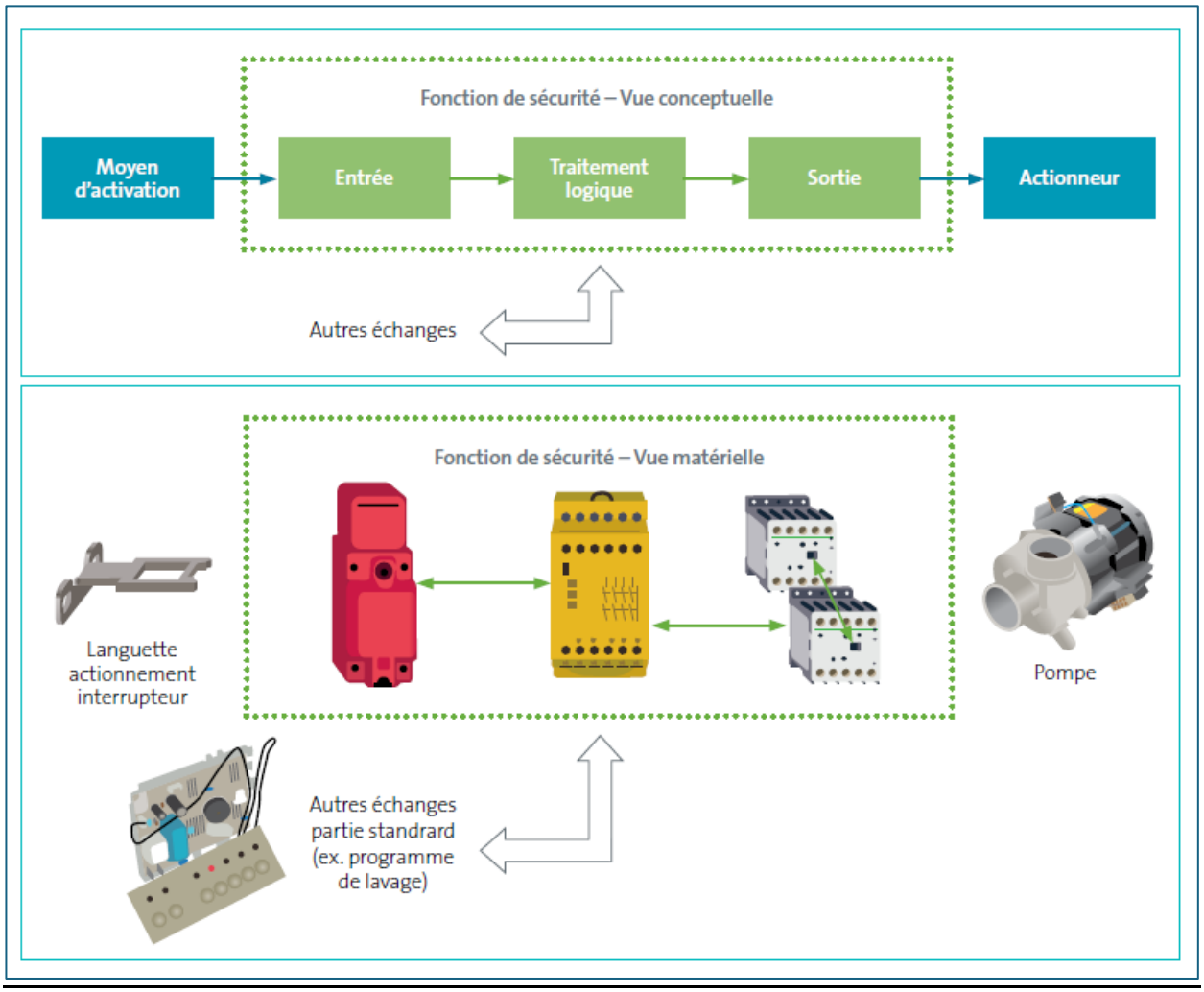
Détermination d'un Système de Commande de la Fonction de Sécurité (SC/FS)

Source : document INRS.
Sécurité des machines.
Principes de conception des systèmes de commande.

