

CHAPITRE 1

SOMMAIRE:

- ☐ Les risques..... P 02.
- ☐ La directive machines..... P 04.
- ☐ Les normes de sécurité..... P 05.
- ☐ Estimation du risque..... P 06.
- ☐ Signalisation de sécurité..... P 18.
- ☐ Terminologie..... P 19.

Principal risque :

- Le risque mécanique est le plus important.
- Le risque de blessure est dû à l'action mécanique d'éléments de machines, d'outils, de pièces, ou de matériaux solides ou de fluides projetés.
- L'opérateur peut être victime d'écrasement, cisaillement, coupure, happement, entraînement, emprisonnement, choc, chute...

Autres risques :

- Energie alimentant une machine :
 - électrique,
 - hydraulique,
 - pneumatique,
- Transformation des produits :
 - bruit,
 - températures extrêmes,
 - vibrations,
 - rayonnements ionisants, optiques,
 - produits polluants...

Principaux facteurs d'accident :

- Mauvaise conception des machines
- Utilisation d'une machine inadaptée aux travaux à réaliser
- Interventions en cours de fonctionnement
- Modes opératoires inappropriés et dangereux
- Insuffisance de formation des opérateurs
- Manque de sensibilisation à la sécurité des utilisateurs

Prévention :

- Eliminer les risques
- Evaluer les risques qui ne peuvent être éliminer
- Combattre les risques à la source
- Adapter le travail à l'homme

Objectif de la directive :

- Assurer un haut niveau protection de la santé et de la sécurité des salariés.
- Garantir la libre circulation des machines sur le marché de l'UE.

Aspect juridique :

- La directive machine est une directive européenne basée sur les articles 95 et 137 du traité CE.
- L'application de la directive machine se fait par des **normes européennes (EN)** :
 - Conception et estimation du risque de la machine : EN ISO 12100 et EN ISO 14121-1
 - Conception et réalisation des **systèmes de commande** relatifs à la sécurité :
EN/CEI 62061 et **EN ISO 13849-1**
 - Aspect électrique de la sécurité : EN 60204-1
- La directive machines concerne les constructeurs de machine et les exploitants procédant à des modifications affectant la sécurité de la machine.
- Le code du travail indique qu'il est interdit d'exposer, de mettre en vente, de vendre, d'importer, de céder, de mettre à disposition, de louer des machines qui ne seraient pas conformes à la directive machine.
- La conformité à la directive machine peut être garantie de plusieurs manières :
 - Vérification de la machine par un organisme de contrôle
 - Respect de normes harmonisées
 - Attestation de sécurité établie par le constructeur
- La conformité est indiquée par le marquage CE et le dossier associé.

Objectif :

- Aider les concepteurs à développer le système de commande qui assurera un niveau de sécurité désiré.
- Garantir qu'un dysfonctionnement du circuit de commande ne génère pas de situation dangereuse.

Principe :

- Norme **EN ISO 13849-1** → Niveau de performance **PL** (Performance Level)
Elle considère tous les appareils impliqués dans les fonctions de sécurité : électrique, hydraulique, mécanique, pneumatique.
- Norme **EN/CEI 62061** → Niveau d'intégrité de sécurité **SIL** (Safety Integrity Level)
Elle considère l'ensemble de la chaîne de sécurité à commande électrique.

Méthodologie :

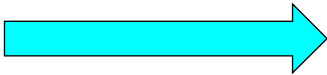
- Analyse globale des risques → détermination des fonctions de sécurité à implanter sur la machine :
 - définition des spécificités qu'elles doivent respecter (fréquence de sollicitation, temps de réponse...),
 - détermination du niveau de performance requis qu'elles doivent atteindre.
- Analyse technologiques (recherche des possibilités d'apparition d'une défaillance)
 - détermination des parties constitutives de la fonction de sécurité (matériel et logiciel)
 - estimation du niveau de performance atteint par la fonction (niveau suffisant par rapport au Plr défini par l'analyse des risques)
 - étude des combinaisons des fonctions de sécurité.

