INCERTITUDES DANS LES CALCULS DE FIABILITÉ SELON LES NORMES IEC 61508 ET IEC 61511

UNCERTAINTIES IN RELIABILITY CALCULATIONS ACCORDING TO IEC 61508 & 61511 STANDARDS

Marie BOITEAU et Frédéric DOUX
FRACTAL SYSTÈME
64 rue Raymond IV, 31000 Toulouse
Tél. : +33 (0)5 61 44 93 61
E-mail : marie.boiteau@fractal-systeme.com
E-mail : frederic.doux@fractal-systeme.com

Nicolas CLAVÉ
Total S.A.
CSTJF - Avenue Larribau
64018 Pau Cedex France
Tél. : +33 (0)5 33 43 32 72
E-mail : nicolas.clave@total.com

Jean-Pierre SIGNORET
Total Professeurs Associés
2, route de GARLIN
64160 SEDZERE
E-mail : j-p.signoret@orange.fr

Résumé

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 requièrent de prendre en compte les incertitudes relatives aux données de fiabilité pour les mesures probabilistes concernant les systèmes instrumentés de sécurité et proposent deux méthodes pour ce faire: utilisation des bornes supérieures à 70% ou des distributions complètes des paramètres de calcul. Dans la présente communication, les deux méthodes sont appliquées à trois cas d'étude : un système série, un système parallèle et un cas industriel. Pour cela, la suite logicielle GRIF (© Total S.A.) a été utilisée afin d'évaluer la probabilité moyenne de défaillance dangereuse en cas de sollicitation (PFD_{avg}). Les calculs montrent qu'une des méthodes est plus pessimiste que l'autre lorsque l'incertitude sur les données de fiabilité est grande.

Summary

Functional safety standards IEC 61508 and IEC 61511 require to take into account data uncertainties for probabilistic measures related to safety instrumented system and propose two approaches for doing that: use of the 70% upper bound or the full distribution of calculation parameters. In this paper, the two methods are applied to three application cases: a system in series, a system in parallel and a typical business case. The software GRIF (© Total S.A.) has been used in order to evaluate the mean probability of failure on demand (PFD_{avg}). The results indicate that a method is more pessimistic when the reliability data uncertainty is great.

1. Introduction

L'évaluation probabiliste de la sécurité fonctionnelle est à l'heure actuelle de plus en plus utilisée dans la gestion des risques liés aux systèmes instrumentés de sécurité des installations industrielles. Selon la dernière version des normes IEC 61508 *(Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité*, Ed. 2.0) [3] et IEC 61511 *(Sécurité fonctionnelle – systèmes instrumentes de sécurité pour le secteur des industries de transformation*, Ed. 2.0) [1], la prise en compte des incertitudes relatives aux données est requise pour les calculs de probabilité de défaillance des systèmes instrumentés de sécurité.

Dans les faits, cette exigence est rarement satisfaite. Aussi, l'objectif de cet article est de présenter les deux méthodes de prise en compte des incertitudes proposées dans ces normes, d'étudier leur faisabilité et de les mettre en œuvre sur trois cas d'école afin de comparer leur impact sur les résultats finaux et leur facilité de mise en œuvre.

2. Contexte

Dans les industries de procédé (pétrole et gaz, pétrochimie…), la sécurité fonctionnelle des systèmes instrumentés de sécurité est régie par les normes internationales IEC 61508 et IEC 61511. Les calculs de fiabilité mentionnés dans ces normes imposent :

- soit de calculer l'indisponibilité moyenne (*PFD_{avg}*) pour les systèmes instrumentés de sécurité fonctionnant à faible demande,
- soit de calculer la fréquence moyenne de défaillance (*PFH*) pour les systèmes instrumentés de sécurité fonctionnant à forte demande ou en continu.

La norme IEC 61508 exige que les incertitudes sur les données de fiabilité soient prises en compte (voir, par exemple les clauses 7.4.4.3.3 et 7.4.9.5 de l'IEC 61508-2) dans le calcul des mesures probabilistes (*PFD_{avg}* ou *PFH*). D'autre part, lorsque la *Safe Failure Fraction* (*SFF* - proportion du taux de défaillance global produisant des défaillances sûres) n'est pas prise en compte (route dite 2_H), la norme exige d'améliorer le système instrumenté de sécurité jusqu'à ce qu'une confiance supérieure à 90% soit obtenue pour la réalisation de l'objectif visé pour la mesure considérée (*PFD_{avg}* ou *PFH*).

De même, la nouvelle version de la norme IEC 61511 (publication prévue en 2016) précise également que *« les incertitudes concernant les données de fiabilité doivent être évaluées et prises en compte lors du calcul des niveaux de défaillance »* (voir la clause 11.9.4 de l'IEC 61511-1).

Deux méthodes sont alors proposées pour évaluer ces incertitudes :
1. *« l'utilisation de la limite supérieure de confiance à 70 % pour chaque paramètre de fiabilité d'entrée au lieu de sa moyenne afin d'obtenir des estimations ponctuelles conservatives des niveaux de défaillance »* ;
2. *« l'utilisation des fonctions de distributions probabilistes des paramètres de fiabilité d'entrée, la réalisation de simulations de Monte-Carlo pour produire un histogramme représentant la distribution de la probabilité/fréquence de défaillance et l'évaluation d'une valeur conservative de cette distribution (ex.: évaluation d'un niveau tel que la véritable valeur a 90 % de chances d'être meilleure) »*.

3. Méthode

La satisfaction des exigences normatives ci-dessus implique donc la prise en compte des incertitudes relatives aux données de fiabilité dans les calculs et deux méthodes préconisées sont analysées ci-après.