En application de la norme NF EN ISO 13849-1 :

<u>Décomposition d'un (SC/FS) et éléments externes</u>

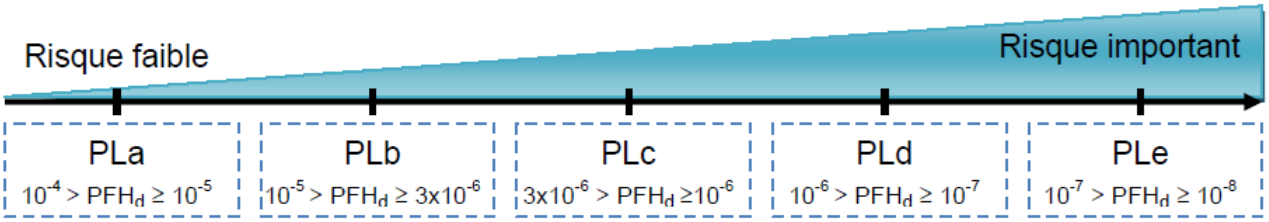


<u>Niveau de performance (PL)</u>

*Mesure **quantitative** de la fiabilité d'une fonction de sécurité, exprimée de **a à e** (du plus faible au plus fort). Il dépend de la probabilité moyenne de défaillance dangereuse par heure (**PFHd**).*

Un Système de Commande de la Fonction de Sécurité (SC/FS) doit posséder un certain niveau de performance de sécurité pour pouvoir assurer la fonction de sécurité qui lui est confiée. La capacité d'un SC/FS à réaliser une fonction de sécurité est exprimée au travers de la détermination du niveau de performance (PL). La norme définit 5 niveaux de performance possibles pour un système de commande, qui s'échelonnent de PL « a » à PL « e ».

Pour chaque niveau de performance, la norme fait correspondre une valeur de probabilité moyenne d'une défaillance dangereuse par heure (PFHd) du système de commande. Une défaillance est qualifiée de dangereuse lorsqu'elle peut conduire à une situation potentiellement dangereuse.

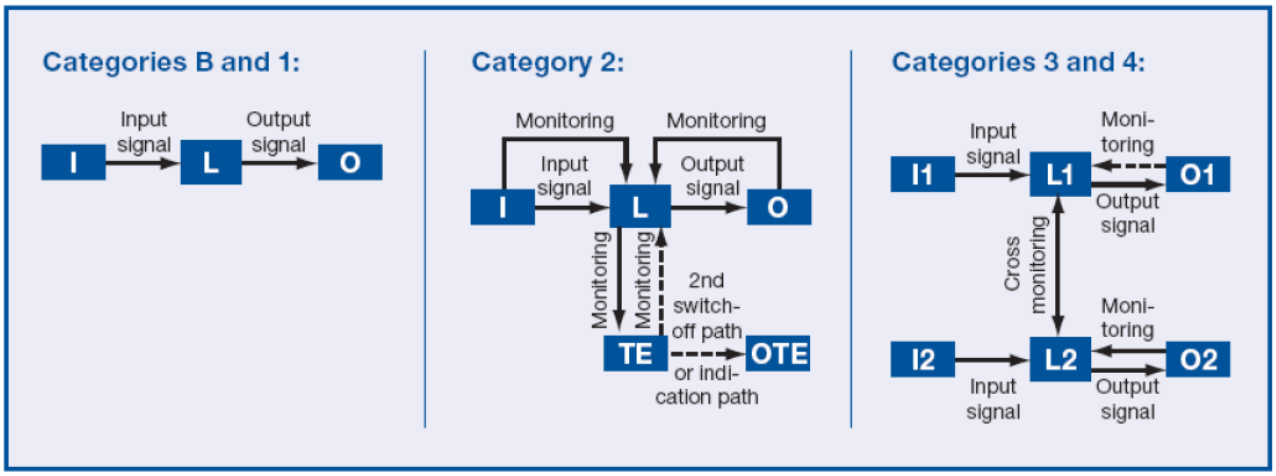


Catégorie

*Classification **structurelle** d'un système de commande selon son **architecture** et sa **capacité à résister aux défaillances**. Les catégories vont de **B, 1, 2, 3 à 4**.*

