## NORME CEI 61508

# La sécurité fonctionnelle dans l'industrie

JEAN BUFFERNE [1]

***La conception des systèmes électroniques et électrotechniques doit répondre à des normes de sécurité fonctionnelle souvent difficiles à comprendre. S'appuyant sur le cycle de vie des systèmes, un expert en la matière nous livre les clés qui permettront d'appréhender à la fois les normes et les ouvrages sur le sujet.***

**mots-clés**
normes, sûreté de fonctionnement, système

L'International Electrotechnical Commission (IEC, CEI en français) précise les objectifs de la norme CEI 61508 « Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables [E/E/PE] relatifs à la sécurité » :

– optimiser le déploiement des systèmes intégrés de sécurité pour améliorer la sécurité (obtenir un niveau de risque acceptable) et les performances économiques des installations ;

– fixer un cadre global de sécurité incluant les développements techniques ;

– fournir une approche système rigoureuse et flexible ;

– acquérir une confiance justifiée dans les technologies des systèmes intégrés de sécurité ;

– définir une base générique applicable dans différents domaines industriels.

Cette norme présentée comme générique est déclinée en d'autres normes applicables dans différents domaines : CEI 61511, industries de transformation ; CEI 62061, machines ; CEI 61513, nucléaire ; ISO 26262, automobile ; EN 50126/128/129, ferroviaire.

Basée sur les notions de cycle de vie d'un produit et de cycle de vie de sécurité, cette norme CEI 61508 est incompréhensible sans référence à la structure des systèmes de sécurité, mais aussi au vocabulaire utilisé.

Pour la conformité à la norme, il doit être démontré que toutes les exigences du cycle de vie du système (conception, réalisation, exploitation) sont satisfaites et que les objectifs sont atteints. Mais, de par le vocabulaire utilisé, ces exigences sont absconses si l'on ne connaît pas la structure des systèmes de sécurité fonctionnelle, et on peut se demander si la norme ne confond pas respect des procédures et qualité du résultat obtenu.

Je voudrais présenter ici les bases structurelles de la sécurité fonctionnelle. J'ai été obligé de ne retenir que l'essentiel, mais j'espère que cela permettra aux personnes concernées par ce sujet d'étudier les ouvrages spécialisés (il y en a peu) et de s'orienter dans la jungle normative.

L'analyse préalable des risques (APR) relatifs à une installation prend en compte :

– la probabilité W de survenue de l'événement indésirable (taux d'occurrence) ;

– la conséquence C du risque (gravité) ;

– la fréquence d'exposition F (probabilité que la zone dangereuse soit occupée) ;

– la possibilité P d'éviter l'événement (moyens matériels et organisationnels).

$$\text{Probabilité de risque} = W \cdot C \cdot F \cdot P$$

On utilise parfois la notion de classe de probabilité, qui correspond à la somme des indices attribués à F, P et W.

### Fonction intégrée de sécurité (FIS) et système intégré de sécurité (SIS)

L'exploitant d'une installation doit comparer la probabilité de chaque risque au risque tolérable qu'il s'est lui-même fixé (c'est l'utilisateur qui doit s'engager sur le risque tolérable) 1. Cette confrontation définit la réduction de risque à obtenir par la mise en œuvre d'une fonction intégrée de sécurité (FIS) indépendante du système de commande du processus concerné.

*Exemple* : Si dans un système la probabilité qu'une défaillance fasse une victime est de $5 \times 10^{-3}$ alors que l'on s'est fixé un risque tolérable de $2 \times 10^{-6}$ par an, la réduction de risque à obtenir est de :

$$2 \times 10^{-6} / 5 \times 10^{-3} = 4 \times 10^{-4}$$

Elle s'exprime donc par un *facteur de réduction de risque* (FFR) de

$$1 / 4 \times 10^{-4} = 2\,500$$

Une fonction de sécurité définit ce qui doit être réalisé pour *éviter* des situations dangereuses (arrêter un

| Risque tolérable | = | Probabilité que la défaillance fasse une victime | × | Réduction de risque à obtenir |
|---|---|---|---|---|

