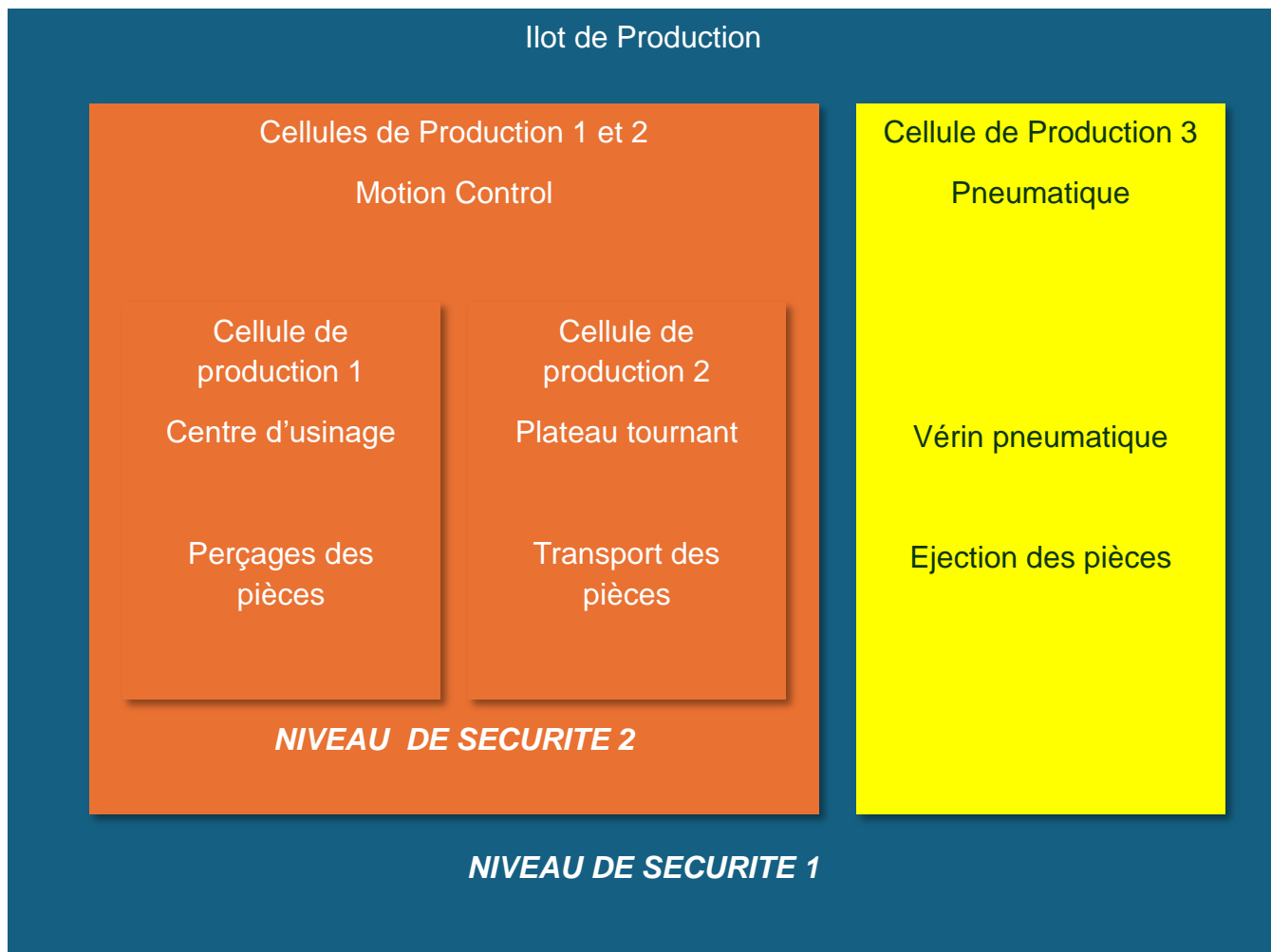


Contexte industriel



NIVEAU DE SECURITE 1 : ACCES A L'ILOT DE PRODUCTION

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-systèmes
6. Déterminer les PFHD & PL ← Pour chaque sous-système
7. Déterminer le PL global
8. Atteinte du $PL \geq PL_r$?
9. Validation globale

