Note Méthodologique : Safety in Design SID et Ingénierie de Sécurité

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

Contexte & finalité de la méthodologie

La prévention intégrée inscrit la maîtrise des risques dès l'amont des projets, de la conception à la validation.

- Articulation analyses de risques, exigences réglementaires et normes en critères d'architecture, dimensionnement, acceptation.
- Périmètre large : machines, procédés, bâtiments, utilités, logiciels de sécurité, interfaces opérateur.
- Objectif : réduire probabilité/gravité, améliorer maintenabilité et résilience, produire des preuves vérifiables sur le cycle de vie.
- Nécessite gouvernance claire, données traçables et arbitrages documentés entre performance, coûts, protection.

> **Point clé :** Prioriser la réduction à la source des dangers (ISO 12100), puis compléter par des protections et validations proportionnées.

Objectifs de la mission

- Vérifier la réduction à la source des dangers majeurs avant protections complémentaires.
- Confirmer la cohérence entre analyse de risques, spécifications et architecture technique.
- Attester la conformité aux normes et référentiels prioritaires (p. ex. ISO 45001, ISO 31000).
- Documenter les arbitrages performance / coûts / niveaux de protection.
- Valider par essais/inspections l'atteinte des niveaux cibles (SIL/PL).

Périmètre / livrables attendus

- Matrice des parties prenantes, cartographie des interfaces, charte de traçabilité.
- Base de dangers, arbres de défaillances critiques, liste d'exigences avec niveaux cibles (SIL/PL).
- Spécifications de sécurité, analyses d'architectures, matrices cause–effet.
- Stratégie et protocoles de tests, plan d'inspection/essais, procès-verbaux et plans d'actions.
- Guides d'exploitation en mode dégradé, procédures d'essais périodiques, matrice de compétences.
- Dossier technique mis à jour et preuves de conformité auditables.

Démarche méthodologique (étapes)

1) Cadrage, gouvernance et périmètre

- Diagnostic des référentiels existants; identification exigences externes (p. ex. 2006/42/CE) et internes.
- Structuration du plan de management des risques et des critères d'acceptation.
- Livrables: matrice parties prenantes, cartographie interfaces, charte de traçabilité.

2) Analyse des risques et exigences de sécurité

- Ateliers HAZID/HAZOP, AMDEC; identification des fonctions de sécurité; sélection des normes clés.
- Livrables: base de dangers, arbres de défaillances, liste d'exigences avec niveaux cibles (SIL/PL).
- Vigilance: hypothèses conservatoires tracées; mises à jour itératives; validation des scénarios dimensionnants avec MOA/exploitation.

3) Conception détaillée et spécifications

- Conversion des exigences en architectures: séparation, redondance, diagnostic; choix composants; allocation des fonctions.
- Livrables: spécifications de sécurité, analyses d'architectures, matrices cause–effet.
- Vigilance: limiter la complexité; garantir la testabilité indépendante; marges de sécurité explicites.

4) Vérification, validation et preuves

- Stratégie de tests, protocoles, revue indépendante; plan d'inspection/essais (p. ex. EN ISO 13849-2).
- Livrables: fiches de tests, PV, écarts et plans d'actions.
- Vigilance: ressources/équipements disponibles; critères d'acceptation verrouillés; gestion des dérogations formalisée.

5) Mise en service, transfert et retour d'expérience

- Transfert vers exploitation/maintenance; MAJ dossiers techniques; préparation des audits de réception (si applicable).
- Livrables: guides d'exploitation en mode dégradé, procédures d'essais périodiques, matrice de compétences.
- Vigilance: revues post-démarrage; ajustement des plans d'essais; traçabilité des évolutions sur le cycle de vie.

Étape	Activités clés	Livrables / résultats
Cadrage	Diagnostic référentiels; exigences ext./int.; plan de risque	Matrice parties prenantes; interfaces; charte traçabilité
Analyse risques	HAZID/HAZOP; AMDEC; définition fonctions; choix normes	Base de dangers; arbres; exigences avec SIL/PL
Conception	Architecture; séparation/redondance/diagnostic; composants	Specs sécurité; analyses architectures; cause–effet
Validation	Stratégie tests; protocoles; revue indépendante; PVI	Fiches tests; PV; plans d'actions
Mise en service & REX	Transfert O&M; MAJ dossiers; préparation audits	Guides modes dégradés; procédures essais périodiques; matrice compétences

Planning / durée / jalons

Jalon	Objectif	Principales sorties
Revue de cadrage	Valider périmètre, gouvernance, critères d'acceptation	Plan de management des risques; charte de traçabilité
Revue d'analyse de risques	Entériner scénarios dimensionnants et niveaux cibles	Base de dangers; exigences SIL/PL
Revue de conception	Vérifier séparation, redondance, testabilité (check-lists)	Justifications d'architecture; décisions tracées
Validation / Essais	Exécuter protocoles; formaliser preuves et écarts	PV d'essais; plans d'actions; gestion des dérogations
Mise en service & audit de réception	Transférer vers O&M; confirmer conformité	Guides modes dégradés; procédures essais périodiques
Revue post-démarrage	Capitaliser REX; ajuster fréquences d'essai	Mises à jour analyses de risques et plans d'essais

Rôles & responsabilités

Client

- Définir objectifs, périmètre et critères d'acceptation; aligner décideurs et équipe technique.
- Fournir référentiels internes, données d'entrée et accès terrain/équipements.
- Participer aux ateliers; valider scénarios dimensionnants avec MOA et exploitation.
- Allouer ressources pour essais; statuer sur arbitrages et dérogations.
- Assurer transfert à l'exploitation/maintenance; organiser essais périodiques et REX.

Consultant

- Conduire le diagnostic initial; structurer gouvernance et traçabilité.
- Animer HAZID/HAZOP/AMDEC; consolider exigences et normes applicables.
- Appuyer la conception (séparation, redondance, diagnostic) et les spécifications testables.
- Définir stratégie de tests; préparer protocoles; mener revues indépendantes.
- Accompagner transfert, préparation des audits de réception et capitalisation.

Prérequis & données nécessaires (inputs)

- Exigences externes (p. ex. 2006/42/CE, 2014/34/UE ATEX, SEVESO III) et référentiels internes identifiés.
- Données d'entrée sur dangers, scénarios, gravité/fréquence, possibilités d'évitement.
- Données de fiabilité composants: taux de défaillance, couverture diagnostique, durée de vie, facteurs communs.
- Descriptions d'architecture/processus, interfaces et contraintes d'exploitation/maintenance.
- Hypothèses conservatoires tracées; mécanisme de mises à jour itératives.

- Ressources et équipements disponibles pour essais/inspections; métrologie adaptée.
- Rôles/compétences clarifiés; indépendance de vérification prévue.
- Matrice d’applicabilité normative et critères d’acceptation définis.

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

- Gouvernance formalisée; charte de traçabilité liant danger → exigence → décision → preuve.
- Jalons de revue de conception avec check-lists; minutes, actions et décisions tracées.
- Indépendance de vérification/validation; critères d’acceptation verrouillés; gestion des dérogations.
- Boucle courte hypothèses–essais–ajustements; mise à jour continue des analyses de risques.
- Anticipation ressources/indisponibilités pour essais; modes dégradés cadrés pendant les tests.
- Définition des périodicités d’essais post-mise en service (p. ex. IEC 61511, EN ISO 13849-2).
- Surveillance des risques de dérive: périmètre flou, données lacunaires, complexité excessive, sous-estimation des temps de test.