3.1 Méthode 1

L'objet de cette méthode est d'agir directement sur les taux de défaillance de chaque équipement. En effet, au lieu d'utiliser la valeur moyenne calculée par l'estimateur du maximum de vraisemblance à partir de données issues du retour d'expérience, c'est la borne supérieure de l'intervalle de confiance unilatéral à 70% qui est utilisée.

Soient les notations suivantes, pour un équipement donné :
- $\hat{\lambda}$: estimateur du taux de défaillance (moyenne) ;
- $\lambda_{70\%}$: borne supérieure à 70% ;
- n : nombre de défaillances en fonctionnement observées ;
- T : durée cumulée de fonctionnement observé.

L'estimation du maximum de vraisemblance donne :

$$\hat{\lambda} = \frac{n}{T} \quad \{1\}$$

On peut démontrer que (voir [5], p215) :

$$2\lambda T \sim \chi^2_{(2n+2)} \quad \{2\}$$

où $\chi^2(.)$ représente la fonction du Chi^2 couramment utilisée en statistiques.

Donc, on peut en déduire :

$$P\left(2\lambda T \leq {\chi^2_{2n+2}}^{-1}(\alpha)\right) = 1-\alpha \Leftrightarrow P\left(\lambda \leq \frac{{\chi^2_{2n+2}}^{-1}(\alpha)}{2T}\right) = 1-\alpha \quad \{3\}$$

Où ${\chi^2_{2n+2}}^{-1}$ est la fonction réciproque d'une loi Chi-2 à $2n+2$ degrés de liberté.

3.2 Méthode 2

L'objet de cette méthode consiste à simuler les incertitudes liées aux données par le biais de lois probabilistes. On évalue tout d'abord les bornes d'un intervalle de confiance encadrant l'estimateur du maximum de vraisemblance et tel que la probabilité d'être à l'extérieur de cet intervalle est soit égale α%. Si on considère un intervalle symétrique la probabilité d'être inférieur (respectivement supérieur) à la borne inférieure (respectivement supérieure) est égale à 1-α/2.

Par défaut, on considère un intervalle de confiance à 90%, donc $\alpha = 10\%$.

Soient les notations suivantes, pour un équipement donné :
- $\hat{\lambda}$: estimateur du taux de défaillance ;
- λ_{sup} : borne supérieure de l'intervalle de confiance au niveau de confiance 1 - $\frac{\alpha}{2}$;
- λ_{inf} : borne inférieure de l'intervalle de confiance au niveau de confiance 1 - $\frac{\alpha}{2}$;
- n : nombre de défaillances en fonctionnement ;
- T : durée cumulée de fonctionnement.

On en déduit que :

$$\lambda_{sup} = \frac{{\chi^2_{2n+2}}^{-1}\left(1-\frac{\alpha}{2}\right)}{2T} \; ; \; \lambda_{inf} = \frac{{\chi^2_{2n}}^{-1}\left(\frac{\alpha}{2}\right)}{2T} \quad \{4\}$$

Dans cette méthode de prise en compte des incertitudes, on considère donc que $\hat{\lambda}$ n'est pas une valeur déterministe mais qu'elle suit une certaine distribution. Pour pouvoir utiliser cette méthode dans *GRIF-Tree* (outil de modélisation par arbres de défaillance propriété de Total), on utilise la loi log-normale qui paraît relativement bien approprié. Pour ce faire on considère que l'intervalle de confiance à $1-\alpha$% de cette loi log-normale est le même que celui obtenu par la loi du Chi-2. Le lien est facile à faire en utilisant une autre grandeur, appelée Facteur d'Erreur (noté FE), associée à la loi log-normale.

Ce facteur d'erreur est symétrique vis à vis des bornes de l'intervalle de confiance et on a:

$$\lambda_{sup} = FE \times Med \; ; \; \lambda_{inf} = \frac{Med}{FE} \quad \{5\}$$

Où *Med* représente la valeur médiane du taux de défaillance.

Il en résulte :

$$FE = \sqrt{\frac{\lambda_{sup}}{\lambda_{inf}}} = \sqrt{\frac{X_{\left(1-\frac{\alpha}{2}\right)}}{X_{\left(\frac{\alpha}{2}\right)}}} \quad \{5\}$$

Où $X_{\left(1-\frac{\alpha}{2}\right)}$ et $X_{\left(\frac{\alpha}{2}\right)}$ sont les quantiles de la loi log-normale de paramètre (μ, σ^2) respectivement d'ordre $1-\frac{\alpha}{2}$ et $\frac{\alpha}{2}$.

3.3 Exemple

On considère le taux de défaillance des pannes dites « dangereuses non détectées » qui équivaut dans ce cas au « *Fail to function on demand* » d'un capteur de niveau issu d'OREDA 2009 [7].

Les paramètres extraits sont les suivants :

- $\mathrm{T} = 561\,000$ heures ;
- $n = 1$;
- $\hat{\lambda} = \frac{n}{T} = 1.78 \times 10^{-6}$.

