Modélisation des causes communes de défaillance d'un système instrumenté de sécurité particulier

Torbjorn Lilleheier, Florent Brissaud

MODELISATION DES CAUSES COMMUNES DE DEFAILLANCE D'UN SYSTEME INSTRUMENTE DE SECURITE PARTICULIER

Torbjørn LILLEHEIER [1,2,3] & Florent BRISSAUD [1]

[1] *Institut National de l'Environnement Industriel et des Risques (INERIS)*
Parc Technologique ALATA BP-2, 60550 Verneuil-en-Halatte, France
florent.brissaud@ineris.fr

[2] *The Norwegian University of Science and Technology (NTNU)*
7034 Trondheim, Norvège

[3] *Safetec Nordic AS*
Lilleakerveien 10, 0216 Oslo, Norvège
torbjorn.lilleheier@safetec.no

Résumé :

Depuis le milieu des années soixante-dix, les causes communes de défaillance (CCF) ont donné lieu à de nombreuses études de fiabilité [1], notamment pour les systèmes instrumentés de sécurité (SIS). L'objectif de cet article est de présenter différentes approches de modélisation des causes communes de défaillance, appliquées à un système de surveillance de pression d'huile pour une turbine à gaz. Ce système présente quelques particularités qui rendent la modélisation délicate : une architecture *2oo3* avec un sous-système interne d'architecture *1oo2*, ainsi que des taux de défaillance hétérogènes. Les trois méthodes étudiées sont : le facteur β, la méthode PDS [2] et l'analyse par processus Markovien. Le modèle du facteur β est relativement simple mais ne permet pas une modélisation exhaustive des causes communes de défaillance, notamment en omettant les causes communes de défaillance partielles. La méthode PDS cherche à pallier cela, moyennant l'utilisation de quelques paramètres supplémentaires. L'analyse par processus Markovien est la plus souple et peut s'adapter plus simplement aux architectures complexes et à de nombreux paramètres d'entrée. Les probabilités moyennes de défaillance obtenues pour le système instrumenté de sécurité peuvent varier de façon significative d'un modèle à l'autre. Il convient alors de choisir la méthode la plus adéquate en fonction des hypothèses requises, de l'architecture du système, du degré de modélisation voulu et des informations disponibles.

Abstract:

Common cause failures (CCFs) are an important part of reliability analysis when working with safety instrumented systems (SIS), and engineers have been aware of these types of failures since the mid-seventies [1]. The purpose of this article is to develop a strategy to study an example on oil-pressure system and propose a CCF-strategy for that present example. The focus is given to the following three methods: the β-factor model, the PDS method [2], and Markov analysis with stochastic simulation. The need for Markov analysis becomes evident when working with SIS of a more complex nature, for instance non-identical components. Finally, it is always important to remember that if there exists any feedback data or expert knowledge describing the distribution of the number of components that fail in a CCF, this is vital in deciding the most descriptive CCF model. By the term descriptive model, we mean a model that both describes the architecture of the system as accurately as possible, and also makes as few assumptions as possible.

Mots clés : Cause commune de défaillance, CCF, Système instrumenté de sécurité, SIS, facteur β, méthode PDS, Processus de Markov

Keywords: Common cause failure, CCF, Safety instrumented system, SIS, β-factor, PDS method, Markov analysis

1. Introduction

De nombreux travaux cherchent à expliquer l'origine des causes communes de défaillance (CCF) et à modéliser leurs impactes sur la fiabilité des systèmes. Bien qu'ils aient donné lieu à une grande quantité de références, la nature relativement complexe de ces défaillances rend leurs quantification encore difficile et leurs inclusion dans les études de fiabilité n'est pas une chose aisée. En effet, lorsqu'une défaillance d'un composant se produit, il est par exemple difficile de savoir si la cause a eu un effet sur plusieurs autres composants, ou alors si l'origine du phénomène est plus individuelle, comme le vieillissement. Ceci explique probablement que peu de retour d'expérience détaillent les défaillances de cause commune, ce qui rend la modélisation relativement difficile, faute de données exploitables. De plus, les différences importantes entre les systèmes expliquent qu'un modèle peu parfois être adapté à certaines situations mais inapproprié à d'autres cas.