**1** Le risque tolérable

[1] Ingénieur-conseil et instructeur TPM (*Total Productive Maintenance*) certifié JIPM (Japan Institute of Plant Maintenance), auteur de l'ouvrage *Fiabilité des équipements : Application à la maintenance industrielle*, éd. IFEAS, 2013.

moteur) ou pour *prévenir* le danger (interdire le démarrage d'un moteur). Pour chaque fonction il faut préciser :

– ce qui doit être surveillé ;

– ce que doit faire la fonction (action à réaliser et temps de réponse) ;

– quel doit être le comportement du système en cas de défaillance.

La fonction de sécurité est assurée par un système intégré de sécurité (SIS). *SIS* est utilisé en remplacement du terme *système E/E/PE* de la norme. Un SIS comprend tous les éléments nécessaires à l'exécution de la fonction de sécurité : alimentation, matériel, logiciel, unités logiques, unités d'entrées et de sorties, transmetteurs, actionneurs, systèmes de communication, actions humaines 2.

On considère qu'une seule défaillance du SIS peut empêcher d'assurer la fonction de sécurité et donc d'obtenir le facteur de réduction de risque fixé. Ce qui conduit à définir que la *probabilité de défaillance* du SIS doit être inférieure à la réduction de risque à obtenir.

Il y a donc corrélation entre réduction de risque à obtenir et probabilité de défaillance matérielle du SIS. Cette corrélation est exprimée par un *niveau de sécurité intégré* (SIL, *safety integrity level*).

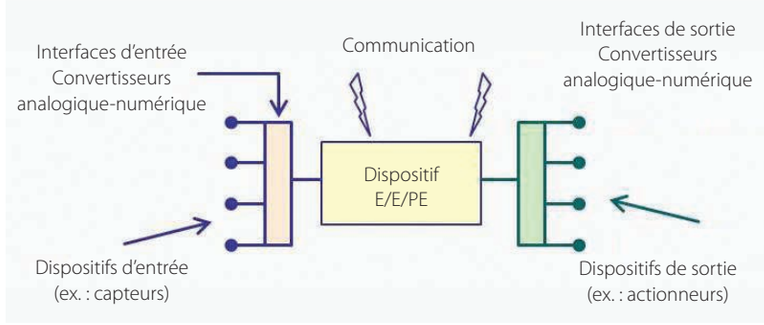
Certains fabricants proposent du matériel qualifié d'un niveau de SIL, ce qui signifie *seulement* qu'il peut être intégré dans un système visant ce niveau. La probabilité de défaillance due à ce matériel doit être calculée en tenant compte de son taux estimé d'avaries aléatoires et de l'architecture du SIS dans lequel il est intégré (redondance, temps de sollicitation, sensibilité aux causes communes, couverture de diagnostic, possibilité de test, temps de réparation, etc.). On utilisera les termes de *SIL revendiqué* ou *SIL capable*.

## Le niveau intégré de sécurité (SIL)

La norme CEI 61508 définit quatre niveaux de sécurité (SIL de 1 à 4), qui correspondent à des classes de facteurs de réduction de risque : de 10 à 100, de 101 à 1 000, etc. L'objectif de SIL est affecté à une fonction de sécurité pour définir les objectifs à satisfaire ainsi qu'une limite inférieure aux exigences quantitatives et qualitatives correspondantes.

Quatre niveaux sont suffisants compte tenu de la faible précision avec laquelle on est capable d'estimer la fiabilité des matériels. Fixer un objectif de niveau élevé signifie que l'on a besoin d'obtenir, pour une seule fonction, une réduction de risque importante. La solution technique retenue pour assurer cette réduction est donc critique par rapport à la sécurité fonctionnelle. Il faudra la maintenir, dans le temps, au même niveau malgré les risques techniques et organisationnels propres à chaque structure industrielle.