Etape 1 : Définition de la fonction de sécurité

• Exigences de sécurité

L'accès à l'îlot de production est autorisé quand le verrou de sécurité TR10 est dans l'état déverrouillé. Ce qui implique l'arrêt en mode **arrêt de sécurité** des cellules de production 1, 2 et 3 :

+ Activation des entrées de sécurités des préactionneurs des cellules de production 1 et 2.

+ Mise hors énergie pneumatique de la cellule de production 3.

Condition de déverrouillage du verrou de sécurité TR10 :

+ BP ATU enclenché et verrouillé.

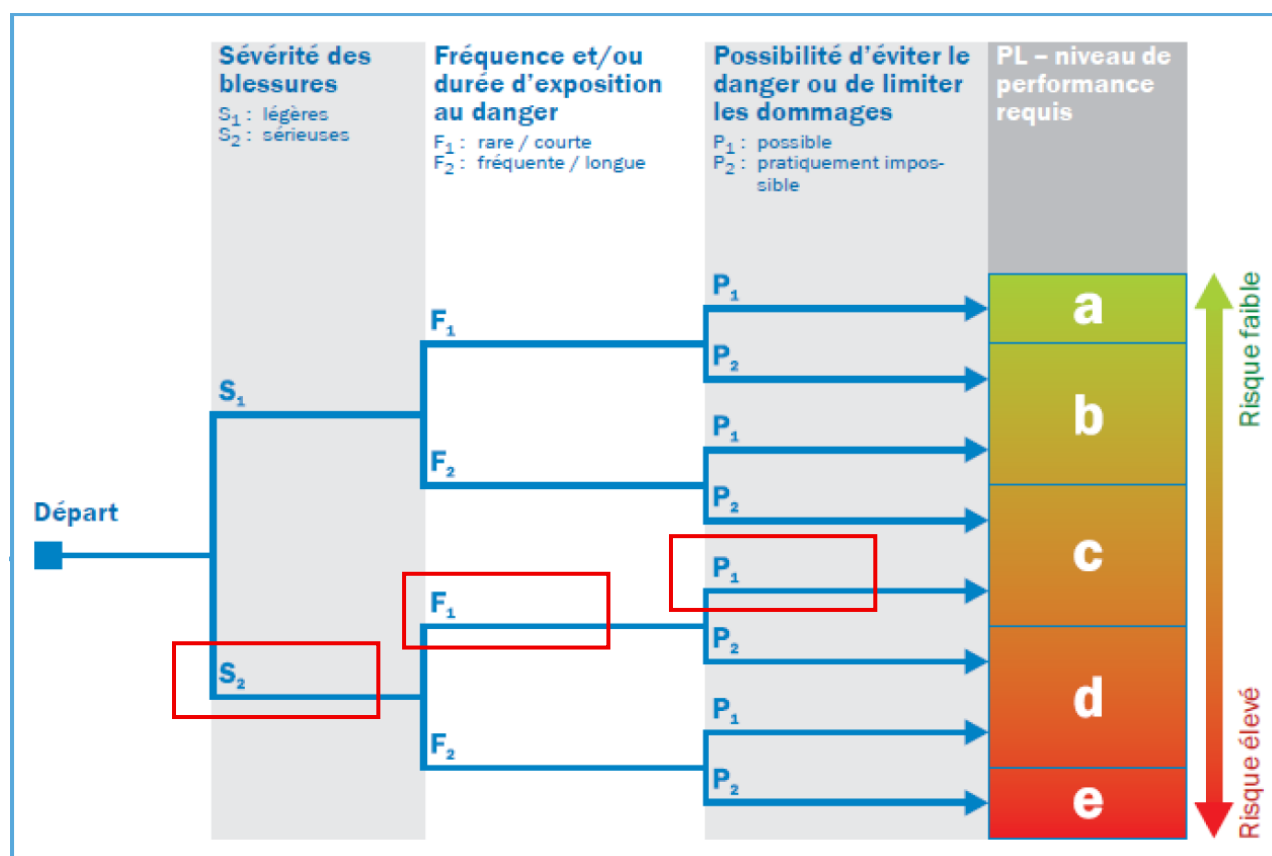
L'accès à l'îlot de production est interdit quand le verrou de sécurité TR10 est dans l'état verrouillé. Ce qui implique la mise en service normale des cellules de production 1, 2 et 3.

