Chaînes de Markov multi-phases floues pour l'évaluation de la performance imprécise des Systèmes Instrumentés de Sécurité

Walid MECHRI[1], Christophe SIMON[2], Kamel BEN OTHMAN[1], Mohamed BENREJEB [1]

[1]LARA Tunis, Ecole Nationale d'Ingénieurs de Tunis,
BP37 le Belvédère, 1002 Tunis, Tunisie.
walid.mechri@isim.rnu.tn ,kamel.benothman@enim.rnu.tn ,mohamed.benrejeb@enit.rnu.tn

[2]CRAN – Nancy Université – CNRS UMR 7039,
ESSTIN, 2 rue Jean Lamour, 54509, Vandœuvre, France.
christophe.simon@esstin.uhp-nancy.fr

Résumé— **Dans cet article, nous traitons du problème d'imprécision dans l'évaluation de la performance des systèmes instrumentés de sécurité à l'aide des chaînes de Markov floues multi-phases. Les probabilités élémentaires des chaînes de Markov sont remplacées par des nombres flous permettant aux experts fiabilistes d'exprimer leur incertitude dans l'énoncé des valeurs de probabilités de défaillance et autres paramètres des systèmes. Nous montrons comment l'imprécision sur la valeur d'un unique paramètre, ici le taux de couverture de diagnostic, induit des variations particulièrement significatives sur la qualification du niveau d'intégrité de sécurité d'un SIS. Nous montrons également l'intérêt pour le décideur de connaître l'imprécision sur le paramètre de performance servant à qualifier les SIS.**

Mots-clés— **Système Instrumenté de Sécurité, niveau d'Intégrité de Sécurité, Chaînes de Markov multi-phases, probabilités floues, incertitude, imprécision.**

I. INTRODUCTION

L'application de la norme IEC61508 [1] et des normes filles, notamment la 61511 [2] pour l'industrie de process, a radicalement changé la position des entreprises par rapport au problème de la sécurité. En effet, ces normes imposent une obligation de résultats plutôt qu'une obligation de moyens. Dans ce contexte, un élément majeur développé dans ces normes est l'évaluation quantitative de la performance du système de sécurité mis en œuvre et la qualification de cette performance par des niveaux référencés. Ainsi, lorsque les installations présentent un risque non tolérable, qui ne peut être réduit par des solutions passives ou des conceptions plus fiables, les systèmes instrumentés de sécurité (SIS) sont mis en œuvre pour ramener le risque à un niveau acceptable. Cette performance doit alors être prouvée par des évaluations selon des méthodes référencées comme les arbres de défaillances, les chaînes de Markov, les réseaux de Petri... pour s'indicer aux niveaux d'intégrité de sécurité (SIL) définis dans la norme. Cette évaluation s'apparente à un calcul d'indisponibilité de la fonction de sécurité lors de sa sollicitation [4]. Dans ce cadre, les chaînes de Markov ont été largement utilisées avec les avantages et inconvénients qu'on leur connaît. Dans les études d'indisponibilité des systèmes, les probabilités manipulées sont souvent précises et considérées parfaitement déterminables. Les problèmes réels sont difficilement appréhendés par une connaissance précise des probabilités en jeu [7]. Ce problème de précision dans la connaissance des valeurs des probabilités est connu et traité de diverses manières. La modélisation des probabilités par un intervalle est une forme simple et séduisante de l'imprécision [6]. La modélisation des probabilités par des nombres flous est une forme plus riche de représentation de l'imprécision [8], [9], [10]. Buckley l'a proposée pour l'étude de l'imprécision dans les chaînes de Markov [7], [8], [12].

Dans ce travail, nous proposons d'utiliser ces travaux dans le cadre de l'évaluation des performances des systèmes en modélisant l'imprécision sur la connaissance des taux de défaillance des composants et autres paramètres caractéristiques, notamment le taux de couverture de diagnostic, d'un système instrumenté de sécurité par des nombres flous car les ingénieurs fiabilistes disposent souvent de plus d'information qu'un simple intervalle. La deuxième section de l'article est consacrée à l'évaluation des performances des systèmes instrumentés de sécurité par les chaînes de Markov. La troisième section concerne la modélisation des paramètres imprécis des SIS par des nombres flous. L'objet de la quatrième section sera l'intégration de la modélisation floue des paramètres imprécis dans les chaînes de Markov multi-phases. La dernière section sera consacrée à l'évaluation de la performance d'un système instrumenté de sécurité d'un puits en guise d'application.