Méthode 1 :
On obtient le résultat suivant :

$$\lambda_{70\%} = \frac{{\chi^2_{2n+2}}^{-1}(\alpha)}{2T} = \frac{4.8784}{1.122\times10^6} = 4.35 \times 10^{-6} \quad \{6\}$$

Méthode 2 :
On obtient les résultats suivants :

$$\lambda_{sup} = \frac{{\chi^2_{2n+2}}^{-1}(1-\frac{\alpha}{2})}{2T} = \frac{9.4877}{1.122\times10^6} = 8.46 \times 10^{-6} \text{ ; } \lambda_{inf} = \frac{{\chi^2_{2n}}^{-1}(\frac{\alpha}{2})}{2T} = \frac{0.1026}{1.122\times10^6} = 9.14 \times 10^{-8} \quad \{7\}$$

$$FE = \sqrt{\frac{X_{\left(1-\frac{\alpha}{2}\right)}}{X_{\left(\frac{\alpha}{2}\right)}}} = \sqrt{\frac{\lambda_{sup}}{\lambda_{inf}}} = \sqrt{\frac{8.46\times10^{-6}}{9.14\times10^{-8}}} = 9.6169 \quad \{8\}$$

Nota: ce facteur d'erreur correspond à une loi relativement dispersée. Ceci est normal car seulement une seule observation a été enregistrée

4. Applications

4.1 Système en série

On considère un séparateur deux phases (une sortie liquide et une sortie gaz) équipé de deux capteurs de niveau. En cas de niveau haut dans le séparateur, les capteurs de niveau (LT A et LT B) en configuration 2 sur 2 transmettent un signal au système d'arrêt d'urgence qui vient fermer une vanne de sectionnement en amont du séparateur (voir Figure 1).

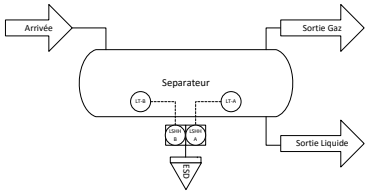

Figure 1. Schéma d'une détection de niveau

On s'intéresse exclusivement à la partie détection de ce système instrumenté de sécurité. En cas de défaillance d'un des capteurs, la détection n'est plus assurée. En diagramme de fiabilité, cela correspond à une configuration en série (voir Figure 2) :

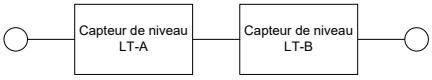

Figure 2. Diagramme de fiabilité des capteurs de niveau en 2 sur 2

Le mode de défaillance critique pour la détection de niveau haut ainsi que la donnée de fiabilité sont fournis au §3.3. Le système instrumenté de sécurité fonctionne à faible demande. La grandeur à quantifier est donc la probabilité de défaillance à la demande (PFD_{avg}).

Calcul sans incertitudes:
Un premier calcul sans les incertitudes (c.-à-d. $\hat{\lambda} = 1.78 \times 10^{-6}$), donne le résultat suivant : $\boldsymbol{PFD_{avg} = 5.78 \times 10^{-3}}$

La fonction de détection est alors SIL 2 c.-à-d. que le PFD_{avg} est compris entre 10^{-2} et 10^{-3}.

Méthode 1 :
Pour rappel : $\lambda_{70\%} = 4.35 \times 10^{-6}$

Les capteurs de niveau sont testés tous les quatre mois : $\tau = 2\,920\ heures$

On construit l'arbre de défaillances (voir Figure 3) équivalent au diagramme de fiabilité et on renseigne les paramètres de la loi. Pour cela, nous avons utilisé la loi test périodique simple de l'outil *GRIF-Tree*.

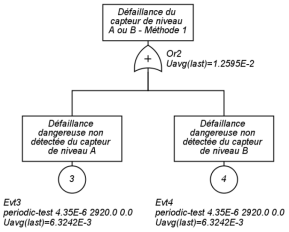

Figure 3. ADD Méthode 1 - cas 2oo2

GRIF-Tree permet de réaliser des calculs ponctuels (probabilité ou fréquence de défaillance) sur un intervalle de temps donné (ici 3 ans). La valeur moyenne PFD_{avg} est alors obtenue sur cet intervalle de temps :

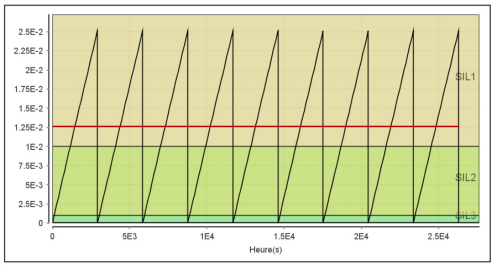

Figure 4. Résultats Méthode 1 - cas 2oo2

La Figure 4 représente *PFD(t)* ainsi que la moyenne PFD_{avg}. Sur la courbe noire (PFD(t)), on remarque que tous les quatre mois, le système est réinitialisé c.-à-d. que le test des capteurs est parfait et qu'il permet de détecter l'ensemble des défaillances dangereuses non détectés. La moyenne est représentée en rouge sur le graphique et on a :

$$\boldsymbol{PFD_{avg} = 1.26 \times 10^{-2}}$$

De plus, on remarque que la fonction de détection est SIL 1 au sens de la norme IEC 61508 c.-à-d. que la moyenne PFD_{avg} est comprise entre 10^{-1} et 10^{-2}.

<u>Méthode 2</u> :

Pour rappel : $\hat{\lambda} = 1.78 \times 10^{-6}$; $\tau = 2\,920\ heures$

On construit alors l'arbre de défaillance qui est rigoureusement similaire à celui montré en Figure 3.

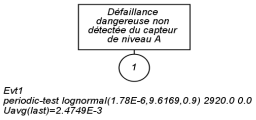

Figure 5. Événement de l'arbre - Méthode 2 - cas 2oo2

On considère « Evt1 » un événement (Voir Figure 5) ayant une loi de probabilité d'occurrence exponentielle (λ), λ n'étant pas une valeur absolue. On souhaite prendre en compte une incertitude. On a alors λ = lognormale ($\hat{\lambda}$, FE, α). FE correspond au facteur d'erreur comme défini dans §3.3. Le paramètre λ va donc être distribué en fonction d'une loi log-normale mais « Evt1 » suit bien une distribution exponentielle.