Condition de verrouillage du verrou de sécurité TR10 :

+ Présence du capteur RFID au-dessus du verrou de sécurité TR10

+ Impulsion sur BP REARM.

Etape 2 : Détermination du PLr



L'appréciation du risque pour le niveau 1 de sécurité qui correspond à l'accès à l'îlot de production recommande un niveau de sécurité PLr d'indice « c ».

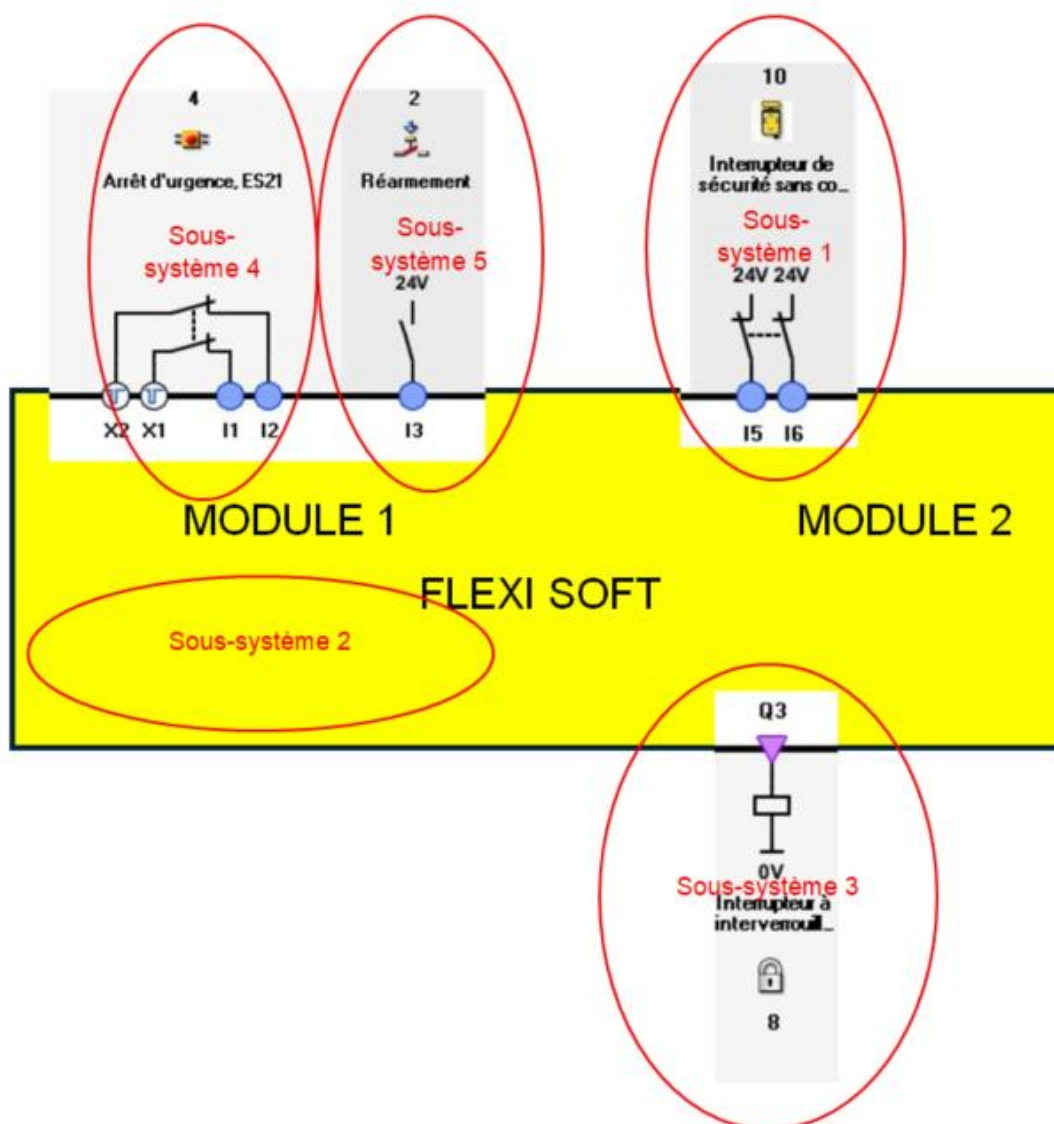
Etape 3 : Conception pour la chaîne « verrou »