L'étude présentée dans cet article est le fruit d'un travail universitaire [3] effectué en collaboration avec l'Institut National de l'Environnement Industriel et des Risques (INERIS) et l'Université de Science et Technologie de Norvège (NTNU). L'évaluation d'un système de surveillance de pression d'huile pour une turbine à gaz a été rapportée. Il s'agit d'un système instrumenté de sécurité (SIS) dont la fonction instrumentée de sécurité (SIF) étudiée est la détection de la pression basse d'huile. L'enjeu pour la sécurité étant important, la norme CEI 61508 [4] définie certaines exigences en sécurité fonctionnelle pour une telle fonction. Il convient notamment d'évaluer l'intégrité de sécurité : *probabilité qu'un système concerné par la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps donnée* [4]. Dans le cas de ce système, la quantification de l'intégrité de sécurité passe par l'évaluation de la probabilité moyenne de défaillance à la demande (PFD) de la fonction instrumentée de sécurité. L'objectif de cet article est de présenter différentes méthodes pour la prise en compte des causes communes de défaillance dans cette évaluation.

La Section 2 présente brièvement le système étudié. Ensuite, trois approches ont été retenues pour modéliser les causes communes de défaillance : le modèle du facteur β, la méthode PDS [2], et une analyse par processus Markovien. Après la présentation et l'application de chacune d'elle au cas d'étude dans la Section 3, les résultats obtenus sont discutés dans la Section 4.

Notations et hypothèses préalables

■ ***MooN* – architecture d'un système/ sous-système** : le système/ sous-système est formé de N composants et est opérant si et seulement si au moins M de ces composants sont opérants (avec $M \leq N$)

■ ***λ(t)* – taux des défaillances dangereuses et non détectées d'un élément (composant/ système/ sous-système)** [par heure] : sachant que l'élément est opérant à l'instant t, $\lambda(t)\cdot\Delta t$ est la probabilité pour qu'une défaillance dangereuse et non détectée de l'élément se produise dans l'intervalle $[t, t+\Delta t]$ lorsque Δt tend vers 0

■ ***T1* – période des tests de révision** [heure] : après chaque test de révision, tous les éléments (composants/ systèmes/ sous-systèmes) sont comme neuf (les tests sont complets et parfaits). La durée des actions de maintenance ne sera pas prise en compte dans les calculs de probabilité de défaillance

***PFD* – probabilité moyenne de défaillance à la demande du système**

2. Cas d'étude : système de surveillance de pression d'huile pour une turbine à gaz

Le cas d'étude porte sur un système de détection de pression basse d'huile pour une turbine à gaz. Celui-ci est constitué de quatre composants et d'une unité logique. Cette dernière n'est pas prise en compte dans l'évaluation. Les composants 1 et 2 sont des manostats en redondance (architecture *1oo2*) et forment un sous-système interne. Il est lui-même monté dans une architecture *2oo3* avec les composants 3 et 4 qui sont des pressostats. La Figure 1 représente l'architecture générale du système.

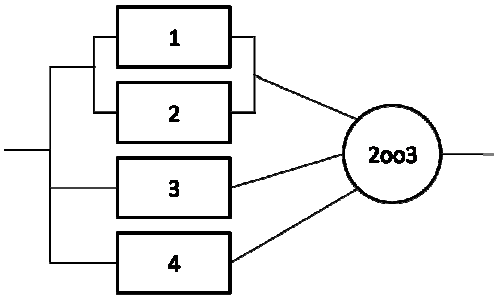

Figure 1. *Architecture du système de surveillance de pression d'huile*

Les taux des défaillances dangereuses et non détectées des composants 1 à 4 sont respectivement : $\lambda_1 = 1.7 \cdot 10^{-6}$ *heures*$^{-1}$; $\lambda_2 = 6.0 \cdot 10^{-6}$ *heures*$^{-1}$; $\lambda_3 = 3.4 \cdot 10^{-5}$ *heures*$^{-1}$ et $\lambda_4 = 3.4 \cdot 10^{-5}$ *heures*$^{-1}$. La proportion des défaillances dues à des causes communes, tous composants compris, est estimée à *5%*. Enfin, nous utiliserons une période des tests de révision d'un an, c'est-à-dire $T_1 = 8760$ *heures*.

L'objectif est d'évaluer la probabilité moyenne de défaillance à la demande de ce système, en incluant les effets des causes communes de défaillance. Les trois approches utilisées sont : le modèle du facteur β, la méthode PDS, et une analyse par processus Markovien.