II. EVALUATION DE LA PERFORMANCE DES SIS

A. Système Instrumenté de sécurité (SIS)

Un SIS est un système visant à mettre le procédé qu'il surveille en position de repli de sécurité (c'est-à-dire dans un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque ce procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu ...). Un SIS se compose de trois couches :

- Une couche capteur chargée de surveiller la dérive de paramètres (pression, température ...) vers un état dangereux.
- Une couche système de traitement logique chargée de récolter le signal provenant de la partie capteur, de traiter

celui-ci et de commander la partie actionneur associée.
- Une couche actionneur chargée de mettre le procédé dans sa position de sécurité et de l'y maintenir.

S'agissant de fonctions de sécurité, les couches des SIS sont élaborées à partir de composants certifiés pour de telles fonctions. En outre, les SIS ne peuvent assurer d'autres fonctions pouvant compromettre le niveau de sécurité exigé.
La norme IEC 61508 [1] relative à l'évaluation de la performance des systèmes instrumentés de sécurité établit la classification des systèmes étudiés selon 4 niveaux définis dans le tableau 1 à partir du calcul de la probabilité moyenne de défaillance sur demande (PFD_{avg} en faible sollicitation) ou de la probabilité de défaillance par heure (PFH en forte sollicitation).

TABLE I
NIVEAUX D'INTEGRITE DE SECURITE (SIL)

SIL	Faible demande (PFD_{avg})	Demande élevée (PFH)
1	$10^{-2} \leq PFD_{avg} \leq 10^{-1}$	$10^{-6} \leq PFH \leq 10^{-5}$
2	$10^{-3} \leq PFD_{avg} \leq 10^{-2}$	$10^{-7} \leq PFH \leq 10^{-6}$
3	$10^{-4} \leq PFD_{avg} \leq 10^{-3}$	$10^{-8} \leq PFH \leq 10^{-7}$
4	$10^{-5} \leq PFD_{avg} \leq 10^{-4}$	$10^{-9} \leq PFH \leq 10^{-8}$

B. Modélisation du taux de couverture de diagnostic

Le calcul de l'indice de performance se base sur les hypothèses suivantes :
- L'évaluation probabiliste des boucles de sécurité s'applique à des composants ayant des défaillances aléatoires et modélisées par une distribution exponentielle [3].
- Les taux de défaillance sont présumés être constants et indépendants du temps.
- Les pannes sont classées en quatre catégories. Sont distinguées les défaillances sûres des défaillances dangereuses, chacune de ces catégories étant divisée en défaillances détectées *(DD)* et non détectées *(DU)*.

L'hypothèse usuelle de lois exponentielles correspond au modèle Markovien utilisé et à la période utile d'usage des composants. Les SIS étant périodiquement testés, cette hypothèse est tout à fait raisonnable. D'autres formes de distributions conduiraient à l'emploi de modèles plus sophistiqués comme les processus semi-Markoviens, pseudo-Markoviens …
Les tests de diagnostic sont des tests en ligne qui détectent les défaillances aléatoires latentes d'un composant ou d'un module du SIS. Ils sont le plus souvent exécutés dés la mise sous tension, puis périodiquement. Ils sont caractérisés par un taux de couverture D_C, défini comme étant la probabilité qu'une défaillance soit détectée:

$$D_C = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (1)$$

$$\lambda_{DD} = D_C.\lambda_D \text{ et } \lambda_{DU} = (1 - D_C).\lambda_D \quad (2)$$

L'évaluation quantitative de la performance d'un SIS doit être prouvée par des évaluations selon des méthodes référencées comme les arbres de défaillances, les chaînes de Markov, les réseaux de Petri... Il s'agit des méthodes qui permettent de calculer la PFD des SIS à partir des probabilités de défaillances de leurs composants, pour s'indicer aux niveaux d'intégrité de sécurité (SIL) définis dans la norme (Table I). Pour évaluer la performance des SIS, nous nous appuyons sur une chaîne de Markov pour modéliser les états du SIS au cours de sa mission tout en tenant compte des différents types de défaillances, du taux de couverture de diagnostic D_C et du taux de défaillance de cause commune β.