La partie sécurité de l'îlot de production est confiée à un système de commande de sécurité Flexi Soft de la société SICK. Elle met en œuvre :

- Un module Flexi Soft CPU0. Pour la programmation des scénarios de sécurité
- Un module Flexi Soft GETC ETHERCAT. Pour la remontée des informations vers le PLC
- Deux modules Flexi Soft XTIO. Pour les interfaces d'entrées/sorties
- **Un verrou à interverrouillage et capteur RFID de sécurité TR10-SRM01C**
- Un bouton d'arrêt d'urgence à verrouillage (d'usage courant) : BP ATU
- Un bouton poussoir de réarmement (d'usage courant) : BP REARM.

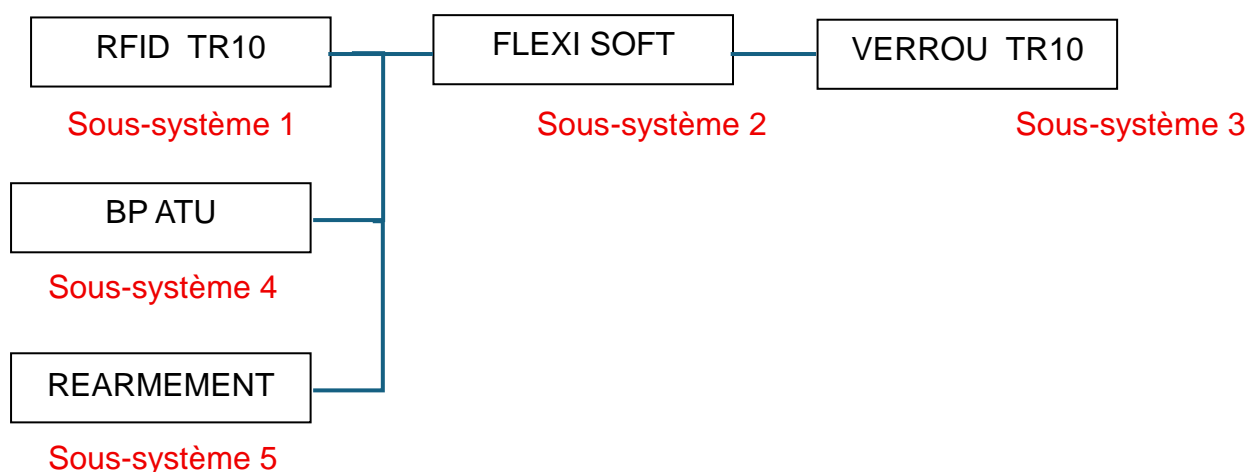
Etape 4 : Identification des SRP/CS

SRP/CS : Partie d'un système de commande relatif à la sécurité selon NF EN ISO 13849-1.