Catégorie	Résumé des exigences	Comportement du Système	Base principale de la Sécurité
B	Les parties des systèmes de commande relatives à la sécurité et/ou les dispositifs de protection ainsi que leurs pièces constitutives doivent être choisis et/ou réalisés, assemblés et/ou combinés dans le respect des Normes applicables de manière à faire face aux influences attendues.	L'apparition d'un défaut peut conduire à la perte de la fonction de sécurité	Principalement caractérisé par le choix des composants
1	Les exigences de B doivent être remplies. Des composants et des principes éprouvés doivent être absolument utilisés	L'apparition d'un défaut peut conduire à la perte de la fonction de sécurité mais la probabilité d'une telle apparition est inférieure à celle de la catégorie B	Principalement caractérisé par le choix des composants
2	Les exigences de B ainsi que l'utilisation de principes de sécurité sont obligatoires. La fonction de sécurité doit être vérifiée périodiquement en observant le résultat effectif sur la commande de la machine.	L'apparition d'un défaut peut conduire à la perte de la fonction de sécurité entre 2 vérifications. La perte de la fonction de sécurité doit être identifiée par une vérification	Principalement caractérisé par la structure du système de sécurité.
3	Les exigences de B ainsi que l'utilisation de principes de sécurité sont obligatoires. Les éléments constitutifs du système de sécurité doivent être réalisés de sorte que: ▪ L'apparition d'un défaut unique dans chacun de ces éléments ne puisse pas conduire à la perte de la fonction de sécurité et ▪ Dans le cas où il est possible de détecter le défaut, celui-ci soit effectivement reconnu.	Lors de l'apparition d'un défaut unique, la fonction de sécurité est toujours conservée. Les défauts principaux sont reconnus. L'apparition d'un défaut non reconnu peut conduire à la perte de la fonction de sécurité	Principalement caractérisé par la structure du système de sécurité.
4	Les exigences de B ainsi que l'utilisation de principes de sécurité sont obligatoires. Les éléments constitutifs du système de sécurité doivent être réalisés de sorte que: ▪ L'apparition d'un défaut unique dans chacun de ces éléments ne puisse pas conduire à la perte de la fonction de sécurité et ▪ Le défaut soit détecté avant ou au moment de l'appel à la fonction de sécurité ▪ Ou si cela n'est pas possible, l'accumulation de plusieurs défaut ne conduise pas à la perte de la fonction de sécurité.	Lorsque les défauts se produisent, la fonction de sécurité est toujours conservée. Les défauts sont reconnus à temps afin de prévenir la perte de la fonction de sécurité	Principalement caractérisé par la structure du système de sécurité.

Architecture électrique :



Mono canal | Mono canal + Test | Double canal

Relations entre Catéforie et niveau de performance (PL)

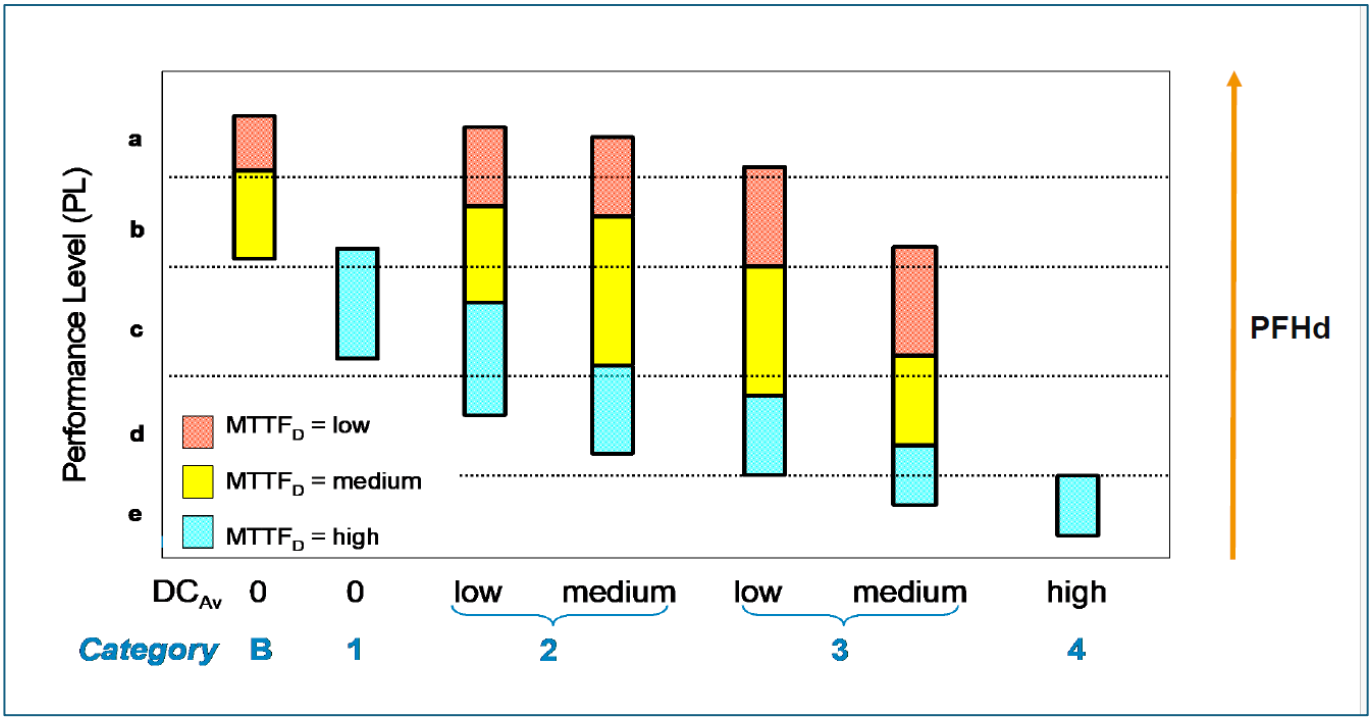
*La **catégorie** influence le **PL atteignable**, mais ne le détermine pas seule.*
*Le **PL** dépend de trois paramètres principaux :*