C. Chaine de Markov

La modélisation par chaînes de Markov est une des approches évoquées dans la norme. Cette technique est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants à taux de défaillance constants et réparables (pour la prise en compte des taux de réparation) [3]. Elle permet ainsi de faire une analyse précise et dynamique du système. La loi de transition d'une chaîne de Markov est définie par l'équation suivante :

$$p^{(n)}(S_j) = \sum_i p^{(n-1)}(S_i) a_{ij} \qquad i, j = 1,.....r \quad (3)$$

$$p^{(n)} = p^{(n-1)}.A \quad (4)$$

où $p^{(n)}$ de dimension $(1 \times r)$ est la distribution de probabilités sur les états à l'instant n ; $p^{(n)}(S_j)$ est la mesure de probabilité d'être dans l'état S_j à l'instant n, $j = 1, \ldots, r$.
L'équation (3) permet donc le calcul de la probabilité que le système étudié soit dans l'état S_j à chaque l'instant n à partir de n'importe quel autre état S_i à l'instant $(n-1)$ selon une probabilité de transition a_{ij} de S_i à S_j définie dans la matrice de transition $A = (a_{ij})$ de dimension $(r \times r)$. Cette matrice est caractérisée par le fait que la somme de chacune de ses lignes est égale à un et chaque coefficient $a_{ij} \geq 0$.
Finalement, en utilisant l'équation (4), nous obtenons la formule de Chapman-Kolmogorov :

$$p^{(n)} = p^{(0)}.A^n \quad (5)$$

où $p^{(0)}$ de dimension $(1 \times r)$ est le vecteur de probabilités à l'instant initial.
Les SIS ont toutefois la particularité d'être périodiquement testés. L'état du SIS est donc connu à ces instants et les probabilités des différents états sont également connues. Nous sommes donc en présence d'une chaîne de Markov multi-phases [5].
Il existe donc une matrice de passage M permettant l'affectation de la distribution de probabilités d'être dans les différents états S_j aux instants d'inspection t_1 vers la distribution de probabilités aux instants post-inspection t_2.

$$p^{(t_2)} = p^{(t_1)}.M \quad (6)$$

Les SIS étant composés de plusieurs sous-systèmes et composants, il est possible que plusieurs matrices de passage M soient utilisées au cours du temps selon la stratégie de test employée. Les inspections sont normalement répétées à

intervalles de temps constants. Grâce aux précédentes équations (eq. 3, 4), nous pouvons déterminer la probabilité de défaillance à la demande du SIS modélisé par une chaîne de Markov multi-phases et calculer la performance moyenne par intégration dans le temps.

III. EVALUATION DE PERFORMANCE IMPRECISE

Lorsque les systèmes instrumentés de sécurité sont faiblement sollicités, le retour d'expérience est faible et les probabilités manipulées peuvent paraître peu crédibles, peu précises. Le problème de précision sur les taux de défaillance ou de défaillance de cause commune existe également lorsque l'on travaille avec de nouveaux composants. Dans ce cas, les experts ou les concepteurs fournissent des estimations imprécises des taux caractéristiques des composants. Il faut également tenir compte du fait que les conditions d'exploitation (environnement) des SIS sont souvent différentes des conditions de la base de données. L'impact sur la probabilité de défaillance des composants est mal connu et est souvent négligé. D'autre paramètres spécifiques aux SIS sont également concernés par le problème de connaissance des experts fiabilistes. Par exemple, le taux de couverture de diagnostic est très souvent mal déterminé. Sa valeur résulte dans la plupart des cas d'un travail d'expertise, pouvant être guidée par l'expérience ou par estimation, d'où cette imprécision.

