevoir l'architecture sécurité et interfaces IHM; prévenir les contournements.
- Piloter plans d'essais, enregistrements, traçabilité; livrer protocoles/rapports/dossier technique.
- Structurer procédures d'accès/consignation/retour automatique; mettre en place indicateurs et revues.

Client (HSE, méthodes, production, maintenance)

- Fournir scénarios d'usage, accès, modes spéciaux et données de mouvement/énergie.
- Conduire les tests périodiques et reconnaître les défauts en exploitation.
- Appliquer consignes; gérer habilitations et clés/sélecteurs; respecter les procédures de consignation.
- Exploiter retours d'expérience; analyser écarts; mettre à jour les analyses après changement.

Prérequis & données nécessaires (inputs)

- Cartographie des flux, limites de cellule, modes de marche, interfaces voisines.
- Mouvements, vitesses, forces, énergies; liste des accès et points d'intervention.
- Scénarios de réglage, nettoyage, déblocage; temps de réponse mesurés/cibles.
- Données de fiabilité (MTTFd/DC), performances des composants; architecture automate/variateurs sécurité existante.
- Références normatives: EN ISO 12100; EN ISO 10218-1/-2; EN ISO 13849-1; IEC 62061; EN ISO 13855; EN ISO 14119/14120; EN 61496-1.
- Moyens de test/mesure (déclenchements, temps d'arrêt) et dispositifs de traçabilité.
- Données d'exploitation: déclenchements, causes, temps de redémarrage.

Modalités de pilotage & qualité (comités, validations, risques)

- Gouvernance du changement: toute modification méca/logicielle déclenche une réévaluation formelle.
- Plans d'essais, enregistrements et traçabilité; essais périodiques terrain réalistes et tracés.
- Validation: distances selon EN ISO 13855 et temps d'arrêt mesurés; niveaux PL/SIL visés (PL d/SIL 2 min) avec justification des écarts.

- Indicateurs et revues périodiques: déclenchements, causes, temps de redémarrage; actions correctives prioritaires.
- Documentation claire et accessible pour équipes postées et maintenance.
- Maîtrise des risques de dérive: by-pass maintenance, prêt de badges, non-reproductibilité des temps d'arrêt.