Performance Level :

➤ Le Performance Level (**PL**) est un **niveau d'aptitude à réaliser une fonction de sécurité** dans des conditions prévisibles.

➤ La valeur du PL est défini en 5 niveaux classés de a à e :

- a niveau de performance **faible**
- e niveau de performance **élevé**.

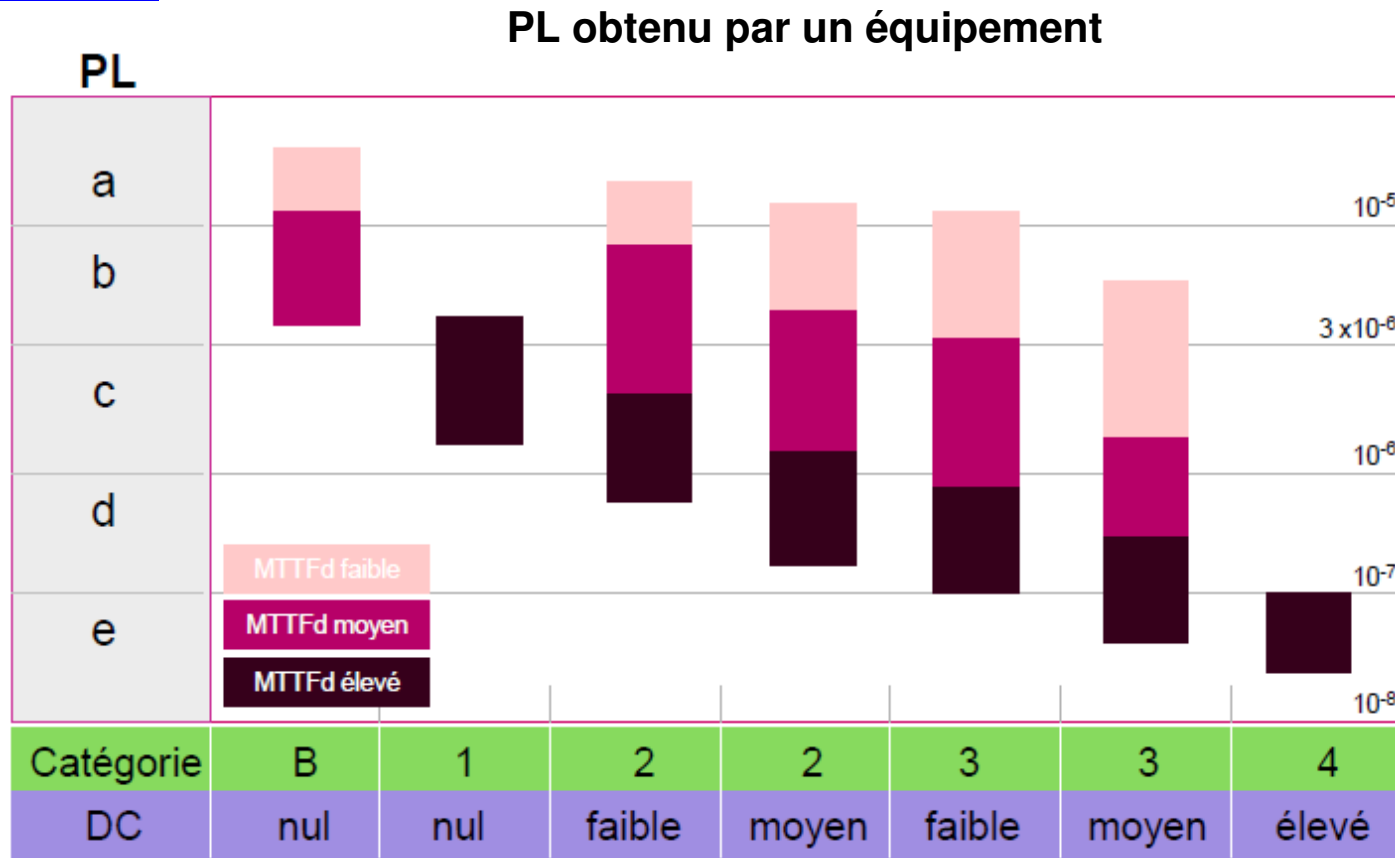
➤ Un niveau de performance est caractérisé par une **probabilité de défaillance dangereuse par heure** : 
Probability of dangerous failure per hour = PFH_D