3. Modélisation des causes communes de défaillance

3.1. Le modèle du facteur β

Le modèle du facteur β est sans doute le plus utilisé pour la modélisation des causes communes de défaillance. Il a initialement été proposé par K. Fleming en 1974 [1]. L'hypothèse principale est que chaque composant i du système (avec $i = 1,\ldots,N$) peut être défaillant à cause :

■ de circonstances n'ayant eu un effet que sur le composant en question – le taux des défaillances correspondantes, dites « indépendantes », est noté $\lambda_i^{(i)}$
■ de l'occurrence d'un évènement qui a provoqué la défaillance de tous les N composants du système simultanément – le taux des défaillances correspondantes, dites « de cause commune », est noté $\lambda_i^{(c)}$

On remarque alors que, d'après ce modèle, une défaillance de cause commune provoque systématiquement la défaillance tous les N composants du système. Les défaillances de causes communes partielles, c'est-à-dire qui ne provoquent la défaillance que d'un sous ensemble de j composants du système (avec $1 < j < N$) ne sont donc pas pris en compte.

Le taux de défaillance total de chaque composant i du système (avec $i = 1,\ldots,N$), noté λ_i, est alors :

$$\lambda_i = \lambda_i^{(i)} + \lambda_i^{(c)} \qquad (1)$$

Le facteur β est le facteur de cause commune de défaillance. Il est défini comme la probabilité d'une défaillance de cause commune, sachant la présence d'une défaillance. La Figure 2 représente la répartition des défaillances selon le modèle du facteur β, pour un système formé de trois composants. Comme ce facteur est spécifié pour l'ensemble des composants du système, par défaut, la moyenne géométrique des taux de défaillance des composants du système est souvent utilisée [2], notée λ_{mean} (elle-même décomposée en une partie indépendante, $\lambda_{mean}^{(i)}$, et une partie de cause commune, $\lambda_{mean}^{(c)}$) :

$$\beta = \frac{\lambda_{mean}^{(c)}}{\lambda_{mean}^{(i)} + \lambda_{mean}^{(c)}} = \frac{\lambda_{mean}^{(i)}}{\lambda_{mean}} \qquad (2)$$

La probabilité moyenne de défaillance à la demande d'un système *MooN*, notée *PFD*, peut alors être approximé par la somme de la probabilité moyenne de défaillance indépendante à la demande, notée $PFD^{(i)}$, et de la probabilité moyenne de défaillance de cause commune à la demande, notée $PFD^{(c)}$:

$$PFD \approx PFD^{(i)} + PFD^{(c)} \quad (3)$$

$PFD^{(i)}$ s'exprime en fonction de l'architecture du système et avec les taux des défaillances indépendantes des composants. Afin d'utiliser l'équation approchée (4), valable lorsque tous les composants du système ont le même taux de défaillance [5], la moyenne géométrique $\lambda_{mean}^{(i)}$ est utilisée par défaut [2] :

$$PFD^{(i)} \approx \binom{N}{M-1} \cdot \frac{\left(\lambda_{mean}^{(i)} \cdot T_1\right)^{N-M+1}}{N-M+2} = \binom{N}{M-1} \cdot \frac{\left((1-\beta) \cdot \lambda_{mean} \cdot T_1\right)^{N-M+1}}{N-M+2} \quad (4)$$

D'après le modèle du facteur β, une défaillance de cause commune provoque la défaillance de tous les composants du système. Ainsi, le taux des défaillances de cause commune de chacun des composants du système est également le taux des défaillances de cause commune de tout le système. $PFD^{(c)}$ s'exprime alors selon une architecture *1oo1*, quelque soit l'architecture *MooN* du système, et avec le taux des défaillances de cause commune. Pour les mêmes raisons que pour l'équation (4), la moyenne géométrique $\lambda_{mean}^{(c)}$ est utilisée :

$$PFD^{(c)} \approx \frac{\lambda_{mean}^{(c)} \cdot T_1}{2} = \frac{\beta \cdot \lambda_{mean} \cdot T_1}{2} \quad (5)$$