La norme machines CEI 62061 ne prend pas en compte le niveau 4, considéré comme trop important et ne pouvant donc être obtenu que par une révision de la conception de l'installation. L'idéal est de disposer d'équipements présentant par eux-mêmes un niveau de risque acceptable, donc ne nécessitant pas l'attribution de fonctions de sécurité.




**2** **Les éléments constitutifs d'un SIS**

## Probabilité moyenne de défaillance et fréquence moyenne de défaillance

Réduction de risque à obtenir, facteur de réduction de risque, niveau de sécurité intégré (SIL) et probabilité de défaillance des SIS quantifient le même objectif. En particulier, SIL et probabilité de défaillance du SIS sont liés. Par contre, on distinguera deux types de fonctionnement :

- Les systèmes faiblement sollicités : exécution de la fonction sur demande ou fréquence de sollicitation inférieure à une par an
- Les systèmes fonctionnant en continu ou fortement sollicités : fréquence de sollicitation supérieure à une par an

Le tableau 3 traduit ces valeurs.

La norme machines IEC 62061 considère que tous les SIS sont en mode de fonctionnement continu.

| Niveau objectif SIL | Facteur de réduction de risque | Système faiblement sollicité | Système fortement sollicité ou en fonctionnement continu |
|---|---|---|---|
| | | $PFD_{avg}$ Probabilité moyenne de défaillance | PFH Fréquence moyenne de défaillance par heure |
| 4 | De 10 001 à 100 000 | $10^{-5} \leq PFD_{avg} \leq 10^{-4}$ | $10^{-9} \leq PFH \leq 10^{-8}$ par heure |
| 3 | De 1 001 à 10 000 | $10^{-4} \leq PFD_{avg} \leq 10^{-3}$ | $10^{-8} \leq PFH \leq 10^{-7}$ par heure |
| 2 | De 101 à 1 000 | $10^{-3} \leq PFD_{avg} \leq 10^{-2}$ | $10^{-7} \leq PFH \leq 10^{-6}$ par heure |
| 1 | De 10 à 100 | $10^{-2} \leq PFD_{avg} \leq 10^{-1}$ | $10^{-6} \leq PFH \leq 10^{-5}$ par heure |

**3** **Les intégrités de sécurité**

### La probabilité de défaillance dangereuse (PFD et $PFD_{avg}$)

*Définitions :*

● **PFD** : *probabilty of failure on demand*, probabilité de défaillance dangereuse en cas de *faible sollicitation*.

$$PFD = \lambda \times 1 \text{ sollicitation}$$

C'est la probabilité que le SIS ne puisse pas réaliser la fonction de sécurité spécifiée, lors de la sollicitation de l'installation ou de son système de commande. C'est le mode le plus répandu en industrie de process.

● **$PFD_{avg}$** : *average probabilty of failure on demand*, moyenne des taux d'avarie durant une période donnée ou proportion de défaillances durant l'intervalle de temps T.

$PFD_{avg}$ est une fonction de $\lambda(t)$ et de T.

$\lambda(t)$ : taux d'avarie par unité de temps à l'instant *t*

T : durée durant laquelle le système peut être dans un état de fonctionnement critique du fait de la non-détection de la défaillance de certains éléments (périodicité des tests) ou du temps de réparation des éléments défectueux

L'annexe 3, accessible sur le site www.jean-bufferne.com, rubrique Publications, comme les autres annexes appelées ici, définit le mode de détermination de ces temps.

$PFD_{avg}$ est comparée à la probabilité fixée par le SIL.

Les valeurs des taux d'avarie des différents éléments sont obtenues soit à partir de bases de données, soit par des essais sur des échantillons limités, soit par exploitation du retour d'expérience de l'utilisateur (la norme tient compte d'un critère « reconnu par l'usage »). Ces données doivent être exprimées sous forme statistique, c'est-à-dire en précisant leur intervalle de confiance bilatéral, au moins 90 % pour les constructeurs. Attention à la divergence des résultats en fonction :

– des conditions des essais (conditions d'utilisation) ;

– du type de défaillances pris en compte ;

– des conditions d'entretien et de maintenance ;

– des références de temps utilisées (taux par heure de fonctionnement, taux de défaillance par année type d'utilisation, taux d'avarie par $10^9$ heures ou FIT).