PL	$\text{PFH}_D (1/H)$
a	$\geq 10^{-5}$ à $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ à $< 10^{-5}$
c	$\geq 10^{-6}$ à $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ à $< 10^{-6}$
e	$\geq 10^{-8}$ à $< 10^{-7}$

➤ Le PL obtenu par un équipement est déterminé par :

- ❖ la structure de son système de commande qui est définie par sa **catégorie** (catégories B, 1, 2, 3, 4 issues de la norme EN 954-1),
- ❖ son **MTTFd** (Mean Time To Failure dangerous) : temps moyen avant une défaillance dangereuse,
- ❖ son **DCavg** (Diagnostic Coverage) : mesure de l'efficacité de la surveillance des défauts,
- ❖ du **CCF** (Common Cause Failure) défaillance de cause commune : capacité d'un équipement à éviter des défaillances affectant plusieurs entités à partir d'un même événement.

Performance level :



Mean time to failure dangerous

MTTFd de chaque canal	
Indice	Gamme (an)
Faible	$3 \leq \text{MTTFd} < 10$
Moyen	$10 \leq \text{MTTFd} < 30$
Élevé	$30 \leq \text{MTTFd} \leq 100$

Diagnostic Coverage

DC	
Indice	Gamme (%)
Nulle	$\text{DC} < 60$
Faible	$60 \leq \text{DC} < 90$
Moyenne	$90 \leq \text{DC} < 99$
Elevée	$99 \leq \text{DC}$

Performance Level :

- Détermination du **niveau de performance requis** à respecter à l'aide d'un graphique de risque :

- **Gravité de la blessure : S**

- S1 = légère (blessure réversible)
- S2 = sérieuse (blessure normalement irréversible, y compris décès)

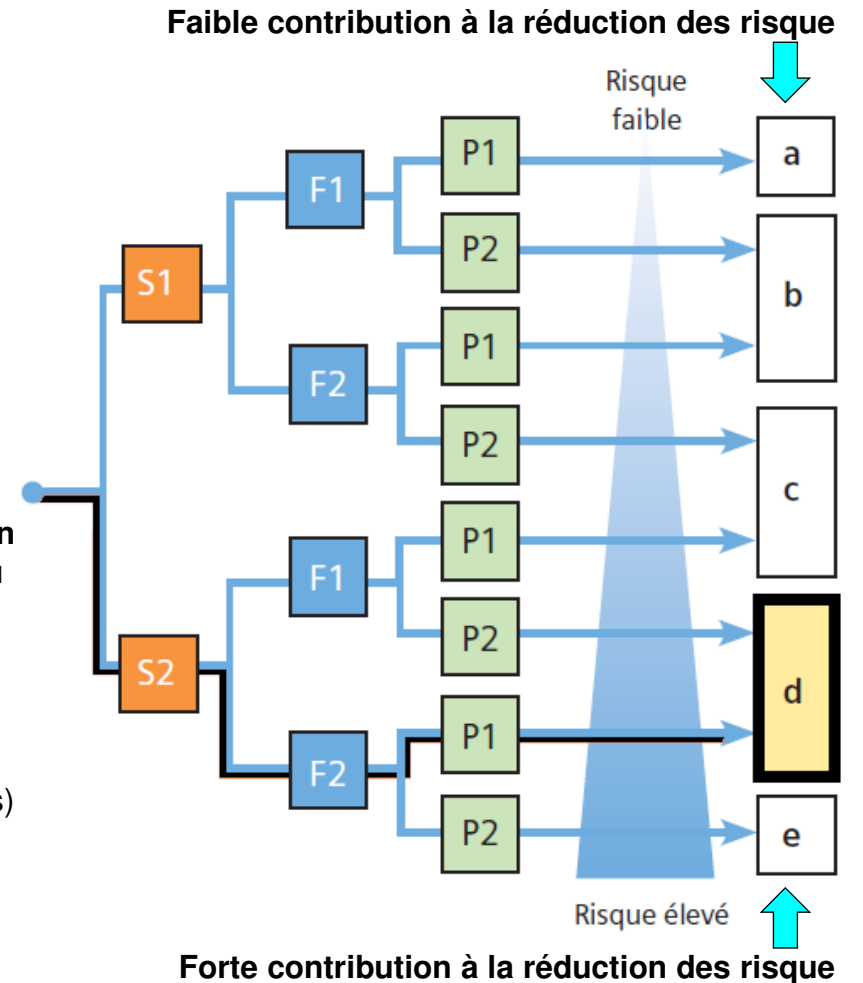
- **Fréquence et / ou exposition à un danger : F**