On effectue ce que l'on appelle une propagation d'incertitude sur un intervalle de temps donné (ici 3 ans) ; et par une simulation de Monte-Carlo, on calcule 10 000 fois la valeur moyenne PFD_{avg}.

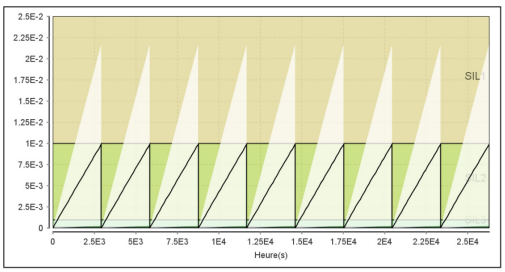

Figure 6. Résultats Méthode 2 - cas 2oo2

La Figure 6 représente le $[PFD(t)]_{avg}$ ainsi que le $[PFD(t)]_{90\%}$. La courbe noire fournit les valeurs moyennes de la $[PFD(t)]_{avg}$ instantanées sur 10 000 histoires (sur 3 ans). Sa moyenne est donc la $[PFD_{avg}]_{avg}$. L'enveloppe de l'aire blanche observée sur le graphique fournit le quantile à 90% des valeurs instantanées sur 10 000 histoires noté ici $[PFD(t)]_{90\%}$.

La norme IEC 61511-2 indique qu'il est préférable de comparer $[PFD_{avg}]_{90\%}$ au lieu de $[PFD_{avg}]_{avg}$ *à* l'objectif. Pour cela, nous avons récupéré l'ensemble des quantiles de la distribution du PFD_{avg} *afin* de tracer un histogramme et de déterminer le $[PFD_{avg}]_{90\%}$.

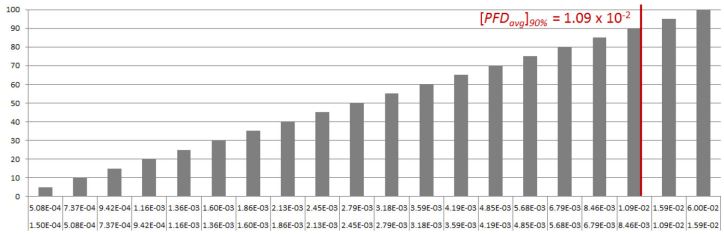

Figure 7. Histogramme des quantiles du PFD_{avg}

$$\left[\boldsymbol{PFD_{avg}}\right]_{\mathbf{90\%}} = \mathbf{1.09 \times 10^{-2}}$$

Comparaison des résultats :
Lorsque l'on compare le résultat de la Méthode 1 avec le PFD_{avg} du calcul sans prise en compte des incertitudes celui-ci-est plus conservatif de 118%. Concernant la Méthode 2, celui-ci est plus conservatif de 88%.

Cette première mise en application sur un système en série montre que la Méthode 2 semble moins pessimiste que la première. Dans cette configuration, la prise en compte des incertitudes entraine des calculs de fiabilité plus conservatifs (SIL 1) en comparaison de la méthode classique (SIL 2).

4.2 Système en parallèle

Le système considéré est le même que celui décrit dans le §4.1 à l'exception des capteurs de niveau qui sont en configuration 1 sur 2. En cas de niveau haut dans le séparateur, les capteurs de niveau (LT A ou LT B) en configuration 1 sur 2 transmettent un signal au système d'arrêt d'urgence qui vient fermer une vanne de sectionnement en amont du séparateur (voir Figure 2). En cas de défaillance d'un des capteurs, la détection reste assurée. En diagramme de fiabilité, cela correspond à une configuration en parallèle.

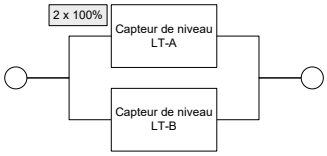

Figure 8. Diagramme de fiabilité des capteurs de niveau en 1oo2

Calcul sans incertitudes:
Un premier calcul sans les incertitudes (c.-à-d. $\hat{\lambda} = 1.78 \times 10^{-6}$), donne le résultat suivant : $\boldsymbol{PFD_{avg}} = \mathbf{2.67 \times 10^{-4}}$

La fonction de détection est alors SIL 3 c.-à-d. que le PFD_{avg} est compris entre 10^{-3} et 10^{-4}.

Méthode 1 :
Tout d'abord, on construit l'arbre de défaillance équivalent au diagramme de fiabilité (Figure 8) et on renseigne les paramètres de la loi (voir §4.1). Le facteur β de cause commune de défaillance (CCF pour *Common Cause Failure*) est pris égal à 10% (CCF1 = 10%). L'arbre de défaillance est alors le suivant :

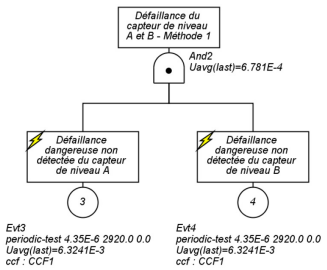

Figure 9. ADD Méthode 1 - cas 1oo2

Afin de faciliter la création de modèle, le module Arbre de défaillance de *GRIF* permet la création de causes communes de défaillance, et permet de lier certaines entités (évènements de base, etc.) à une ou plusieurs défaillances de causes

communes. Les entités liées à une CCF active sont marquées graphiquement par un éclair jaune et cela évite de représenter explicitement les CCF. La Figure 10 représente *PFD(t)* ainsi que la moyenne PFD_{avg}.