Dans notre étude de cas, le système a une architecture *2oo3*, formé du sous-système interne et des composants 2 et 3. Pour déterminer λ_{mean} nous proposons donc tout d'abord d'évaluer le taux de défaillance moyen du sous-système interne, formé des composants 1 et 2 en redondance (architecture *1oo2*), noté $\lambda_{1,2}$. Afin d'utiliser l'équation (6), valable lorsque les deux composants ont le même taux de défaillance [6], nous utiliserons la moyenne géométrique de λ_1 et λ_2, noté $\lambda_{mean,1,2}$:

$$\lambda_{1,2} \approx \left(\lambda_{mean,1,2}\right)^2 \cdot T_1 = \left(\sqrt{\lambda_1 \cdot \lambda_2}\right)^2 \cdot T_1 = \lambda_1 \cdot \lambda_2 \cdot T_1 = 8.94 \cdot 10^{-8} \ \textit{par heure} \quad (6)$$

La moyenne géométrique des taux de défaillance des trois composants/ sous-système interne du système d'architecture *2oo3* est alors :

$$\lambda_{mean} = \sqrt[3]{\lambda_{1,2} \cdot \lambda_3 \cdot \lambda_4} = 4.69 \cdot 10^{-6} \ \textit{par heure} \quad (7)$$

Avec un facteur $\beta = 0.05$ (cf. section 2), et d'après les équations (3) à (5), appliquées à une architecture *2oo3*, nous obtenons la probabilité moyenne de défaillance à la demande du système :

$$PFD \approx PFD^{(i)} + PFD^{(c)} \approx \left((1-\beta) \cdot \lambda_{mean} \cdot T_1\right)^2 + \frac{\beta \cdot \lambda_{mean} \cdot T_1}{2} = 1.53 \cdot 10^{-3} + 1.03 \cdot 10^{-3} = 2.55 \cdot 10^{-3} \quad (8)$$

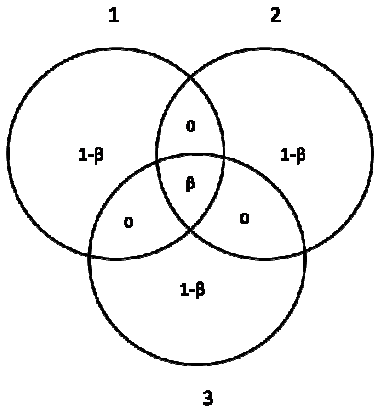

Figure 2. *Répartition des défaillances selon le modèle du facteur-β pour un système à 3 composants*

3.2. La méthode PDS

La méthode PDS a initialement été développée par la SINTEF pour l'industrie pétrolière offshore [2]. PDS est un acronyme norvégien pour *fiabilité et disponibilité des systèmes gérés par informatique*. Contrairement au modèle du facteur β, la méthode PDS cherche à modéliser les causes communes de défaillance partielles, ce qui a pour conséquence d'adapter la probabilité de défaillance de cause commune ($PFD^{(c)}$) en fonction de l'architecture *MooN* du système. L'idée principale est d'introduire un coefficient d'architecture *MooN*, noté C_{MooN}, tel que :

$$PFD^{(c)} \approx C_{MooN} \cdot \frac{\beta \cdot \lambda_{mean} \cdot T_1}{2} \tag{9}$$

Un nouveau paramètre est alors introduit, noté β_p, qui est la probabilité d'une défaillance additionnelle d'un composant *i* spécifique, sachant que *p* composants sont défaillants (*p* n'inclut pas le composant *i*). La même valeur de β_p étant attribuée à tous les composants *i* du système (avec $i = 1,\ldots,N$), une homogénéité complète est supposée, c'est-à-dire que chaque combinaison de *j* composants défaillants et *N-j* composants non défaillants a la même probabilité d'occurrence. La Figure 3 représente la répartition des défaillances selon la méthode PDS, pour un système formé de trois composants. L'égalité $\beta_1 = \beta$ est posée par défaut, ce qui permet de faire correspondre les résultats de la méthode PDS avec ceux du modèle du facteur β, pour un système d'architecture *1oo2*. Soit β_2 ayant une valeur singulière et $\beta_3 = \beta_4 = \ldots = \beta_{N-1} = \theta$, le coefficient C_{MooN} s'exprime alors ainsi [2] :

$$C_{MooN} = \beta_2 \cdot \sum_{j=N-M+1}^{N} \binom{N}{j} \cdot \theta^{j-3} \cdot (1-\theta)^{N-j} \quad \text{pour } M = 1,2,\ldots,N-2 \tag{10}$$