- F1 – rare à peu fréquente et / ou temps d'exposition court
- F2 – fréquente à continue et / ou temps d'exposition long

- **Possibilités de prévention ou de limitation du danger : P**

- P1 – Possible sous certaines conditions spécifiques
- P2 – Presque impossible

Point de départ de l'estimation de la contribution à la réduction du risque



- Vitesse à laquelle le danger se produit (exemple : rapide ou lente)
- Possibilités d'éviter le danger (exemple : par la fuite)
- Expérience pratique relative à la sécurité dans le cadre du processus
- Exploitation par un personnel formé et adapté
- Exploitation avec ou sans surveillance

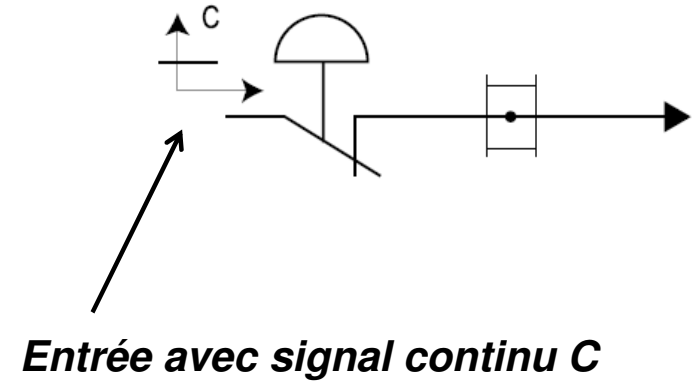
Les catégories du système de commande :

- Les catégories définissent, par rapport à la sécurité, l'architecture et **le comportement en présence de défauts des systèmes de commandes.**

Catégories	Base principale de la sécurité	Exigence du système de commande	Comportement en cas de défaut	Structure typique d'un circuit de sécurité en cas de défaut	Commentaires
B	Par la sélection des composants conformes aux normes pertinentes	Contrôle correspondant aux règles de l'art en la matière	Perte possible de la fonction de sécurité		Perte possible de la fonction de sécurité
1	Par la sélection de composants conformes aux normes pertinentes	Utilisation de constituants et de principes éprouvés	Perte possible de la fonction de sécurité. Probabilité plus faible qu'en B		<ul style="list-style-type: none"> • Pas de redondance sur E • Pas de redondance interne assurée par un relais à contacts liés mécaniquement • Pas de redondance sur S
2	Par la structure des circuits de sécurité	Test par cycle. La périodicité du test doit être adaptée à la machine et à son application	Défaut détecté à chaque test		<ul style="list-style-type: none"> • Redondance ou pas sur les entrées • La boucle de retour permet d'assurer un test cyclique sur la sortie
3	Par la structure des circuits de sécurité	Un défaut unique ne doit pas conduire à la perte de la fonction de sécurité. Ce défaut doit être détecté si cela est raisonnablement faisable	Fonction de sécurité garantie, sauf en cas d'accumulation de défauts		<ul style="list-style-type: none"> • Redondance sur les E • Redondance sur les S
4	Par la structure des circuits de sécurité	Un défaut unique (ou une accumulation de défauts) ne doit pas mener à la perte de la fonction de sécurité. Ce défaut doit être détecté dès, ou avant la prochaine sollicitation de la fonction de sécurité	Fonction de sécurité toujours garantie		<ul style="list-style-type: none"> • Redondance sur les E • Redondance sur les S • La boucle de retour permet d'assurer un test cyclique sur les sorties