### La probabilité moyenne de défaillance par heure (PFH)

En fait, le PFH (*probabilty of dangerous failure per hour)* n'est pas une probabilité, mais une fréquence (nombre d'avaries par heure), mais on peut confondre ces deux valeurs (voir l'annexe 1).

### L'hypothèse du taux d'avarie constant

La norme suppose que tous les constituants d'un système ont un taux d'avarie constant (loi exponentielle de la période dite de vie utile, paramètre de forme $\beta = 1$ dans la loi de Weibull). Mais attention : même si le taux d'avarie est constant, la probabilité de défaillance est une fonction de *t*. En effet, cette probabilité est par définition égale à $F(t) = e^{-\lambda t}$. Cette hypothèse de taux d'avarie constant suppose :

– que la période infantile n'existe pas (ou plus) ;

– qu'il n'existe pas de période de vieillissement (est-ce le cas pour des vannes, des soupapes, des composants présentant un phénomène de dérive ?) ;

– que l'on est capable d'empêcher l'apparition du vieillissement (pour cela, il faut le connaître) par remplacement systématique à T tel que :

$$R_{usure}(T) \leq R_{vie\ utile}(t)$$

*t* : durée de mission ou mission unique

T : durée d'utilisation très courte durant la période d'usure (dans ce cas, la probabilité de défaillance due à l'usure $F_{usure}$ est très faible, mais différente de 0, surtout si de nombreux composants sont en série)

– que l'on pourra contrôler le bon fonctionnement des éléments montés en parallèle et si besoin les réparer. Cela, pour tenir compte, comme le présente l'annexe 2, du fait que le taux d'avarie équivalent d'un montage parallèle (redondance) d'éléments ayant un taux d'avarie constant n'est plus constant mais fonction du temps (l'hypothèse $\beta = 1$ est invalidée), et que le ou les éléments redondants « en secours » peuvent être défaillants.

Dans tous les cas, on doit disposer de résultats d'essais d'endurance pour quantifier les phénomènes éventuels de vieillissement et pouvoir les éviter.

*Pour utiliser la loi exponentielle, il faut que le PFH calculé soit inférieur à $10^{-5}$ ou que le PFD calculé soit inférieur à $10^{-1}$ (limites basses de revendication du SIL).*

### Les différentes causes de défaillance

Suivant la théorie de la variabilité des processus développée par Deming, Juran et Shewart, un matériel peut subir deux types de défaillances, selon leurs causes **4** :

| | | |
|---|---|---|
| Causes aléatoires | Dégradations naturelles<br>Erreurs humaines aléatoires (étourderies) | Mesurées par le PFD ou le PFH |
| Causes spéciales | Spécifications incorrectes<br>Prescriptions de sécurité incorrectes<br>Erreur humaine de conception (matériel ou logiciel), de fabrication, d'exploitation, de maintenance<br>Erreur humaine (fausses manœuvres, non-respect des conditions d'exploitation ou des standards)<br>Influence de l'environnement<br>Perturbation de l'alimentation : électricité, air comprimé, etc. | Il n'existe pas de loi de distribution, mais la norme suppose que l'objectif de défaillance associé est atteint si toutes les exigences de la norme sont remplies |

**4** **Les causes de défaillance**

● **Les défaillances aléatoires**, caractérisées par une loi de distribution (de la fiabilité, des contraintes, de certaines erreurs humaines), sont exprimées par le PFD ou le PFH.