L'imprécision sur un paramètre peut être représentée de plusieurs manières. Une vision probabiliste appuyée par le principe d'insuffisance de Laplace conduit à la modélisation d'un paramètre imprécis par une distribution uniforme sur l'ensemble des valeurs qu'il peut prendre. Une simulation de type Monte-Carlo permet alors de combiner l'ensemble des valeurs des paramètres imprécis au travers du modèle choisi, ici une chaîne de Markov multi-phases. L'imprécision peut être représentée tout aussi simplement en ne faisant pas d'hypothèse sur la distribution mais en utilisant des intervalles. Il n'y a plus de simulation de Monte-Carlo mais des calculs par la théorie des intervalles de Moore [13]. Les experts fiabilistes peuvent dans certains cas fournir plus d'information qu'un simple intervalle. Ils peuvent par exemple fournir une série d'intervalles emboîtés liées au niveau de confiance α sur la connaissance qu'ils formalisent. Il s'agit en fait d'un nombre flou au sens de Zadeh [11]. L'expert fiabiliste peut éventuellement préciser le nombre flou directement à partir des bornes minimale, maximale et la valeur modale. Dans ce cas, les limites extérieures des intervalles emboités indicés peuvent être reliées par une interpolation linéaire pour former un nombre flou triangulaire. Il s'agit d'une extrapolation de connaissance minime si on doit combiner avec finesse des nombres flous à des niveaux de confiance différents. Le nombre flou triangulaire joue le rôle de la distribution uniforme pour les probabilités puisqu'il encode une famille de probabilités (probabilités imprécises) [14].

A. Nombre flou

Un sous ensemble flou A sur un référentiel Ω est caractérisé par une fonction d'appartenance μ_A qui associe à chaque x de Ω un nombre réel dans l'intervalle $[0,1]$:

$$\mu_A : \Omega \rightarrow [0,1] \tag{7}$$

Un nombre flou est un sous-ensemble satisfaisant les conditions suivantes [11]:

- $\mu(x)$ est continue par morceaux
- $\mu(x)$ est convexe
- $\mu(x)$ est normale (il existe au moins une valeur x_0 telle que $\mu(x_0 = 1)$.

Nous pouvons caractériser un nombre flou triangulaire par un intervalle de confiance à un certain niveau α. En effet, si nous considérons un nombre flou $\tilde{A}$ de fonction d'appartenance $\mu_{\tilde{A}}(x)$, on obtient plusieurs intervalles emboîtés en utilisant la méthode des $\alpha-$coupes. Ainsi, un intervalle créé par la coupe de niveau α présente un indice de confiance $(1-\alpha)$.

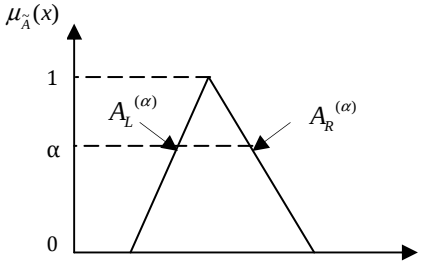

Fig. 1. α-coupe d'un nombre flou

$A_L^{(\alpha)}$ et $A_R^{(\alpha)}$ représenteront respectivement les limites gauche et droite de la fonction d'appartenance à chaque α−coupe. Comme le montre la figure 1, on peut représenter un nombre flou, en utilisant l'expression suivante :

$$\tilde{A} \rightarrow [A_L^{(\alpha)}, A_R^{(\alpha)}], \_ 0 \le \alpha \le 1 \tag{8}$$

B. Chaînes de Markov floue

Dans la matrice de transition $A = (a_{ij})$ tous les a_{ij} doivent être connues exactement. Ces valeurs sont généralement estimées ou fournies par des experts. Ainsi, nous supposons qu'une partie des a_{ij} est imprécise et on modélise cette incertitude en utilisant des nombres flous. Ainsi, à chaque a_{ij} est associée une valeur floue $\tilde{a}_{ij}$ et la matrice de transition floue, $\tilde{A} = (\tilde{a}_{ij})$, avec $\tilde{a}_{ij}$ la probabilité de transition floue de l'état S_i vers l'état S_j.

On définit la restriction suivante sur les $\tilde{a}_{ij}$: il existe une valeur $a_{ij} \in \tilde{a}_{ij}^{(1)}$ de telle sorte que $\tilde{A} = (\tilde{a}_{ij})$ soit la matrice de transition de la chaîne de Markov. Cette matrice est caractérisée par le fait que la somme de chacune de ses lignes est égale à un. Cette restriction sera la base de l'approche proposée dans cet article.