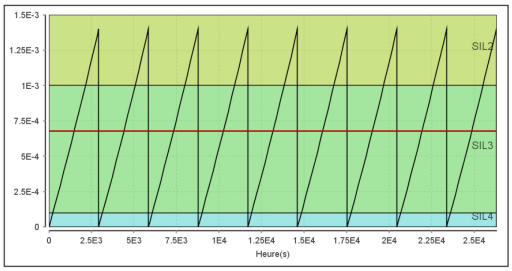

Figure 10. Résultats Méthode 1 - cas 2oo2

PFD$_{avg}$, en rouge sur le graphique, vaut : $\boldsymbol{PFD_{avg} = 6.78 \times 10^{-4}}$

On remarque que la fonction de détection est SIL 3 au sens de la norme IEC 61508 c.-à-d. que la moyenne PFD_{avg} est comprise entre 10^{-3} et 10^{-4}.

Méthode 2 :
On construit un arbre de défaillance similaire à celui de la Figure 9.

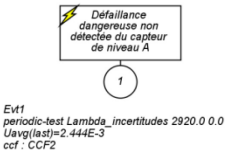

Figure 11. Évènement de l'arbre - Méthode 2 - cas 1oo2

La seule différence avec les évènements de base présentés dans le §4.1 – Méthode 2 est la prise en compte d'une défaillance de cause commune dont le facteur de cause commune de défaillance β est égal à 10% (CCF2 =10%). Le paramètre « Lambda_incertitudes » est égal à lognormale ($\hat{\lambda}$, FE, α) et permet la propagation des incertitudes automatique sur les défaillances de causes communes. On calcule le $PFD_{(t)}$ avec une propagation d'incertitude par simulation de Monte-Carlo; et on obtient les résultats suivants :

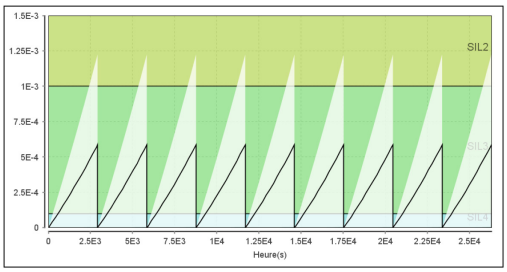

Figure 12. Résultats Méthode 2 - cas 1oo2

La figure 12 représente le $[PFD(t)]_{avg}$ ainsi que le $[PFD(t)]_{90\%}$. La courbe noire fournit les valeurs moyennes de la $[PFD(t)]_{avg}$ instantanées sur 10 000 histoires (sur 3 ans). Sa moyenne est donc la $[PFD_{avg}]_{avg}$. L'enveloppe de l'aire blanche observée sur le graphique fournit le quantile à 90% des valeurs instantanées sur 10 000 histoires noté ici $[PFD(t)]_{90\%}$.

L'objectif est de récupérer le $[PFD_{avg}]_{90\%}$ et pour cela on trace un histogramme (voir §4.1 – Méthode 2).

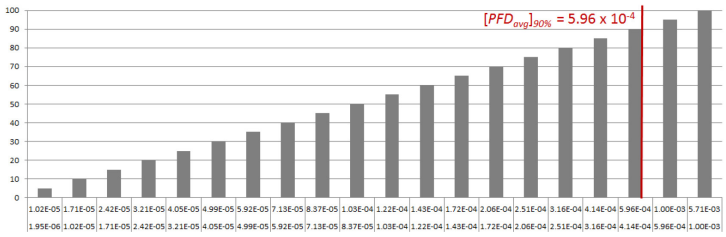

Figure 13. Histogramme des quantiles du PFD$_{avg}$

$$\boldsymbol{[PFD_{avg}]_{90\%} = 5.96 \times 10^{-4}}$$

Comparaison des résultats :
Lorsque l'on compare le résultat de la Méthode 1 avec le PFD_{avg} du calcul sans prise en compte des incertitudes celui-ci-est plus conservatif de 154%. Concernant la Méthode 2, celui-ci est plus conservatif de 123%.

Cette seconde mise en application sur un système en parallèle montre une nouvelle fois que la Méthode 1 semble plus pessimiste que la seconde. Là encore, la prise en compte des incertitudes entraine des calculs de fiabilité plus conservatifs en comparaison de la méthode classique.

4.3 Analyse
La Méthode 1 permet, actuellement, de fournir plus de renseignement sur la probabilité de défaillance à la demande (PFD) du système instrumenté de sécurité. En effet, GRIF fournit le temps passé dans chaque zone SIL et non pas simplement le PFD_{avg}. Pour la Méthode 2, GRIF ne donne que $[PFD_{avg}]_{90\%}$ mais le temps passé dans les zones de SIL pourra être implémenté ultérieurement. On remarque que dans les deux applications ci-dessus la Méthode 1 est plus conservative que la Méthode 2. Il apparait alors que la Méthode 1 peut conduire à un surdimensionnement (donc à un surcoût) des systèmes instrumentés de sécurité par rapport à ce qui est exigé par la norme.

La comparaison des résultats obtenus avec et sans prise en compte des incertitudes montre que la prise en compte des incertitudes est une approche plus conservative qui peut entrainer une augmentation des contraintes envisagées sur les systèmes instrumentés de sécurité. La mise en application la Méthode 1 et la Méthode 2 sur un cas industriel typique devrait permettre de s'assurer de la validité de ces premières conclusions.