● **Les défaillances systématiques**, dues à des *causes spéciales* ou systématiques telles que spécifications, prescriptions d'exploitation et de sécurité incorrectes, erreurs humaines entraînant le non-respect des conditions d'exploitation, influence de l'environnement, perturbation des alimentations (électricité, air comprimé, etc.), sont les causes majeures d'accidents.

On se rappellera qu'il est impossible de faire des prévisions sur la fiabilité d'un équipement tant que le système dans lequel il est intégré n'est pas sous contrôle statistique, c'est-à-dire tant qu'il subit des perturbations issues de causes spéciales.

On trouve dans les défaillances systématiques les défaillances dites de *cause commune* : défaillances dépendantes les unes des autres et qui surviennent simultanément. Elles peuvent être dues à des erreurs de conception matérielles ou logicielles, de fabrication, d'exploitation, de maintenance.

L'impact des défaillances aléatoires et systématiques sera minimisé par la qualité du développement (préconisations de la norme CEI 61508) et par la définition de la structure des systèmes.

## Les deux types de défaillances

● **Une défaillance dangereuse** peut mettre l'installation dans un état dangereux ou diminuer la probabilité de bon fonctionnement du système relatif à la sécurité **5**.

● **Une défaillance en sécurité** (ou défaillance sûre) a une influence parasite sur la fonction de sécurité en créant ou augmentant la probabilité de *déclenchement ou maintien* d'un état de sécurité **5**.

On suppose que ces défaillances sont réparables, mais on prend en compte la possibilité de détection : elles peuvent être soit immédiatement perceptibles (ou détectées) soit non perceptibles en dehors d'un test. En pratique, les tests demandent des interventions complexes. Du fait de leur importance, ils ne sont réalisés qu'à des intervalles longs (environ 4 000 h).

## La revendication de SIL par un SIS (SIL capable)

Le niveau de SIL qui peut être revendiqué par un SIS est fixé par deux paramètres : *sa probabilité de défaillance exprimée* en PFD ou PFH, et *le niveau de SIL le plus élevé* dont il est capable.

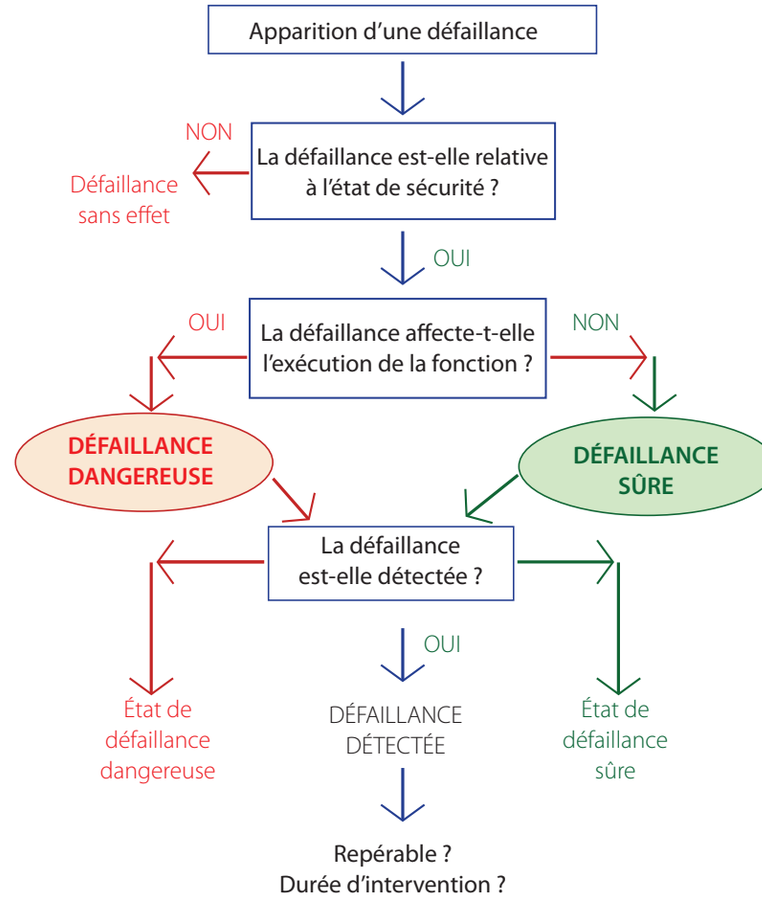
Le schéma **6** présente les éléments qui, à partir de l'architecture du SIS, permettent de calculer le PFD ou le PFH, et d'évaluer le SIL capable.

