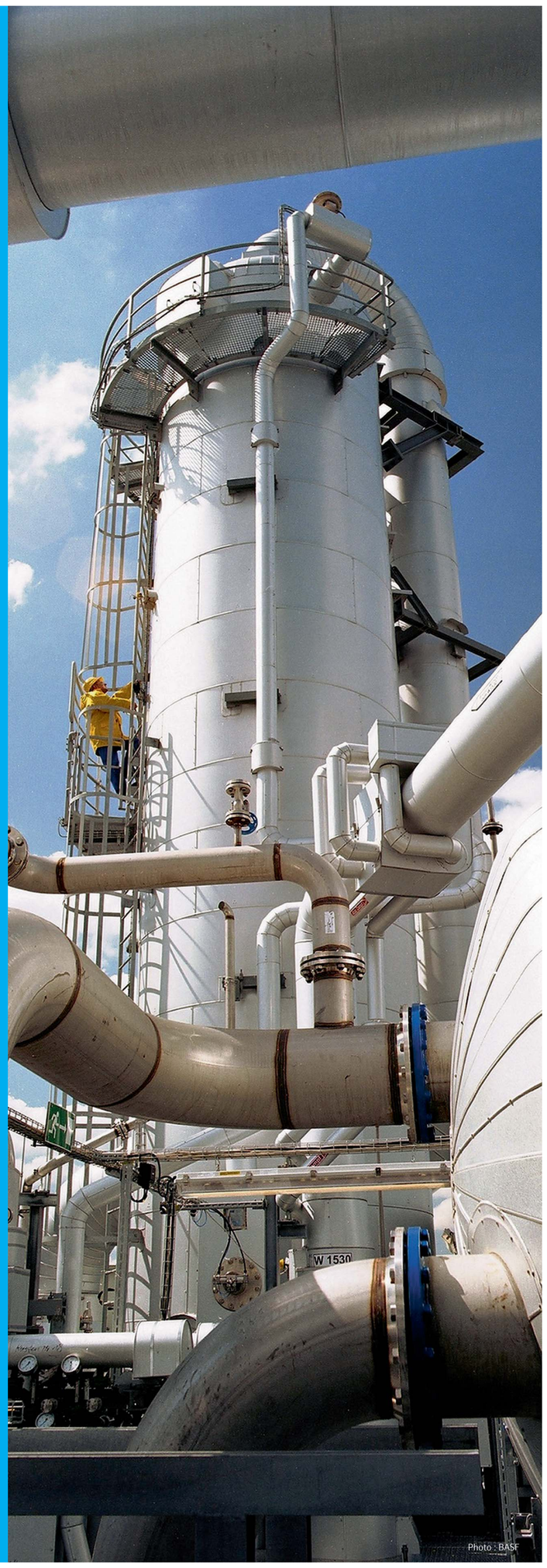
Sécurité fonctionnelle

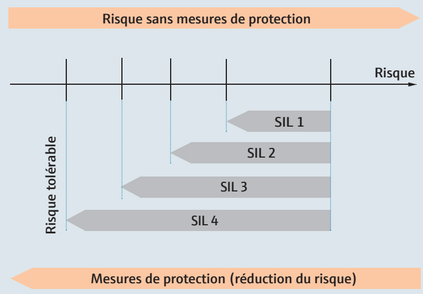
SIL (Safety Integrity Level)

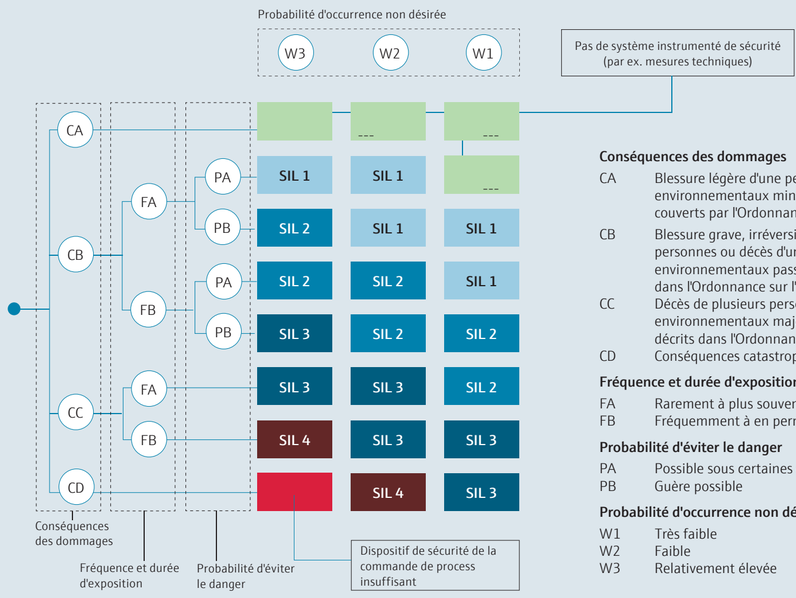


Risque lié au process

Installation de process, machine
Risques pour les personnes, l'environnement et les équipements