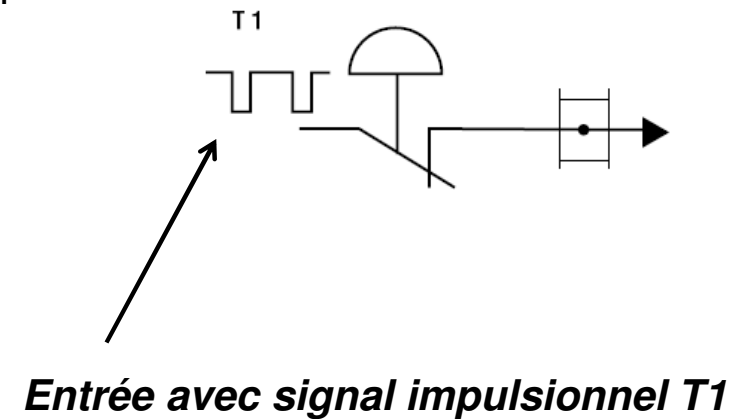
Structure d'une commande de catégorie B et 1 :

- La coupure de fil entraîne la mise en sécurité.
 - Le court circuit dans le câble n'est pas détecté.
 - Catégorie : 1 → si et seulement si il y a détection des pannes des cartes d'entrées TOR.
- B → pas de détection des pannes des cartes d'entrées TOR.



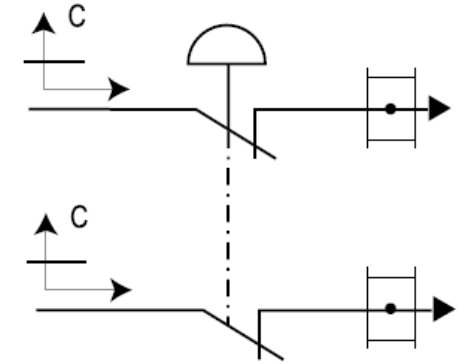
Structure d'une commande de catégorie 2 :

- La coupure de fil, l'alimentation par un signal autre que T1 et la mise à la masse entraîne la mise en sécurité.
- Le court circuit dans le câble n'est pas détecté.
- La catégorie 2 est atteinte s'il n'existe pas de risque de court-circuit dans le câble.



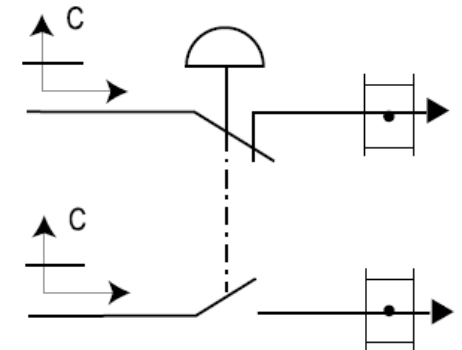
Structure d'une commande de catégorie 3 :

- Contrôle de la discordance des deux entrées par l'automate.
- La coupure de fil, la mise à la masse, les courts-circuits (sauf entre les deux entrées), les défauts de contacts de l'arrêt d'urgence, la discordance ou la désynchronisation provoquent une réaction sûre.
- Les câbles de raccordement doivent être distincts pour chaque entrées (prévention contre les risques de courts-circuits entre les câbles).



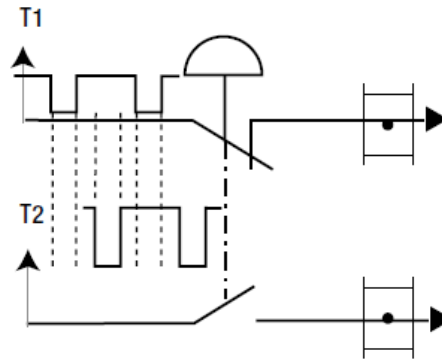
Autre structure pour la catégorie 3 :

- Contrôle de la discordance des deux entrées par l'automate.
- La coupure de fil, la mise à la masse d'une des deux entrées, les courts-circuits (dont ceux entre les deux entrées), les défauts internes de l'arrêt d'urgence, la discordance ou la désynchronisation provoquent une réaction sûre.
- Il est possible d'utiliser un seul câble.