Etape 5 : Isoler des SRP/CS

Représentation schématique



Etape 6 : Détermination des PFHd et PL pour chaque sous-système

- Sous-système 1 et sous-système 3. Composant de sécurité.
Verrou à interverrouillage et capteur RFID de sécurité TR10-SRM01C.


Caractéristiques techniques relatives à la sécurité du verrou TR10 :

Niveau d'intégrité de la sécurité	SIL 3 (CEI 61508)
Catégorie	Catégorie 4 (EN ISO 13849)
Niveau de performance	PL e (EN ISO 13849)
PFH _D (probabilité moyenne d'une défaillance dangereuse par heure)	$9,1 \times 10^{-10}$
T _M (durée d'utilisation)	20 années (EN ISO 13849)
Type	Type 4 (EN ISO 14119)
Degré de codage de l'actionneur	Degré de codage bas (EN ISO 14119)
Etat sécurisé en cas de défaut	Au moins une sortie de sécurité à semi-conducteur (OSSD) se trouve à l'état INACTIF.

Caractéristiques techniques générales du verrou TR10 :

Principe du capteur	RFID
Principe de verrouillage	Mode hors tension
Nombre de sorties sécurisées	2

- Sous-système 2. Composant de sécurité
Flexi Soft CPU et Flexi Soft XTIO.

 SOLUTIONS D'AUTOMATISME INDUSTRIEL	SECURITE MACHINE	JUSTIFICATION SC/FS DU VERROU DE SECURITE TR10
---	-------------------------	--

Caractéristiques techniques relatives à la sécurité Flexi Soft CPU

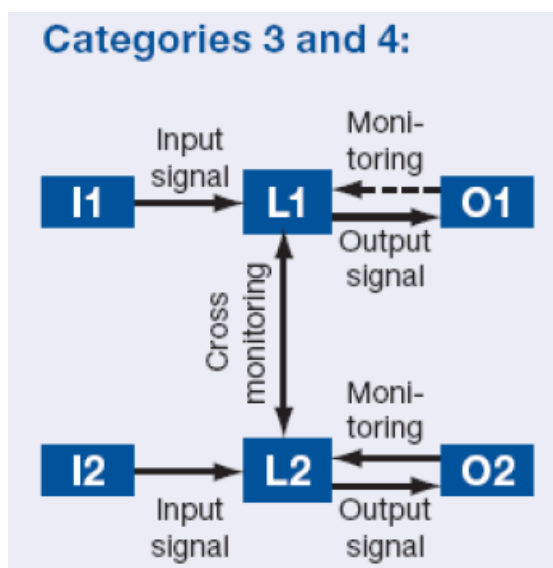
	CPU0	CPU1/2/3
Niveau d'intégrité de la sécurité (CEI 61508) Niveau d'intégrité de la sécurité (CEI 62061)	Niveau d'intégrité de la sécurité 3	
Catégorie (ISO 13849)	Catégorie 4	
Niveau de performance (ISO 13849)	PL e	
PFD _D	1,07 × 10 ⁻⁹	1,69 × 10 ⁻⁹
PFD _D pour station Flexi Line ¹⁾	-	0,40 × 10 ⁻⁹
PFD _D pour Flexi Link / EFI	-	1,69 × 10 ⁻⁹
PFD _{avg}	5 × 10 ⁻⁵	
PFD _{avg} pour station Flexi Line ¹⁾	-	5 × 10 ⁻⁵
T _M (durée d'utilisation) (ISO 13849)	20 ans	