5. Système industriel

5.1 Description
Dans le cadre de la conception d'une unité de séparation, un scénario dangereux pouvant conduire à une fuite d'hydrocarbures hautement inflammables a été identifié. En effet, en cas de fermeture/blocage/bouchage de sortie gaz en aval du séparateur, si la production en amont n'est pas stoppée une augmentation de la pression peut survenir à l'intérieur de celui-ci pouvant dépasser la pression que peut supporter l'unité (= surpression). Dans ce cas, les risques d'apparition de fuites sont alors très élevés et l'accident est quasi-inévitable (ignition de la fuite de gaz conduisant à un feu ou une explosion).

Note : une unité de séparation est un système installé généralement au niveau de la partie de l'usine qui réceptionne les conduits de pétrole brut dont la fonction est de séparer le gaz et les liquides afin de pouvoir traiter chacun des flux séparément.

Afin de réduire la probabilité d'occurrence de cet événement redouté, il a donc été décidé de mettre en place un système instrumenté de sécurité de type HIPPS (pour *High-Integrity Pressure Protection System*) ayant pour fonction de fermer le conduit d'arrivée de production en amont du séparateur en cas de forte montée en pression à l'intérieur de celui-ci.

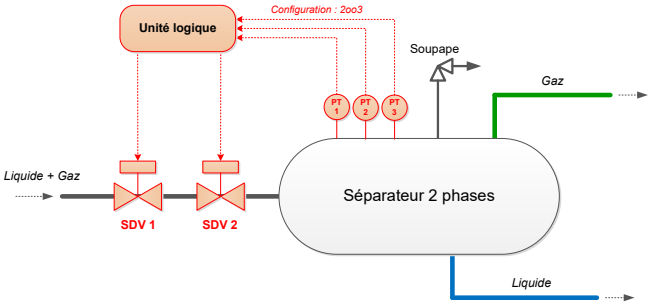

Figure 14. Cas industriel - Schéma du HIPPS

Le but de la Figure 14 est de présenter l'architecture du HIPPS qui protège le séparateur. Si la pression à l'intérieur du séparateur atteint le niveau seuil des capteurs de pression (PT1/2/3) :
- les capteurs de pression en configuration 2 sur 3 envoient des signaux de niveau haut vers l'unité de contrôle logique ;
- l'unité de contrôle logique (dédiée au HIPPS) traite alors les signaux reçus et, lorsqu'il y a au moins deux signaux hauts envoie un ordre de fermeture aux vannes de sécurité SDV 1 et SDV 2 situées sur le conduit en amont du séparateur ;
- la SDV 1 et la SDV 2 se ferment (la fermeture d'une seule de ces vannes est suffisant à fermer la ligne).

5.2 Paramètres d'entrées
Le Tableau 1 fournit l'ensemble des données d'entrée qui permettent de calculer le taux de défaillance des capteurs de pression (PT pour *Pressure Transmitter*) et des vannes de sécurité (SDV pour *ShutDown Valve*) ainsi que les paramètres de prise en compte des incertitudes (voir §3).

D'après [9] p.220, le pourcentage de défaillances dangereuses non détectées en fonctionnement pour les vannes de sécurité (= refus de fermeture à la demande) peut être réparti de la manière suivante :
- 45% des défaillances sont détectées par un test de fermeture partielle ;
- 55% des défaillances sont détectées par un test de fermeture complète.

Sigle	Signification	PT *(note a)*	Unité logique	SDV *(note b)*	SDV *(note c)*
n	Nombre de défaillances en fonctionnement	2	N.A.	8.55	10.45
T	Durée cumulée de fonctionnement (hr)	10 431 800		3 692 800	3 692 800
$\hat{\lambda}$	Estimateur du taux de défaillance (hr^{-1})	1,92 x 10^{-7}		2,32 x 10^{-6}	2,83 x 10^{-6}
$\lambda_{70\%}$	Borne supérieure à 70% (hr^{-1})	3,47 x 10^{-7}		2,94 x 10^{-6}	3.38 x 10^{-6}
FE	Facteur d'erreur	4,2091		1,8644	1,7682
REF	Référence	[8] p.394		[7] p.526	[7] p.526

N.A. : Non-applicable
Note a : Le mode défaillance considéré est « Fail to function on demand ».
Note b : Le mode de défaillance considéré est « Fail to close on demand ». Il est détecté par un test de fermeture partielle.
Note c : Le mode de défaillance considéré est « Fail to close on demand ». Il est détecté par un test de fermeture complète.

Table 1. Cas industriel - Paramètres du taux de défaillance

Causes communes de défaillance :
Une cause commune de défaillance est le résultat d'un (ou de plusieurs) événement(s), qui, à cause de dépendances, provoque une simultanéité d'états de défaillance des composants redondants d'un système.

Il est donc essentiel que les causes communes de défaillance soient correctement modélisées pour chaque groupe de composants en redondance. Le facteur β défini dans les diverses normes internationales est le plus souvent utilisé. Il est supposé être une proportion fixe (β) du taux de défaillances des composants concernés. Il a été considéré ici un facteur β égal à 10% pour les transmetteurs de pression ainsi que pour les vannes de sécurité. A noté que, d'après le tableau D.5 de l'annexe 6 de [3], le facteur β pour une configuration 2 sur 3 (c.-à-d. pour nos transmetteurs de pression) correspond à 1,5β.

Le Tableau 2 fournit l'ensemble des paramètres des lois « test périodique complète » utilisées au niveau des événements de base de l'arbre de défaillance. Les défaillances critiques de l'unité logique sont simulées par une loi constante.