Structure d'une commande de catégorie 4 :

- Contrôle de la discordance des deux entrées par l'automate.
- La coupure de fil, la mise à la masse des deux entrées, les courts-circuits (sauf entre les deux entrées), les défauts internes de l'arrêt d'urgence, provoquent une réaction sure.



Capteur de type de mode négatif :

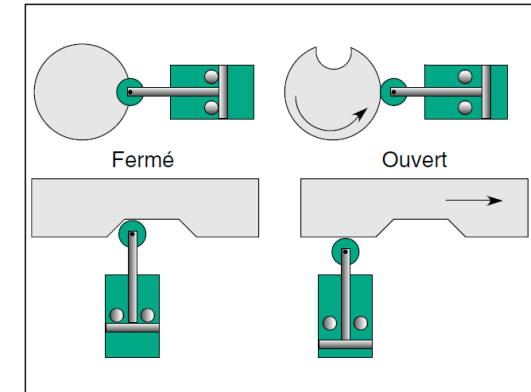
- Une action sur le capteur engendre la fermeture du contact.

Capteur de type de mode positif :

- Une action sur le capteur engendre l'ouverture du contact.

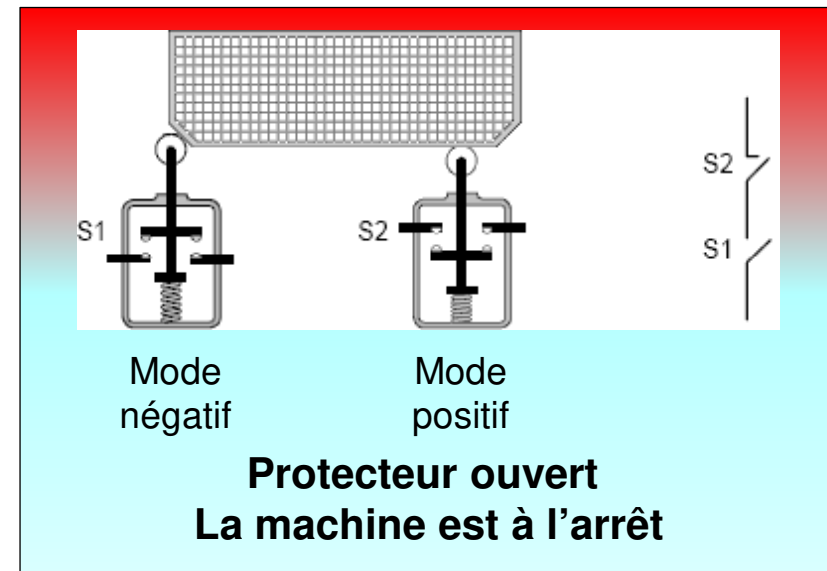
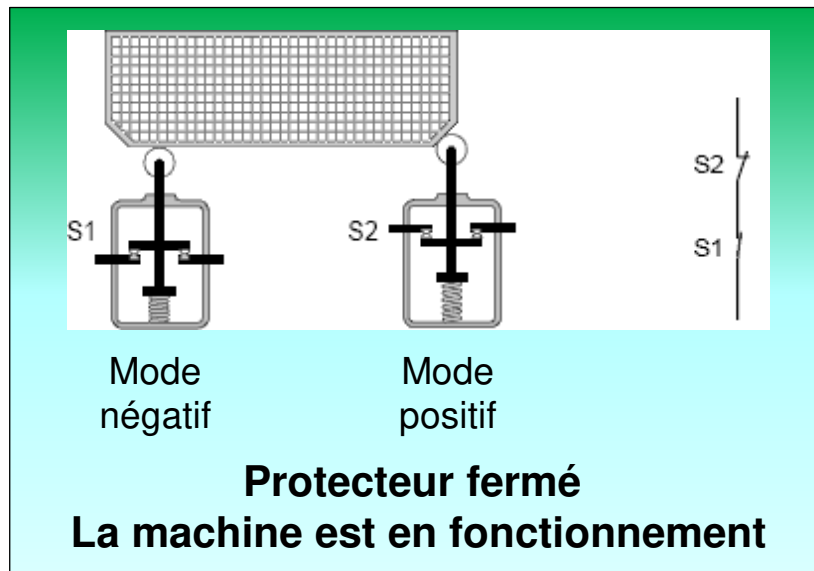