## Le calcul du PFH ou PFD du SIS

Le taux de défaillance (PFH ou PFD) du SIS est une fonction du taux de défaillance $\lambda$ du SIS et de son temps d'utilisation. Il dépend donc :

– de la probabilité de défaillance aléatoire des éléments constitutifs du SIS (voir le paragraphe suivant) ❶ ;

– de leurs taux de défaillance de cause commune exprimés par le *facteur* $\beta$ ❷ qui s'additionne au taux de défaillance aléatoire (taux de défaillance de cause commune = $\beta$ × taux d'avarie de défaillances aléatoires de l'élément) ;




**5** **Défaillance dangereuse et défaillance sûre**

– de leur temps de fonctionnement, fonction de la capacité de détection et de réparation des défaillances dangereuses (voir plus loin) ❸.

(Les puces numérotées renvoient au schéma 6.)

### La probabilité de défaillance du SIS

Le PFH, ou PFD, du SIS est calculé à partir des probabilités de défaillance intrinsèques de ses constituants, en tenant compte de la structure, notamment de leur redondance. Par exemple, pour une redondance du type MooN (*M out of N*, qui spécifie que sur N circuits montés en parallèle il faut que M circuits fonctionnent), la défaillance de la structure survient lorsqu'il y a défaillance de M éléments et que les (N – M) circuits restants sont eux-mêmes en panne et ne peuvent pas prendre le relais (défaillance non encore détectée par un test, ou réparation en cours).

On distinguera les taux de défaillances détectées $\lambda_D$ et non détectées $\lambda_{DU}$ en tenant compte de la possibilité de détection des défaillances exprimée par *le taux de couverture DC* ❼ (DC est la proportion du nombre de défaillances détectées par des essais automatiques de diagnostic ou lors de l'exploitation normale par rapport au nombre total de défaillances dangereuses) :

$$\lambda_D = DC \cdot \lambda T$$
$$\lambda_{DU} = (1 \cdot DC) \cdot \lambda T$$

### Le temps de fonctionnement

Le temps de fonctionnement des différents éléments correspond au temps critique de fonctionnement de la structure ❸, c'est-à-dire au temps d'utilisation entre deux tests de bon fonctionnement ou au temps d'indisponibilité pour réparation de certains composants de la structure. On tiendra compte :

– de la périodicité des tests (automatiques intégrés ou manuels) ;

– du temps de réparation des éléments défectueux MTTR (*mean team to repair)*, exprimé en percentiles (on considère qu'il est toujours possible de réparer). On est amené à faire une hypothèse concernant l'instant d'apparition d'une deuxième défaillance par rapport au traitement de la première ;

– de la probabilité et de l'indisponibilité d'autres parties du système. Cette indisponibilité est représentée par le MDT *(mean down time)* exprimé en percentiles, et tient compte du fait que les défaillances peuvent être détectées et que les éléments sont ou ne sont pas réparables.

On distinguera pour les différentes architectures MooN deux types de situations :

- **Les défaillances perceptibles** (la norme utilise le terme *détectable*) et réparables : c'est la durée d'immobilisation pour réparation qui sera prise en compte.
- **Les défaillances non perceptibles** sans la réalisation d'un test et réparables : la périodicité des tests (très supérieure au temps de réparation) sera prise en compte.

### Les défaillances perceptibles et réparables

La probabilité de défaillance du système est égale au produit du taux de défaillance du système par le temps d'indisponibilité de l'élément en cause. Ce dernier sera représenté par le MDT et non le MTTR, car au temps propre de réparation peuvent s'ajouter les temps nécessaires à la préparation de l'intervention et à la remise en exploitation du système.