Paramètres		Signification	PT1/2/3 (*note a*)	Unité logique	SDV1/2 *(note c)*	SDV1/2 *(note d)*
Sigle	Nature					
λ	Taux	Taux de défaillance en fonctionnement	Voir Tableau 1	SIL 3 γ = 5 x 10^{-4}	Voir Tableau 1	Voir Tableau 1
λ*	Taux	Taux de défaillance durant le test	0 (note e)	N.A.	= λ	0 (prod. SD)
μ	Taux	Taux de réparation/remplacement *(note b)*	0.25	N.A.	prod. SD	prod. SD
τ	Durée	Intervalle entre 2 tests consécutifs (hr)	2190	N.A.	2190	8760
θ	Durée	Date du premier test (hr)	2190 / 2191 / 2192	N.A.	2193 / 2194	8760
γ	Probabilité	Probabilité de défaillance due au test	10^{-3}	N.A.	10^{-3}	10^{-3}
Π	Durée	Durée du test (hr)	0.5	N.A.	0.5	0 (prod. SD)
X	Booléen	Disponibilité durant le test	0 (Note e)	N.A.	0	1
σ	Probabilité	Taux de couverture du test	0,99	N.A.	1	1
ϖ	Probabilité	Probabilité d'oubli de reconfiguration	10^{-3}	N.A.	10^{-3} (note f)	0

N.A. : Non-applicable
prod. SD : Arrêt de la production.
Note a : Les capteurs défaillants ne sont pas réparés mais remplacés.
Note b : Il est considéré que les pièces de rechange pour les capteurs sont disponibles.
Note c : La défaillance est détectée par un test de fermeture partielle.
Note d : La défaillance est détectée par un test de fermeture complète.
Note e : Le capteur est débranché.
Note f : Oubli de retirer le bypass de la SOV.

Table 2. Cas industriel - Paramètres des lois « test périodique complète »

5.3 Résultats

Calcul sans incertitudes:
Un calcul sans les incertitudes donne le résultat suivant : $\boldsymbol{PFD_{avg} = 2.28 \times 10^{-3}}$

La fonction de détection est alors SIL 2 c.-à-d. que le PFD_{avg} est compris entre 10^{-2} et 10^{-3}.

Méthode 1 :
On construit l'arbre de défaillance (Voir Figure 15) décrivant l'indisponibilité non révélée du HIPPS et on paramètre les événements de base comme défini dans les Tables 1 et 2.

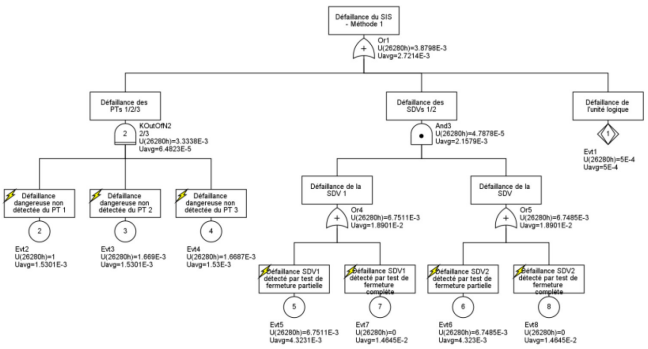

Figure 15. Cas industriel - Arbre de défaillance construit pour l'estimation de PFD(t)

La Figure 16 représente *PFD(t)* ainsi que la moyenne PFD_{avg}.

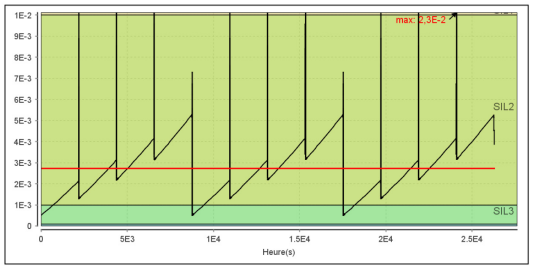

Figure 16. Cas industriel - Résultats méthode 1

PFD_{avg}, en rouge sur le graphique, vaut : $\boldsymbol{PFD_{avg} = 2.72 \times 10^{-3}}$

On peut noter que le HIPPS est SIL 2 c.-à-d. que la moyenne PFD_{avg} est comprise entre 10^{-2} et 10^{-3}.

Méthode 2 :
PFD(t) est calculé avec une propagation d'incertitude par simulation de Monte-Carlo :

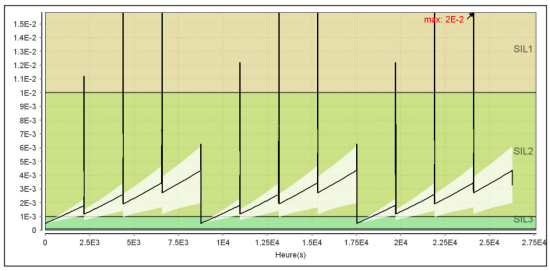

Figure 17. Cas industriel - Résultats méthode 2

La Figure 17 montre $[PFD(t)]_{avg}$ ainsi que $[PFD(t)]_{90\%}$. La courbe noire fournit les valeurs moyennes instantanées de $[PFD(t)]_{avg}$ sur 10 000 histoires d'une durée de 3 ans. Sa moyenne est donc la $[PFD_{avg}]_{avg}$. L'enveloppe de l'aire blanche observée sur le graphique fournit le quantile à 90% des valeurs instantanées sur 10 000 histoires notée ici $[PFD(t)]_{90\%}$.

L'objectif est de récupérer le $[PFD_{avg}]_{90\%}$ et pour cela on trace un histogramme (voir §4.1 – Méthode 2).