Symbole selon la norme
EN 60947-5-1



Le mode combiné :

- L'association du mode négatif pour un capteur et du mode positif pour un autre capteur permet de s'affranchir des défauts de même nature sur les deux capteurs .



Safety Integrity Level :

- Le Safety Integrity Level (**SIL**) est une **quantification** du **niveau de réduction de risque** spécifié pour une fonction de sécurité sur un procédé.
- La valeur du SIL est un nombre entier compris entre 1 et 4.
- Plus la valeur du SIL est élevée, plus la **réduction** du risque est importante.
- Le SIL obtenu par un équipement est déterminé par :
 - ❖ la probabilité de défaillances dangereuses d'une fonction de sécurité,
 - ❖ la tolérance aux pannes hardware (HFT),
 - ❖ le taux de défaillances non dangereuses,
 - ❖ le type des composants,
 - ❖ la périodicité des tests,
 - ❖ la durée de vie utile.

SIL	PFD Probabilité de défaillance à la solicitation	RRF Facteur de réduction de risque	PFH Probabilité de défaillance dangereuse par heure
1	10^{-1} à 10^{-2}	10 à 100	10^{-5} à 10^{-6}
2	10^{-2} à 10^{-3}	100 à 1 000	10^{-6} à 10^{-7}
3	10^{-3} à 10^{-4}	1000 à 10 000	10^{-7} à 10^{-8}
4	10^{-4} à 10^{-5}	10 000 à 100 000	10^{-8} à 10^{-9}

Safety Integrity Level :

- Détermination du **niveau de réduction de risque** à respecter :

- **Conséquence du dommage**

- **CA** = blessure légère d'une personne ou problèmes environnementaux mineurs.
- **CB** = blessure grave, irréversible d'une ou de plusieurs personnes ou décès d'une personne ou problèmes environnementaux passagers majeurs.
- **CC** = décès de plusieurs personnes ou problèmes environnementaux majeurs de longue durée.
- **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 conditions
- **PB** = rarement possible

- **Probabilité de concrétisation**

- **W1** = très faible
- **W2** = faible
- **W3** = relativement élevée

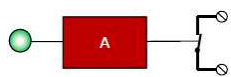
			Probabilité de concrétisation		
			W3	W2	W1
Conséquence du dommage	CA			—	—
		FA	SIL 1	SIL 1	—
		PB	SIL 2	SIL 1	SIL 1
	CB	PA	SIL 2	SIL 2	SIL 1
Fréquence et durée d'exposition		FB	SIL 3	SIL 2	SIL 2
		PA	SIL 3	SIL 3	SIL 2
		PB	SIL 4	SIL 3	SIL 3
	CC	FA	SIL 4	SIL 3	SIL 3
Probabilité d'éviter le danger		FB	—	SIL 4	SIL 3
		PA			
		PB			
	CD	FA			

Conséquence du dommage
 Fréquence et durée d'exposition
 Probabilité d'éviter le danger

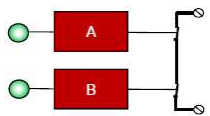
Système de sécurité du contrôle des process insuffisant

Tolérance aux erreurs matérielles (HFT) :

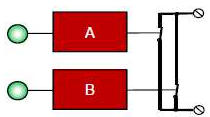
- L'**architecture** d'une fonction de sécurité est déterminée par la **tolérance aux erreurs matérielles** de ces composants. Une tolérance de N erreurs matérielles signifie que N+1 erreurs matérielles peuvent conduire à une perte de la fonction de sécurité.
- Tolérance aux erreurs matérielles : elle est fixée par l'**architecture "MooN"** (*M out of N : M voies sur N*) utilisée.
 - M : nombre de voies redondantes **requis** pour **assurer** la fonction de sécurité
 - N : nombre total de voies redondantes de la fonction de sécurité



