ANNEXE 4: REVENDICATION DE SIL ET PARAMETRES HFT – SFF - SC

1 - Niveaux de SFF requis en fonction du SIL revendiqué

Rappel SFF = Proportion de défaillance en sécurité SFF (Safe Failure Fraction)

$$SFF = \frac{\text{Taux de défaillance moyen des défaillances sûres et dangereuses } \textbf{détectées}}{\text{Taux de défaillances en sécurité et dangereuses } \textbf{totales} \text{ (détectées ou non)}}$$

	SIL visé		
	Pour composants ayant un mode de défaillance bien défini (A)		
SFF requis	**sans redondance**	**redondance m + 1**	**redondance m + 2**
SFF < 60 %	1	2	3
60 < SFF < 90	2	3	4
90 < SFF < 99	3	4	4
SFF > 99 %	3	4	4
	Pour éléments complexes (type B)		
SFF requis	**sans redondance**	**redondance m + 1**	**redondance m + 2**
SFF < 60 %	Non permise	1	2
60 < SFF < 90	1	2	3
90 < SFF < 99	2	3	4
SFF > 99 %	3	4	4

Tableau 5

Composant type A = Tous les modes de défaillances sont définis; la testabilité est de 100%; on dispose d'un retour d'expérience.

Composant type B = Les modes de défaillances ne sont pas tous définis; la testabilité est inférieure à 100%; le retour d'expérience est faible.

2 – Combinaison (SFF / HFT) requise en fonction du SIL revendiqué

Rappel HFT: Tolérances aux anomalies (Hardware Fault Tolerance). La HFT indique le nombre maximum d'erreurs matérielles dangereuses que le sous-système peut accepter tout en maintenant sa capacité d'exécuter la fonction de sécurité.

La HFT est obtenue par l'architecture du système: **Sécurité positive ou Redondance.**

HFT de valeur N signifie que N + 1 erreurs peuvent entraîner la perte de fonction de sécurité.

*HFT = 0 signifie que le système n'autorise aucune défaillance dangereuse (*D= avec diagnostic intégré).

	HFT - Tolérance à une défaillance	
Architecture	**Dangereuse**	**Sûre**
1001	0	0
1002	1	0
2002	0	1
1002 D	1	1
1003	2	0
2003	1	1
2003 D	1	2

Tableau 6

Tolérance minimale aux anomalies (HFT) des capteurs, terminaux et unités logiques non programmables				
SIL	**Sécurité négative**		**Sécurité positive**	
	Non validée en utilisation	Validée en utilisation	Non validée en utilisation	Validée en utilisation
1	HFT = 1	HFT = 0	HFT = 0	HFT = 0
2	HFT = 2	HFT = 1	HFT = 1	HFT = 0
3	HFT = 3	HFT = 2	HFT = 2	HFT = 1
4	Exigences spéciales (Cf. norme CEI 61508)			

Tableau 7

SIL	**Tolérance minimale aux anomalies HFT**			
	des unités logiques de l'électronique programmable (PE)			**des capteurs, éléments terminaux et unités logiques non PE**
	SFF < 60%	**60% < SFF < 90%**	**SFF > 90%**	
1	HFT = 1	HFT = 0	HFT = 0	0
2	HFT = 2	HFT = 1	HFT =0	1
3	HFT = 3	HFT = 2	HFT = 1	2
4	Exigences spéciales (Cf. norme CEI 61508 – 7.4.4)			

Tableau 8

3 – Evaluation de la Capabilité systématique SC Rappel SC: Capabilité systématique SC = Systematic Capability

Elle évalue, sur une échelle de SC1 à SC4, la confiance dans le fait qu'un élément (**Matériel + logiciel**) satisfasse aux exigences concernant l'évitement et la maîtrise des anomalies systématiques.

Une capabilité systématique de SC d'indice N signifie que le SIL d'indice N est satisfait.

Les organismes, départements et personnes réalisant cette évaluation doivent posséder un **niveau d'indépendance** spécifique. La norme CEI 61508 définit cette indépendance de la manière suivante:

" niveau correspondant à celui exigé par les phases 9 et 10 du cycle de vie de sécurité globale et de toutes les phases des cycles de vie de sécurité des SIS et des logiciels".

Personne indépendante: personne distinctement séparée des personnes responsables des activités qui se déroulent lors de la phase spécifique du cycle de vie de sécurité total des systèmes SIS ou du logiciel, chargée de l'évaluation de la sécurité fonctionnelle ou de la validation et qui n'a pas de responsabilité directe dans ces activités.

Département indépendant: département distinctement séparé des départements responsables des activités . . .

Organisme indépendant: organisme distinctement séparé, par sa direction et ses ressources, des organismes responsables des activités . . .