Caractéristiques techniques relatives à la sécurité Flexi Soft XTIO

	XTIO
Niveau d'intégrité de la sécurité (CEI 61508) Niveau d'intégrité de la sécurité (CEI 62061)	Niveau d'intégrité de la sécurité 3
Catégorie (ISO 13849) ¹⁾	
Pour les sorties mono canal avec impulsions de test activées sur toutes les sorties de sécurité (Q1 ... Q4)	Catégorie 4 ²⁾
Pour les sorties mono canal avec impulsions de test désactivées sur cette sortie ou sur n'importe quelle autre sortie de sécurité (Q1 ... Q4)	Catégorie 3 ^{2) 3)}
Pour les sorties double canal avec ou sans impulsions de test désactivées sur cette sortie de sécurité ou sur n'importe quelle autre (Q1 ... Q4)	Catégorie 4 ^{3) 4)}
Niveau de performance (ISO 13849)	PL e
PFD _D ¹⁾	
Pour sorties mono canal	4,8 × 10 ⁻⁹
Pour sorties double canal	0,9 × 10 ⁻⁹
PFD _{avg} ¹⁾	
Pour sorties mono canal	4,2 × 10 ⁻⁴
Pour sorties double canal	5 × 10 ⁻⁵
T _M (durée d'utilisation) (ISO 13849)	20 ans ³⁾

- Sous-système 4. Composant standard à deux contacts.

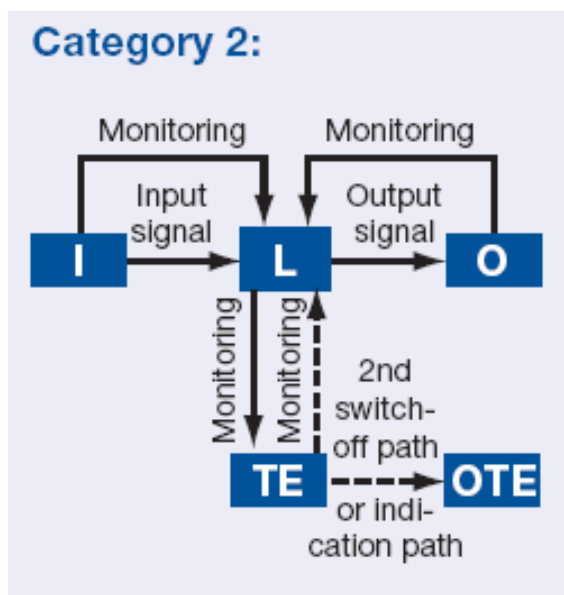
Structure double canal



Catégorie retenue : 3

- Sous-système 5. Composant standard à un contact.

Structure mono canal + Test



Catégorie retenue : 2

 SOLUTIONS D'AUTOMATISME INDUSTRIEL	SECURITE MACHINE	JUSTIFICATION SC/FS DU VERROU DE SECURITE TR10
---	------------------	--

- Catégorie. Synthèse.

Sous- système	Catégorie
1	4
2	3
3	4
4	3
5	2

Détermination du MTTFd : Durée moyenne de fonctionnement avant défaillance (dangereuse) du sous-système 5. (Sert à la détermination du PFHd et du PL)

La norme NF EN ISO 13849-1 (annexe C) donne une méthode simplifiée pour les composants électromécaniques, basée sur :

$$MTTFd = \frac{B_{10d}}{0,1 \times n_{op} \times h_{op} \times d}$$

Symbole	Signification	Unité	Commentaire
MTTFd	Durée moyenne de fonctionnement avant défaillance (dangereuse)	Année	A calculer
B_{10d}	Nombre de cycles avant 10 % de défaillances dangereuses	cycles	Donné ou estimé par le constructeur
n_{op}	Nombre d'opérations par heure	cycles/h	Fréquence d'utilisation
h_{op}	Heures de fonctionnement par jour	h/j	Typiquement 8 à 24
d	Jours de fonctionnement par an	j/an	Typiquement 220 (industriel) à 365 (continu)