Réduction du risque par la mise en oeuvre de SIL





Conséquences des dommages
- CA Blessure légère d'une personne ou problèmes environnementaux mineurs, par ex. ceux qui ne sont pas couverts par l'Ordonnance sur l'incidence des dangers.
- CB Blessure grave, irréversible d'une ou de plusieurs personnes ou décès d'une personne ou problèmes environnementaux passagers majeurs, par ex. ceux décrits dans l'Ordonnance sur l'incidence des dangers.
- CC Décès de plusieurs personnes ou problèmes environnementaux majeurs de longue durée, par ex. ceux décrits dans l'Ordonnance sur l'incidence des dangers.
- CD Conséquences catastrophiques, nombreux morts.

Fréquence et durée d'exposition
- FA Rarement à plus souvent
- FB Fréquemment à en permanence

Probabilité d'éviter le danger
- PA Possible sous certaines circonstances
- PB Guère possible

Probabilité d'occurrence non désirée
- W1 Très faible
- W2 Faible
- W3 Relativement élevée

Exigences techniques

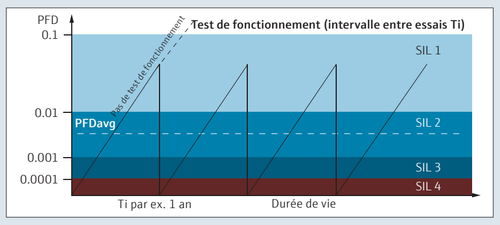
Détermination des paramètres relatifs à la sécurité
FMEDA

Exigences techniques		
Types de défaillance des fonctions et sous-systèmes de sécurité		
Type de défaillance	Détecté	Non détecté
Sûre	Sûre détectée λSD	Sûre non détectée λSU
Dangereuse	Dangereuse détectée λDD	Dangereuse non détectée λDU

SIL – PFDavg – PFH – modes de fonctionnement		
Safety Integrity Level (SIL)	Probabilité de défaillance moyenne de la fonction de sécurité à la sollicitation – PFD (probabilité de défaillance moyenne de la fonction de sécurité à faible sollicitation) (mois de 1/an)	Probabilité de défaillance dangereuse par heure – PFH (mode de fonctionnement à forte sollicitation ou continu)
SIL 4	$\geq 10^{-5}$ à $<10^{-4}$	$\geq 10^{-9}$ à $<10^{-8}$
SIL 3	$\geq 10^{-4}$ à $<10^{-3}$	$\geq 10^{-8}$ à $<10^{-7}$
SIL 2	$\geq 10^{-3}$ à $<10^{-2}$	$\geq 10^{-7}$ à $<10^{-6}$
SIL 1	$\geq 10^{-2}$ à $<10^{-1}$	$\geq 10^{-6}$ à $<10^{-5}$

SFF – HFT – SIL – type A, type B						
Taux de défaillances non dangereuses (SFFD)	**Tolérance aux pannes hardware (HFT)** (Type A – équipement simple)			**Tolérance aux pannes hardware (HFT)** (Type B – équipement complexe)		
	0	1	2	0	1 (0*)	2 (1*)
<60 %	SIL 1	SIL 2	SIL 3	Non autorisé	SIL 1	SIL 2
60 % à <90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % à <99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

* Avec vérification des performances éprouvées conformément à IEC 61511 (pour SIL ≤3 uniquement)

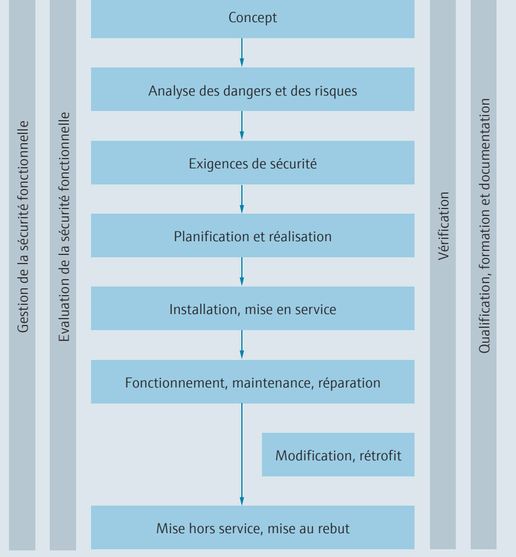


Calcul de SIL

Architecture à voie unique
Les valeurs PFDavg/PFH de tous les composants doivent être additionnées et évaluées.