Ne pouvant déterminer à quel moment surviendra la deuxième défaillance par rapport au traitement de la première, on suppose, dans une approche statistique, qu'elle survient à mi-réparation.

L'annexe 3/1 présente le mode de détermination de ces paramètres suivant l'architecture utilisée.

On considère (D. Smith, *Fiabilité, maintenabilité et risque,* Dunod / L'Usine nouvelle, p. 104 et 409) que le modèle markovien ne permet pas de calculer correctement la probabilité de *défaillance sur sollicitation* (PFD) des systèmes redondants réparables. En effet, le modèle markovien considère que le temps de réparation relève d'un processus aléatoire, et que la transition de l'état de défaillances multiples à l'état de bon fonctionnement ne dépend que de la dernière réparation.

En pratique, le temps de réparation dépend des événements survenus avant la défaillance considérée, et s'il n'y a qu'une seule équipe de réparation, elle terminera la première réparation avant de s'occuper de la suivante.

### Les défaillances non perceptibles et réparables

On suppose qu'une deuxième défaillance peut survenir avant la détection par un test de la première défaillance.

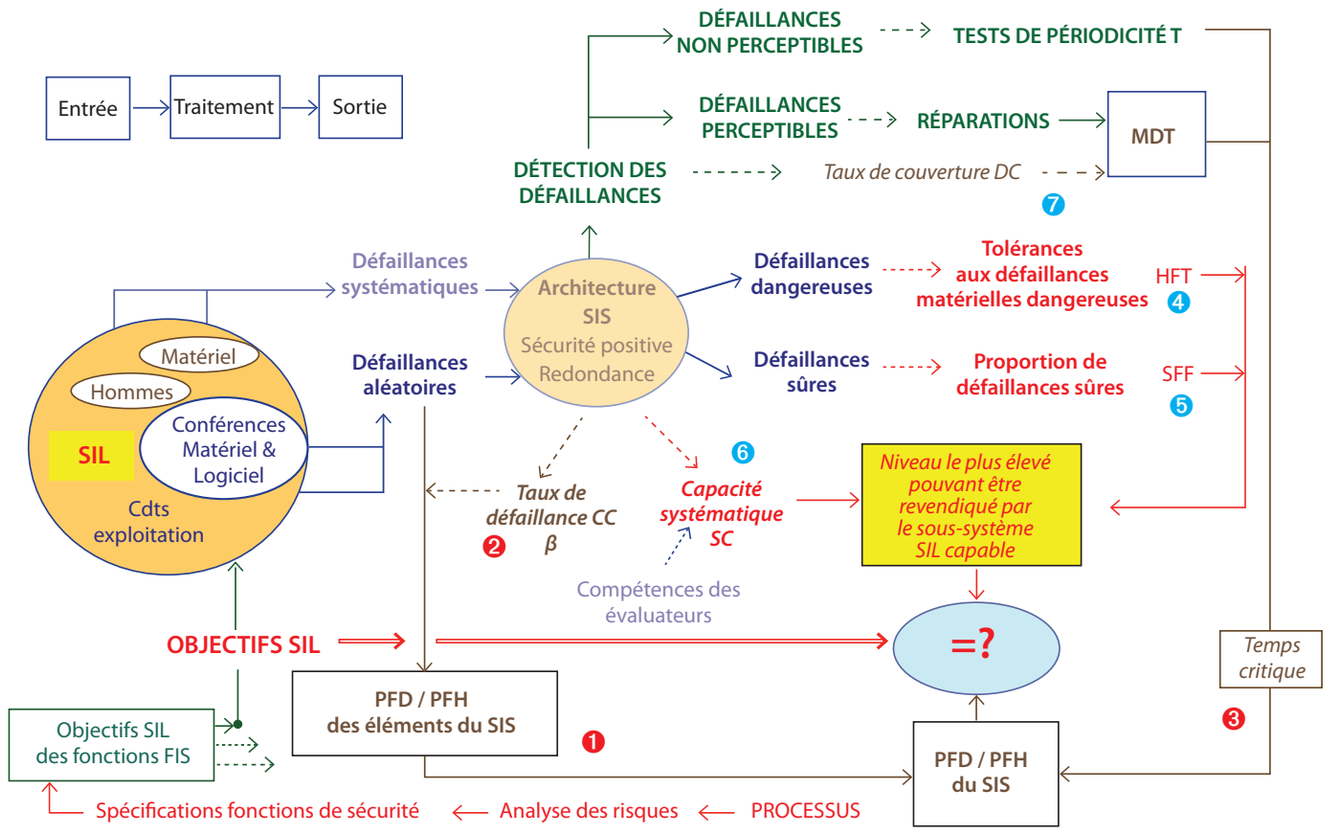
La Sintef (fondation norvégienne pour la recherche scientifique et industrielle), qui fait référence dans le domaine de la sécurité fonctionnelle, a fixé le mode d'évaluation du PFD et du PFH dans l'édition 2010 de son *PDS Method Handbook* (S. Hauge, M. A. Lundteigen, P. Hokstad S. Håbrekke, *Reliability Prediction Method for Safety Instrumented Systems : PDS Method Handbook, 2010 Edition*, éd. Sintef) – PDS étant l'acronyme norvégien pour la fiabilité des systèmes de sécurité informatisés.