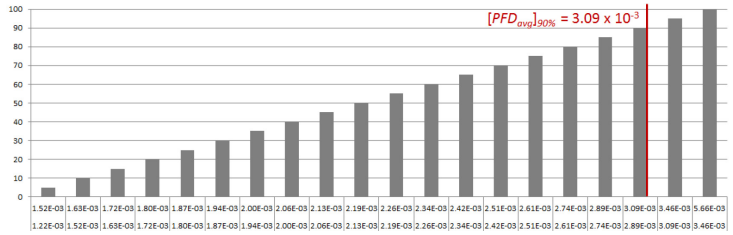

Figure 18. Cas industriel - Histogramme des quantiles du PFD_{avg}

$$\left[\boldsymbol{PFD_{avg}}\right]_{90\%} = \mathbf{3.09 \times 10^{-3}}$$

Comparaison des résultats :
Lorsque l'on compare le résultat de la Méthode 1 avec le PFD_{avg} du calcul sans prise en compte des incertitudes celui-ci-est plus conservatif de 19%. Concernant la Méthode 2, celui-ci est plus conservatif de 35%.

Cette mise en application sur un système industriel montre cette fois que la Méthode 2 est la moins conservative. Ce résultat est surprenant au vue des premières conclusions obtenues sur les systèmes simples (voir §4). Par ailleurs, les principaux contributeurs à l'indisponibilité du HIPPS sont les vannes et il est important de noter que celles-ci ont une faible dispersion. Les calculs du §3 ont été repris avec les données de fiabilité issues de la Table 1, et on remarque que plus l'incertitude sur les données de fiabilité est faible, moins la Méthode 2 est conservative.

Ce résultat montre une nouvelle fois que, quelle que soit la méthode utilisée, la prise en compte des incertitudes donne des résultats plus conservatifs en comparaison de la méthode classique (sans prise en compte des incertitudes).

6. Conclusions

Cette communication a permis de proposer et d'appliquer deux méthodes de prise en compte des incertitudes sur les données de fiabilité et de les comparer à la méthode classique d'évaluation de la fiabilité des systèmes instrumentés de sécurité.

Il apparait que la Méthode 1 est plus pessimiste lorsque l'incertitude sur les données est grande. A l'inverse, la Méthode 2 est plus pessimiste lorsque l'incertitude est faible.

La mise en œuvre de ces deux méthodes n'est en soit pas compliquée en utilisant la suite logicielle GRIF. Les temps de calcul nécessaires pour la Méthode 2 peuvent être significatifs (plusieurs minutes) alors qu'ils sont quasi-instantanés pour la Méthode 1. La méthode 2 peut être réservée aux cas limites où la PFD_{avg} approche une limite de zone de SIL de manière à choisir la meilleure solution des deux.

Enfin, la Méthode 2 calcule le facteur d'erreur à partir des bornes inférieure $\lambda_{5\%}$ et supérieure $\lambda_{95\%}$ via les Chi-2. On aurait pu prendre la valeur de l'écart-type issue des données de [7] et [8] pour calculer le facteur d'erreur mais, comme les détails des valeurs sources ne sont pas disponibles directement, il est difficile de calculer cet écart type. Une autre solution serait d'utiliser directement la loi du Chi-2 à la place de la loi log-normale mais elle n'est pas implémentée actuellement dans GRIF. Ces approches feront l'objet d'études ultérieures.

7. Abréviations

ADD	Arbre De Défaillance
Avg	*Average*
CCF	*Common Cause Failure*
ESD	*Emergency ShutDown*
FE	Facteur d'Erreur
GRIF	GRaphiques Interactifs pour la Fiabilité
HIPPS	*High-integrity pressure protection system*
IEC	*International Electrotechnical Commission*
KooN	K *out of* N (logique de *voting*)
LT	*Level Transmitter*
OREDA	*Offshore and Onshore REliability DAta*
PFD	*Probability of Failure on Demand*
PFH	*Probability of Failure per Hour*
PT	*Pressure transmitter*
SD	*Shut Down*
SDV	*Shut Down Valve*
SFF	*Safe Failure Fraction*
SIL	*Safety Integrity Level*

8. Références

[1] IEC 61511-1 : *Sécurité fonctionnelle – systèmes instrumentes de sécurité pour le secteur des industries de transformation* – Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application, Ed. 2.0 (version en cours de validation)

[2] IEC 61511-2 : *Sécurité fonctionnelle – systèmes instrumentes de sécurité pour le secteur des industries de transformation* – Partie 2: Ed. 2.0 (version provisoire)

[3] IEC 61508 : *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*, Ed. 2.0

[4] F. Brissaud, E. Rosner, *Probabilistic risk assessment considering parameter and model uncertainties*, 25th European Safety and RELiability conference (ESREL), Zürich, Switzerland, September 7-10, 2015

[5] Alain Pagès, Michel Gondran, Fiabilité des systèmes, Eyrolles, 01/11/1980

[6] *Probability and frequency calculations related to protection layers revisited* - Fares Innal, Pierre-Joseph Cacheux, Stéphane Collas, Yves Dutuit, Cyrille Folleau, Jean-Pierre Signoret, Philippe Thomas, Journal of Loss Prevention in the Process Industries 31 (2014) 56-69

[7] OREDA participants, OREDA, Offshore Reliability Data Handbook, Volume 1 – topside data. 5th edition, 2009.

[8] OREDA participants, OREDA, Offshore Reliability Data Handbook, Volume 1 – topside equipment. 6th edition, 2015.

[9] EXIDA : Safety Equipment Reliability Handbook, Third edition, Volume 3: Final Elements

Mots clés

Incertitudes, Données de fiabilité, IEC 61508, IEC 61511, SIL, *PFD_{avg}*, *PFH*, Systèmes instrumentés de sécurité, Arbre de défaillance.