1. ***Catégorie (architecture)***
2. ***MTTFd** (Durée moyenne de fonctionnement avant défaillance (dangereuse)) — fiabilité des composants*
3. ***DCavg** (Diagnostic Coverage) — couverture de diagnostic*
   Plus le DCavg est élevé, plus le système détecte ses propres défaillances et agit avant qu'elles ne provoquent un danger.

Ainsi, pour une même catégorie, le PL peut varier selon la qualité des composants et des diagnostics.

Catégorie	Principe de fonctionnement	DCavg (Couverture de diagnostic)	MTTFd (Fiabilité composants)	PL atteignable	Commentaire
B	Mesures de base – conception sûre, mais sans détection de défaut	– (aucun diagnostic) <60%	Faible → Haut	a	Convient aux risques faibles ; une seule défaillance peut conduire à une perte de la fonction de sécurité.
1	Comme Cat. B, mais avec composants fiables	– (aucun diagnostic) <60%	Moyen à Haut	a → b	Fiabilité accrue mais sans détection de défauts.
2	Diagnostic par tests périodiques	Faible 60%≤DC<90%	Moyen à Haut	b → c	Une défaillance entre deux tests peut rester non détectée.
3	Architecture redondante, détection partielle des fautes	Moyen 90%≤DC<99%	Moyen à Haut	c → d	Une seule défaillance ne doit pas entraîner la perte de la fonction de sécurité.
4	Architecture redondante + surveillance continue	Élevé ≥99%	Moyen à Haut	d → e	Même en cas de défaillances multiples, la sécurité est maintenue ; niveau de fiabilité maximal.

Relations entre PL, Catégorie, MTTFd, PFHd et DCavg



PL : Niveau de performance

MTTFd : Durée moyenne de fonctionnement avant défaillance (dangereuse) — fiabilité des composants

MTTF$_d$	Plage de valeur
Faible	3 ans ≤ MTTF$_d$ <10 ans
Moyen	10 ans ≤ MTTF$_d$ < 30 ans
Elevé	30 ans ≤ MTTF$_d$ < 100 ans

DCavg : Couverture de diagnostic

PFHd : Probabilité moyenne de défaillance dangereuse par heure.

Relations entre PL, Catégorie, MTTFd, PFHd et DCavg

Tableau K.1 (*suite*)

	Probabilité moyenne d'une défaillance dangereuse par heure (1/h) et niveau de performance correspondant (PL)											
$MTTF_d$ pour chaque canal années	Cat. B DC_{avg} = nulle	PL	Cat. 1 DC_{avg} = nulle	PL	Cat. 2 DC_{avg} = faible	PL	Cat. 2 DC_{avg} = moyenne	PL	Cat. 3 DC_{avg} = faible	PL	Cat. 3 DC_{avg} = moyenne	PL	Cat. 4 DC_{avg} = élevée	PL
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

PL : Niveau de performance

MTTFd : Durée moyenne de fonctionnement avant défaillance (dangereuse) — fiabilité des composants

DCavg : Couverture de diagnostic

PFHd : Probabilité moyenne de défaillance dangereuse par heure.

