***5. Sécurité fonctionnelle***

Concept de SIL (Safety Integrity Level) :

Définition et classification en niveaux de 1 à 4.

Application à l’automatisation industrielle.

PL (Performance Level) selon ISO 13849 : Détermination des niveaux de performance pour les systèmes liés à la sécurité.

**Sécurité Fonctionnelle**

La sécurité fonctionnelle est un concept clé dans les systèmes automatisés pour garantir que les fonctions de sécurité opèrent correctement en réponse à des conditions de danger ou de défaillance.

**Concept de SIL (Safety Integrity Level)**

Le **SIL** (niveau d'intégrité de sécurité) est un indicateur utilisé dans la norme **IEC 61508** et ses déclinaisons sectorielles (comme IEC 61511 pour les industries de processus). Il mesure la fiabilité d'une fonction de sécurité en termes de probabilité de défaillance sur demande (PFD) ou en fonctionnement continu.

**Définition des Niveaux SIL**

Les SIL sont classés en quatre niveaux : **SIL 1** à **SIL 4**, avec des niveaux plus élevés correspondant à des exigences de fiabilité accrues. Voici un aperçu des niveaux et des probabilités de défaillance :

| **SIL** | **PFD (faute sur demande)** | **Taux de défaillance (Continu)** |
| --- | --- | --- |
| SIL 1 | Entre 10−210^{-2}10−2 et 10−110^{-1}10−1 | Entre 10−610^{-6}10−6 et 10−510^{-5}10−5 |
| SIL 2 | Entre 10−310^{-3}10−3 et 10−210^{-2}10−2 | Entre 10−710^{-7}10−7 et 10−610^{-6}10−6 |
| SIL 3 | Entre 10−410^{-4}10−4 et 10−310^{-3}10−3 | Entre 10−810^{-8}10−8 et 10−710^{-7}10−7 |
| SIL 4 | Entre 10−510^{-5}10−5 et 10−410^{-4}10−4 | Entre 10−910^{-9}10−9 et 10−810^{-8}10−8 |

**Exemples d'Application**

1. **Industrie chimique/pétrolière** : systèmes de contrôle des urgences (ESD), soupapes de sécurité automatiques.
2. **Transport ferroviaire** : systèmes de signalisation et de freinage d'urgence.
3. **Énergie** : arrêt d’urgence dans les centrales nucléaires.

**Calcul et Validation**

* Une analyse de risques détermine le niveau SIL requis.
* Des méthodes comme **FMEA** (Failure Mode and Effects Analysis) et **FTA** (Fault Tree Analysis) sont utilisées pour vérifier la conformité.

**PL (Performance Level) selon ISO 13849**

Le **Performance Level (PL)**, défini dans la norme **ISO 13849**, est similaire au SIL mais plus orienté vers les systèmes mécatroniques et électromécaniques liés à la sécurité. Il évalue la capacité des systèmes à réduire les risques de manière fiable.

**Définition des Niveaux de Performance**

Les PL sont classés de **PLa** (faible fiabilité) à **PLe** (très haute fiabilité), en fonction de trois paramètres principaux :

1. **MTTFd (Mean Time to Dangerous Failure)** : Temps moyen avant une défaillance dangereuse.
2. **DC (Diagnostic Coverage)** : Taux de couverture diagnostique.
3. **CCF (Common Cause Failure)** : Défaillances causées par des causes communes.

| **PL** | **Probabilité de défaillance par heure (PFH)** |
| --- | --- |
| PLa | ≥ 10−510^{-5}10−5 à < 10−410^{-4}10−4 |
| PLb | ≥ 3×10−63 \times 10^{-6}3×10−6 à < 10−510^{-5}10−5 |
| PLc | ≥ 10−610^{-6}10−6 à < 3×10−63 \times 10^{-6}3×10−6 |
| PLd | ≥ 10−710^{-7}10−7 à < 10−610^{-6}10−6 |
| PLe | ≥ 10−810^{-8}10−8 à < 10−710^{-7}10−7 |

**Application dans l'Industrie**

* **Automatisation industrielle** : systèmes de commande de presses mécaniques.
* **Robots industriels** : capteurs de détection d'obstacles, systèmes de freinage d'urgence.
* **Transport** : barrières automatiques.

**Comparaison SIL vs PL**

| **Aspect** | **SIL (IEC 61508)** | **PL (ISO 13849)** |
| --- | --- | --- |
| **Approche** | Probabiliste | Probabiliste et structurelle |
| **Industries cibles** | Industrie de processus, énergie | Machinerie et robotique |
| **Niveaux** | SIL 1 à SIL 4 | PLa à PLe |

Les deux approches sont complémentaires et parfois utilisées ensemble pour garantir une sécurité optimale dans des contextes variés.