Lorsque $M = N$, le système est en série et donc chaque défaillance d'un composant provoque la défaillance du système. Il n'est alors pas nécessaire de prendre en compte les causes communes de défaillance. Enfin, dans le cas où $M = N-1$, le coefficient C_{MooN} est [2] :

$$C_{(N-1)ooN} = \binom{N}{2} \cdot \left(1 - \frac{\beta_2}{\theta}\right) + \beta_2 \cdot \sum_{j=2}^{N} \binom{N}{j} \cdot \theta^{j-3} \cdot (1-\theta)^{N-j} \tag{11}$$

Pour les applications numériques, il est suggéré de prendre les valeurs $\beta_2 = 0.3$ et $\theta = 0.5$ [2], ce qui nous donnent les coefficients C_{MooN} donnés dans le Tableau 1. D'après les équations (3), (4), (9), et le Tableau 1, nous obtenons la probabilité moyenne de défaillance à la demande du système :

$$PFD \approx PFD^{(i)} + PFD^{(c)} \approx ((1-\beta) \cdot \lambda_{mean} \cdot T_1)^2 + C_{2oo3} \frac{\beta \cdot \lambda_{mean} \cdot T_1}{2} = 1.53 \cdot 10^{-3} + 2.47 \cdot 10^{-3} = 3.99 \cdot 10^{-3} \tag{12}$$

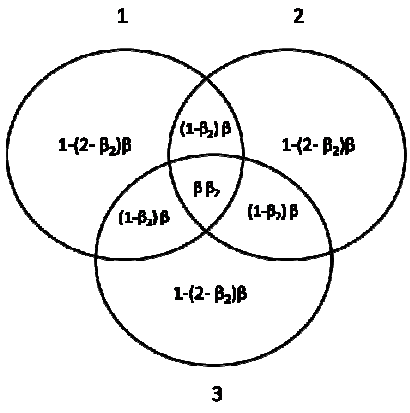

Figure 3. *Répartition des défaillances selon la méthode PDS, pour un système à 3 composants*

Tableau 1. *Coefficients C_{MooN} pour différentes architectures MooN*

	N = 2	***N = 3***	***N = 4***
M = 1	1.00	0.30	0.15
M = 2		2.40	0.75
M = 3			4.00

3.3. Analyse par processus Markovien

Le système étudié est formé de quatre composants, chacun pouvant être dans deux états : opérant ou en défaillance dangereuse et non détectée. Il y a donc $2^4 = 16$ états possibles. Dans l'état initial, tous les composants sont opérants (état 0). Afin de simplifier le graphe de Markov, nous proposons de regrouper dans un même état, la situation où le composant 1 est défaillant mais pas le composant 2, et la réciproque (état 1). Un taux de défaillance identique doit donc être utilisé pour les composants 1 et 2, nous utiliserons pour cela la moyenne géométrique, c'est-à-dire $\lambda_{mean,1,2}$. Il est fait de même pour les composants 3 et 4 (état 3). Les taux de défaillance étant ici les même, nous posons $\lambda_{mean,3,4} = \lambda_3 = \lambda_4$. Lorsque les composants 1 et 2 sont défaillants, le sous-système interne est défaillant (état 2). Une autre situation possible correspond à la défaillance d'un des composants 1 ou 2, et d'un des composants 3 ou 4 (état 4), le système est alors toujours opérant. Dans tous les autres cas seulement, le système est en défaillance dangereuse et non détectée (état 5). La description des états est donnée dans le Tableau 2.

Nous proposons de traduire les causes communes de défaillance sur deux niveaux : défaillance commune totale (i.e. défaillance de l'ensemble des quatre composants du système), et défaillance commune au sous-système interne (i.e. défaillance des composants 1 et 2). Ainsi, lorsqu'un composant devient défaillant :

- il y a une probabilité β pour que la défaillance commune totale se produise
- s'il s'agit du composant 1 ou 2, et si une défaillance commune totale ne s'est pas produite, il y a une probabilité β pour qu'une défaillance commune au sous-système interne se produise

La Figure 4 représente le graphe de Markov utilisé. Il est alors possible de calculer la probabilité d'être dans l'état 5 (i.e. défaillance du système) en fonction du temps. Avec la moyenne de cette probabilité sur l'intervalle $[0, T_1]$, on obtient la probabilité moyenne de défaillance à la demande du système :

$$PFD = 2.97 \cdot 10^{-2} \tag{13}$$

À noter que l'utilisation d'un graphe de Markov « non simplifié » avec les 16 états possibles du modèle, nous amène à une *PFD* proche du résultat (16) à $2 \cdot 10^{-4}$ près.