Les valeurs sont fournies par l'annexe 3/2.

### L'évaluation du niveau le plus élevé de SIL dont le SIS est capable

La valeur maximale de SIL que peut revendiquer un SIS est déterminée en tenant compte de 6 :

– son architecture, lui conférant une tolérance aux défaillances matérielles dangereuses (HFT, *hardware fault tolerance*) ❹. Le HFT indique le nombre maximal d'erreurs matérielles dangereuses que le système peut accepter tout en pouvant continuer à exécuter la fonction de sécurité. Pour une défaillance dangereuse, une architecture 1002 aura un HFT de 1, alors que des architectures 1001 ou 2002 auront un HFT de 0 ;




**6** **Le principe d'évaluation du SIL capable**

– la répartition entre défaillances sûres et défaillances dangereuses, mesurée par la SFF (*save failure fraction*) 5. Cette répartition est obtenue à partir d'une AMDE utilisant les valeurs issues de bases de données, des constructeurs ou du retour d'expérience. Pour des éléments complexes, il n'est pas possible de disposer d'études détaillées, et on accepte une répartition 50-50 ;

– l'évaluation par audit de la capacité d'un élément (matériel ou logiciel) à éviter ou maîtriser les anomalies systématiques, cette évaluation étant exprimée par la capabilité systématique SC 6.

La norme définit une correspondance entre les paramètres HFT, SFF, SC et le niveau maximal de SIL qui peut être revendiqué (voir l'annexe 4).

Ces différents facteurs dépendent, comme le montre le schéma 6, de l'architecture du SIS.

L'exploitant de l'installation s'étant fixé un niveau de risque acceptable, il en déduit par rapport aux résultats d'une analyse de risque le facteur de réduction que doit lui apporter le système de sécurité fonctionnelle. Ce facteur de réduction de risque est converti suivant la norme en un niveau de SIL des différentes fonctions de sécurité FIS, puis décliné à chaque système intégré de sécurité SIS.

Suivant la méthodologie décrite ci-dessus, issue de la norme CEI 61508, le concepteur peut, à partir des caractéristiques intrinsèques des éléments, de leurs conditions d'utilisation et de leur structure d'association, répondre aux deux conditions lui permettant de savoir s'il a atteint les objectifs fixés : le système envisagé est capable de répondre à l'objectif de SIL ; le PFH, ou PFD, du système est inférieur ou égal aux valeurs exigées par le SIL. ■