Pour

- $B_{10d} = 2\,000\,000$ cycles ($2E^6$)
(valeur standard issue de l'annexe C de l'ISO 13849-1)
- $n_{op} = 1$ opérations / h (appui toutes les heures environ)
- $h_{op} = 8$ h / jour
- $d = 220$ jours / an

MTTF_{d5} = 11363 années

Détermination du PFHd et du PL du sous-système 5

Tableau K.1 (suite)

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

PFH_{d5} = 5.28E⁻⁷ . PL₅ indice d

Remarque importante :

Le sous-système 5 n'intervient pas directement dans la chaîne de sécurité car il donne l'ordre de redémarrer quand toutes les conditions de sécurité sont remplies. Une défaillance du BP REARM n'a donc pas de conséquence.

Détermination du MTTF_d : Durée moyenne de fonctionnement avant défaillance (dangereuse) du sous-système 4.

On admet que la MTTF_d du sous-système 4 est la moitié de celle du sous-système 5 :

MTTF_{d4} = 5681 années

Détermination du PFHd et du PL du sous-système 4

Tableau K.1 (suite)

MTTF _d pour chaque canal années	Probabilité moyenne d'une défaillance dangereuse par heure (1/h) et niveau de performance correspondant (PL)									
	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
100			$1,14 \times 10^{-6}$	c	$5,26 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d	$1,01 \times 10^{-7}$	d

$$PFHd_4 = 1.01E^{-7} \text{ . PL}_4 \text{ indice d}$$

- Synthèse.

Sous- système	Catégorie	PL	PFHd	T _M
1	4	e	$9.1E^{-10}$	20 années
2	3	e	$1.07E^{-9} + 4.8E^{-9} = 5.87E^{-9}$	20 années
3	4	e	$9.1E^{-10}$	20 années
4	3	d	$1.01E^{-7}$	
5	2	d	$5.28E^{-7}$	

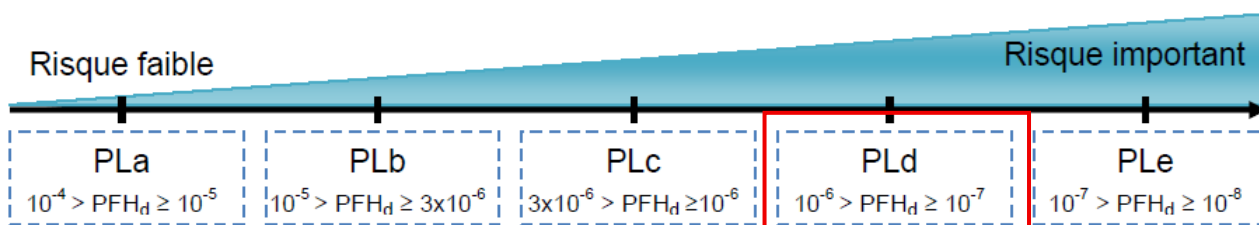
Détermination du PFHd_{Global}

$$PFHd_{GLOBAL} = PFHd_{sous-système1} + PFHd_{sous-système2} + PFHd_{sous-système3} + PFHd_{sous-système4} + PFHd_{sous-système5}$$

$$PFHd_{GLOBAL} = 9.1E^{-10} + 5.87E^{-9} + 9.1E^{-10} + 1.01E^{-7} + 5.28E^{-7} = 1.2E^{-7}$$

$$PFHd_{GLOBAL} = 1.2E^{-7}$$

Etape 7 : Détermination du PL_{GLOBAL}



$$PL_{GLOBAL} = PL \text{ « d »}$$

ETAPE 8 : Objectif atteint : $PL \geq PL_r$?

- Niveau de performance requis : PL_r indice « c »
- Niveau de performance global : PL_{GLOBAL} « d »

OBJECTIF ATTEINT

ETAPE 9 : Validation globale

Pendant l'intégration et les tests, les points suivants doivent également être documentés:

- Modifications
- Information à l'utilisation (formation des utilisateurs)
- Documentation, dossier technique...CE.