Tableau 2. *Description des états du graphe de Markov*

État	**Description**
0	Tous les composants sont opérants
1	Défaillance uniquement du composant 1 ou* 2
2	Défaillance uniquement des composants 1 et 2
3	Défaillance uniquement du composant 3 ou* 4
4	Défaillance uniquement des composants (3 ou* 4) et (1 ou* 2)
5	Autres cas : défaillance du système

*les « ou » marqués d'une étoile sont des « ou exclusifs »

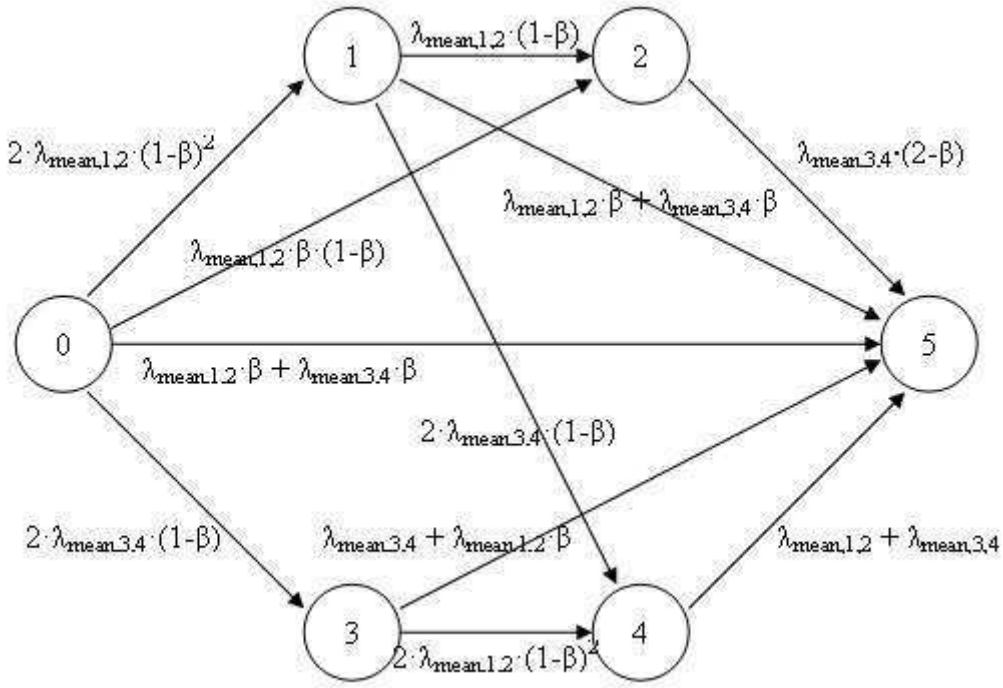

Figure 4. *Graphe de Markov utilisé pour l'analyse du système de surveillance de pression d'huile*

4. Discussion des résultats

Les résultats obtenus par l'application des trois méthodes sont reportés dans le Tableau 3. On remarque que le modèle du facteur β amène à des résultats proches de la méthode PDS. De par la formulation de ces deux approches, les probabilités de défaillance indépendante sont identiques. La probabilité de défaillance de cause commune est quand à elle ajustée par la méthode PDS, afin de prendre en compte les défaillances de cause commune partielle. Compte tenu de l'architecture générale du système, ceci a pour conséquence d'accentuer les probabilités de défaillance, mais d'un ordre de grandeur relativement raisonnable (utilisation d'un coefficient $C_{MooN} = 2.4$).

Avec une analyse par processus Markovien, il est plus difficile de nuancer la partie indépendante de la probabilité de défaillance, de celle de cause commune. Les résultats totaux sont cependant très différents que ceux des deux premières approches, avec un rapport de l'ordre de dix. Ceci peut notamment s'expliquer par les différentes hypothèses qui ont été faites d'un modèle à l'autre. Une analyse par processus de Markov est en effet plus souple sur les possibilités d'inclusion de différents paramètres (utilisation de $\lambda_{mean,1,2}$ et $\lambda_{mean,3,4}$ à la place d'un seul taux de défaillance moyen λ_{mean}), et de prise en compte des causes communes de défaillance (un facteur β pour l'ensemble des composants, et un facteur β uniquement pour les composants du sous-système interne).