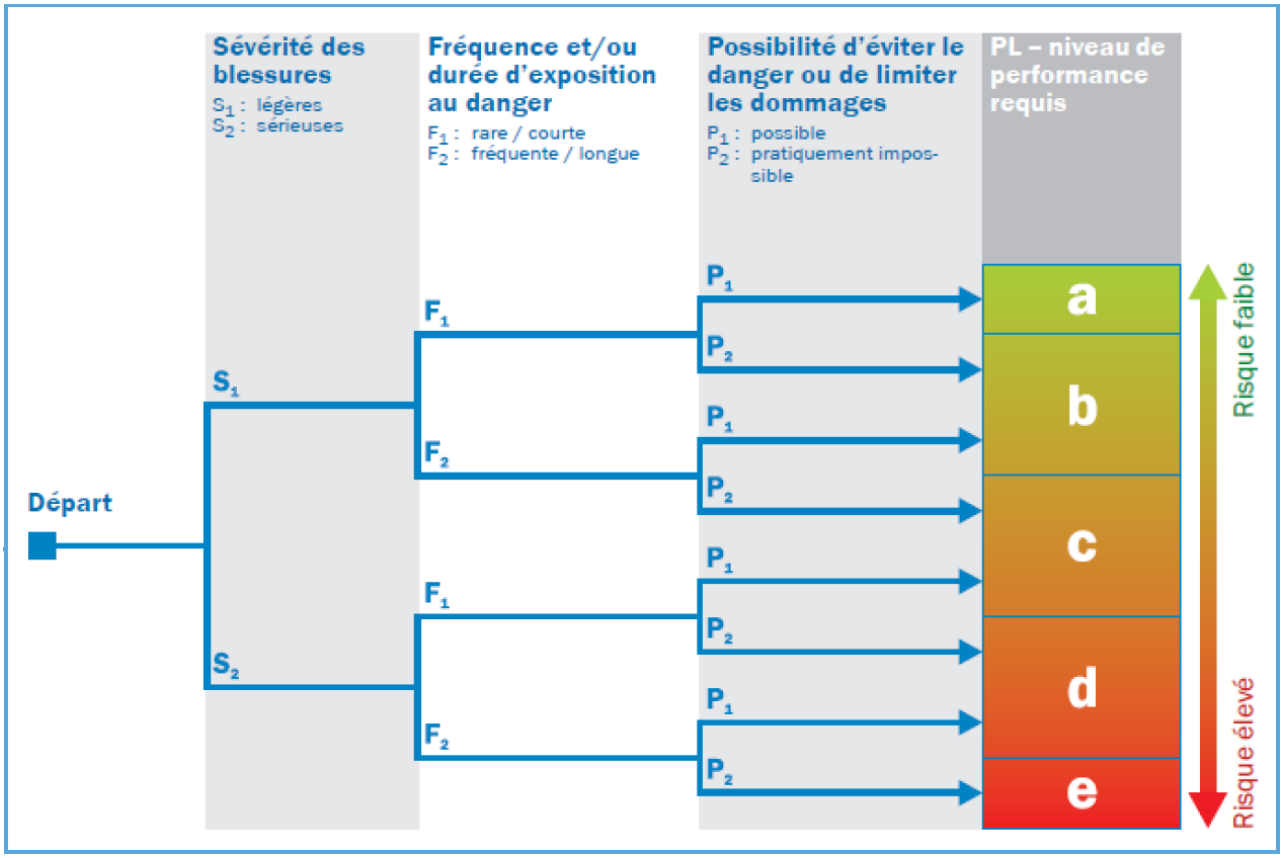
Niveau de performance requis (PLr)

Le niveau de sécurité requis (PLr) est le niveau de performance minimal exigé d'une fonction de sécurité pour atteindre la réduction du risque exigée.

Paramètres d'évaluation du risque :

Facteur	Symbole	Description	Valeurs possibles
Gravité du dommage	**S**	Niveau de gravité de la blessure ou du dommage corporel possible	S1 : Blessure légère (réversible) S2 : Blessure grave (irréversible ou mortelle)
Fréquence / Durée d'exposition	**F**	Fréquence ou durée pendant laquelle une personne est exposée au danger	F1 : Rare à peu fréquente, ou courte durée d'exposition F2 : Fréquente à continue, ou longue durée d'exposition
Possibilité d'éviter le danger	**P**	Capacité d'une personne à éviter ou limiter le danger	P1 : Possible dans certaines conditions P2 : Difficilement possible ou impossible

Gravité (S)	Fréquence / Durée (F)	Possibilité d'éviter (P)	Niveau de performance requis (PLr)
S1	F1	P1	a
S1	F1	P2	b
S1	F2	P1	b
S1	F2	P2	c
S2	F1	P1	b
S2	F1	P2	c
S2	F2	P1	d
S2	F2	P2	e



Application de la norme NF EN ISO 13849-1 en 9 étapes

1. Définir la fonction de sécurité
2. Déterminer le PL_r
3. Conception
4. Identifier les SRP/CS
5. Isoler les sous-systemes
6. Déterminer les PFHD & PL ← Pour chaque sous-système
7. Déterminer le PL global
8. Atteinte du PL ≥ PLr ?
9. Validation globale