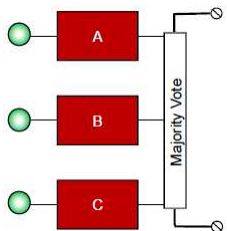
- **Architecture 1oo1** : système à voie unique (mono canal)
Une défaillance de la voie entraîne immédiatement la perte de la fonction de sécurité.
HFT = 0



- **Architecture 1oo2** : système redondant à deux voies (double canal : 1 capteur bicanal ou 2 capteurs monocanal)
Chacune des 2 voies peut exécuter la fonction de sécurité
HFT = 1



- **Architecture 2oo2** : système à deux voies
La fonction de sécurité est déclenchée uniquement par l'action des deux voies simultanément.
HFT = 0







- **Architecture 2oo3** : système redondant à trois voies
2 voies sont nécessaires pour activer la fonction de sécurité. Une voie ayant une erreur matérielle, la fonction de sécurité est encore assurée
HFT = 1

Correspondance PL /SIL :

Probabilité moyenne d'une défaillance Dangereuse par heure 1/h	PL	SIL	SYSTEM INTEGRITY LEVEL
$\geq 10^{-5}$ à $< 10^{-4}$	a	SIL	Pas de correspondance
$\geq 3 \times 10^{-6}$ à $< 10^{-5}$	b	SIL	1
$\geq 10^{-6}$ à $< 3 \times 10^{-6}$	c	SIL	1
$\geq 10^{-7}$ à $< 10^{-6}$	d	SIL	2
$\geq 10^{-8}$ à $< 10^{-7}$	e	SIL	3

Couleurs et formes de sécurité :

Couleur de sécurité	Signification ou but	Couleur de contraste	Couleur des symboles
Rouge	Danger, interdiction	Blanc	Noir
Jaune	Prudence	Noir	Noir
Vert	Sécurité (protection, premiers secours)	Blanc	Blanc
Bleu	Obligation, information	Blanc	Blanc

Couleur	Forme		
			 
Rouge	Interdiction		Matériel de lutte contre l'incendie
Jaune		Attention! Risque de danger	
Vert			Situation de sécurité, dispositifs de secours
Bleu	Obligation		Information ou instruction

Combinaison des voyants lumineux de signalisation :

Couleur	Signification	Explication	Action de l'opérateur	Exemples d'application
ROUGE	URGENCE	Etat dangereux	Action immédiate pour traiter l'état dangereux (exemple : déclenchement d'un arrêt d'urgence)	- Pression en dehors des limites de sécurité; - Chute de tension; - <u>Surcourse</u> au-delà de la position d'arrêt,
JAUNE	ANORMAL	Etat anormal entraînant un état critique imminent	Surveillance ou intervention, (exemple : rétablissement d'une fonction désirée)	- Température en dehors d'une page de fonctionnement normal; - Déclenchement d'un dispositif de protection.
VERT	NORMAL	Etat normale	Libre	- Autorisation de démarrer; - Indication des limites normales de travail.
BLEU	OBLIGATOIRE	Indication d'un état qui requiert l'action de l'opérateur	Action prescrite obligatoire	- Demande pour régler des valeurs présélectionnées.
BLANC	NEUTRE	Toute signification : peut être utilisée à chaque fois qu'il y a un doute sur l'utilisation des couleurs ROUGE, JAUNE, VERT, BLEU	Surveillance	- Information générale

Redondance :

- La redondance est l'utilisation de plus d'un système, pour garantir qu'en cas de défaillance d'un système, un autre soit disponible pour effectuer les fonctions de sécurité.
- Si la première défaillance n'est pas détectée, l'apparition d'une deuxième pourra entraîner la perte de la fonction de sécurité.

Autocontrôle :

- L'autocontrôle consiste à vérifier automatiquement le fonctionnement d'un dispositif de sécurité qui intervient dans le cycle de la machine. Par conséquent, le cycle suivant pourra être interdit ou autorisé.