Tableau 3. *Synthèse des résultats*

Méthodes	$PFD^{(i)}$	$PFD^{(c)}$	PFD
Modèle du facteur β	$1.53\cdot10^{-3}$	$1.03\cdot10^{-3}$	$2.55\cdot10^{-3}$
Méthode PDS	$1.53\cdot10^{-3}$	$2.47\cdot10^{-3}$	$3.99\cdot10^{-3}$
Markov	-	-	$2.97\cdot10^{-2}$

5. Conclusion

Dans cet article nous avons étudié trois méthodes d'inclusion des causes communes de défaillance dans l'évaluation des probabilités de défaillance : modèle du facteur β, méthode PDS, analyse par processus Markovien. L'étude a porté sur un système de surveillance de pression d'huile pour une turbine à gaz. Celui-ci présente certaines caractéristiques particulières : l'architecture est en *2oo3* avec un sous-système interne en *1oo2*, ainsi que des taux de défaillances qui ne sont pas identiques. L'application des méthodes pour la prise en compte des causes communes de défaillance nécessite donc certaines adaptations, souvent utilisées « par défaut ». Ici, nous avons par exemple eu recours à la moyenne géométrique des taux de défaillance afin d'appliquer le modèle du facteur β et la méthode PDS.

De part sa relative simplicité, le modèle du facteur β est le plus communément utilisé. Un inconvénient est que les causes communes de défaillance partielles ne sont pas prises en compte. Ainsi, une défaillance de cause commune implique forcément la défaillance de tous les composants d'un système, et non d'un quelconque sous-ensemble de composants. Ceci implique notamment que la probabilité de défaillance de cause commune indépendante ne soit pas exprimée en fonction de l'architecture du système. Pour pallier cela, la méthode PDS cherche à calculer un coefficient de correction, fonction de l'architecture du système. Ce coefficient multiplicateur du facteur β se fonde sur une répartition des causes communes de défaillance, en accord avec certains paramètres, et de façon homogène parmi les composants du système. Les paramètres introduits sont cependant difficiles à évaluer et des valeurs par défaut sont proposées.

Enfin, une analyse par processus Markovien offre une plus grande liberté dans la modélisation. Il est en particulier plus direct d'inclure des taux de défaillance hétérogènes et plusieurs niveaux de causes communes de défaillance. Lorsque le système possède une architecture non conventionnelle, les processus de Markov sont ainsi avantageux. Néanmoins, le nombre d'états est exponentiel avec le nombre de composants du système, et il est parfois judicieux de faire quelques hypothèses simplificatrices afin d'alléger le graphe, par exemple en regroupant certains composants.

Les différences parfois importantes dans les résultats obtenus par l'application des différentes méthodes, montrent que les hypothèses utilisées sont déterminantes. Il convient donc de choisir la méthode la plus adéquate en fonction des hypothèses requises, du système (architecture, hétérogénéité des composants), du degré de modélisation voulu, et des informations disponibles (coefficient β, paramètres des causes communes de défaillance partielles).

Références

[1] K. Fleming. "A reliability model for common mode failures in redundant systems". *GA-A-13284*, 1974.

[2] S. Hauge, P. Hokstad, H. Langseth and K. Øien. *Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook*. SINTEF, NO-7465 Trondheim, 2006.

[3] T. Lilleheier. *Analysis of common cause failures for complex safety instrumented systems*. Master's thesis, The Norwegian University of Science and Technology, Trondheim, 2008.

[4] Commission Électrotechnique Internationale (CEI). *Norme Internationale CEI 61508, Sécurité fonctionnelle des systèmes électriques/ électroniques/ électrotechniques programmables relatifs à la sécurité*. Genève, 2005.

[5] M. Rausand and A. Høyland. System Reliability Theory; Models, Statistical Methods and Applications (Second Edition). New York: Wiley, 2004.

[6] F. Brissaud et B. Lanternier. « Les Probabilités de Défaillance comme indicateurs de performance des Barrières Techniques de Sécurité – Approche analytique ». *QUALITA 2009 – Qualité et sûreté de fonctionnement*, Besançon, 2009.