PFD = ½ λDU × Ti | PFH = λDU

Exigences organisationnelles



Terminologie

- **Sécurité fonctionnelle :** Composante de la sécurité globale, qui dépend du bon fonctionnement des systèmes de sécurité pour la réduction des risques. La sécurité fonctionnelle est atteinte lorsque chaque fonction de sécurité est réalisée selon les spécifications.
- **Système de sécurité :** Système qui met en oeuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité pour les équipements sous contrôle (EUC).
- **Fonction de sécurité :** Fonction ayant pour but d'atteindre ou de maintenir un état de sécurité pour les équipements sous contrôle (EUC), en ce qui concerne un événement dangereux spécifique.
- **Cycle de vie de sécurité :** Décrit toutes les activités nécessaires à la mise en oeuvre de systèmes de sécurité, de la phase de conception à la mise hors service.
- **Gestion de la sécurité fonctionnelle :** Gestion nécessaire, activités techniques et responsabilités durant le cycle de vie de sécurité pour atteindre la sécurité fonctionnelle.
- **Evaluation de la sécurité fonctionnelle :** Vérification si la sécurité fonctionnelle a été atteinte par les systèmes de sécurité.
- **Niveau d'intégrité de sécurité (Safety Integrity Level = SIL) :** Quatre niveaux distincts (SIL 1 à SIL 4). Plus le SIL d'un système de sécurité est élevé, plus la probabilité que le système ne remplisse pas les fonctions de sécurité requises est faible.
- **Probabilité de défaillance moyenne à la sollicitation (PFDavg) :** Probabilité de défaillance moyenne d'une fonction de sécurité en mode à faible sollicitation.
- **Probabilité de défaillance par heure (PFH):** La mesure numérique de la PFH est utilisée pour les modes à forte sollicitation ou à sollicitation continue ; elle précise la probabilité d'une défaillance de la fonction de sécurité par heure (taux de défaillances dangereuses).
- **Taux de défaillances non dangereuses (SFF) :** Pourcentage de défaillances non dangereuses et de défaillances dangereuses détectées d'une fonction de sécurité ou d'un sous-système par rapport à toutes les défaillances.
- **Tolérance aux pannes hardware (HFT) :** HFT = n signifie que n+1 défauts peuvent entraîner une perte de la fonction de sécurité.
- **Mode de fonctionnement à faible sollicitation :** Fréquence de sollicitation d'un système de sécurité inférieure ou égale à une fois par an et inférieure ou égale à deux fois la fréquence du test de fonctionnement.
- **Mode de fonctionnement à sollicitation élevée ou continue :** Fréquence de sollicitation d'un système de sécurité supérieure à une fois par an ou supérieure à deux fois la fréquence du test de fonctionnement.
- **Type d'appareil A (sous-système simple) :** Les modes de défaillance de tous les composants sont bien définis et le comportement sous des conditions de défaut peut être déterminé totalement.
- **Type d'appareil B (sous-système complexe) :** Le mode de défaillance d'au moins un des composants n'est pas bien défini (par ex. µC, ASIC) et le comportement sous des conditions de défaut ne peut pas être déterminé totalement.
- **FMEDA (Failure Modes, Effects and Diagnostic Analysis) :** Méthode systématique d'identification et d'évaluation des effets des modes de défaillance des différents composants, de détermination de ce qui pourrait éliminer ou réduire le risque de défaillance, et de documentation d'un système.
- **Taux de défaillance :**
  λSD : Taux de défaillances sûres détectées
  λSU : Taux de défaillances sûres non détectées
  λDD : Taux de défaillances dangereuses détectées
  λDU : Taux de défaillances dangereuses non détectées
- **Durée moyenne de fonctionnement avant défaillance (MTBF) :** Mesure statistique du taux de défaillance pour déterminer la fiabilité d'un composant.
- **Intervalle du test de fonctionnement (T1):** Intervalle entre les tests périodiques effectués pour détecter les défaillances dans un système de sécurité.

Normes

- **Norme fondamentale :** IEC 61508
- **Normes spécifiques aux industries :**
  IEC 61511 (industrie de process)
  IEC 61513 (centrales nucléaires)
  IEC 62061 (machines)
  IEC 61800-5-2 (systèmes à entraînement mécanique)

Safety Integrity Level SIL Endress+Hauser

Endress+Hauser

People for Process Automation