Pour calculer $\tilde{A}^n = (\tilde{a}_{ij}^{(n)})$, on doit définir la multiplication restreinte des matrices floues. Buckley [8,14] rappelle la contrainte sur la matrice de transition décrite par l'équation suivante :

$$S = \{\ x = (x_1, x_2, ..., x_r)\ \big|\ x_i \ge 0, \sum_{i=1}^{r} x_i = 1\ \} \tag{9}$$

avec x_i la $i^{\text{ème}}$ entité du vecteur x.

Ainsi, on définit le domaine des α-coupes $Dom[\alpha]$:

$$Dom_i[\alpha] = (\prod_{j=1}^{r} \tilde{a}_{ij}[\alpha]) \cap S, \quad (10)$$

Dans l'équation (14) nous prenons d'abord le produit des *r* intervalles fermés produisant un "rectangle" dans l'espace de dimension *r* qui est alors intersecté avec l'ensemble S .

$$Dom[\alpha] = \prod_{i=1}^{r} Dom_i[\alpha], \quad 0 \le \alpha \le 1, \quad (11)$$

On considère maintenant $f_{ij}^{(n)}$ une fonction de $a = (a_{11}, \cdots, a_{rr}) \in Dom[\alpha]$, les lignes de $f_{ij}^{(n)}$ sur $Dom[\alpha]$ peuvent être formulées comme suit :

Pour $0 \le \alpha \le 1; \quad 1 \le i \le r$

$$\tilde{a}_{ij}^{(n),(\alpha)} = f_{ij}^{(n)}(Dom[\alpha]), \quad (12)$$

Pour calculer tout les $\tilde{a}_{ij}^{(n),(\alpha)}$, les bornes des intervalles doivent être déterminées. Ainsi, nous devons résoudre les équations suivantes [7]:

$$a_{ijL}^{(n),(\alpha)} = \min\{f_{ij}^{(n)}(a) \mid a \in Dom[\alpha]\}, \quad (13)$$

$$a_{ijR}^{(n),(\alpha)} = \max\{f_{ij}^{(n)}(a) \mid a \in Dom[\alpha]\}, \quad (14)$$

avec $\tilde{a}_{ij}^{(n),(\alpha)} = [a_{ijL}^{(n),(\alpha)}, a_{ijR}^{(n),(\alpha)}]$, pour tout α.

En général pour estimer les solutions de ces équations, il faut utiliser un algorithme d'optimisation. Il s'agit donc d'utiliser la formulation optimale de la chaîne de Markov dans les équations (5), (13) et (14). On calcul $\tilde{p}^{(n),(\alpha)}$, la probabilité floue d'être dans les différents états S_j à l'instant n .

C. Paramètres imprécis

La valeur du taux de couverture D_C est souvent difficile à fournir et peut être représenté par un nombre flou triangulaire $\tilde{D}_C$ (cf. équation 8). Le taux de couverture de diagnostic flou $\tilde{D}_C$ peut alors être décrit par l'ensemble de ses α-coupes $[\tilde{D}_C^{(\alpha)}]$tel que $[\tilde{D}_C^{(\alpha_2)}] \subseteq [\tilde{D}_C^{(\alpha_1)}]$ si $\alpha_1 \le \alpha_2$.

$[\tilde{D}_C^{(\alpha)}]$représente l'intervalle des valeurs pouvant être prise par $\tilde{D}_C$ au niveau de confiance $(1-\alpha)$. Ainsi, $[\tilde{D}_C^{(\alpha)}]$est borné par deux valeurs $[\tilde{D}_{CL}^{(\alpha)}, \tilde{D}_{CR}^{(\alpha)}]$. De ce fait, les différents taux de défaillance dangereuse deviennent :

$$\tilde{\lambda}_{DD} = \tilde{D}_C.\lambda_D \Rightarrow [\lambda_{DDL}^{(\alpha)}, \lambda_{DDR}^{(\alpha)}] = [D_{CL}^{(\alpha)}.\lambda_D, D_{CR}^{(\alpha)}.\lambda_D] \quad (15)$$

$$\tilde{\lambda}_{DU} = (1-\tilde{D}_C).\lambda_D \Rightarrow [\lambda_{DUL}^{(\alpha)}, \lambda_{DUR}^{(\alpha)}] = [(1-D_{CR}^{(\alpha)}).\lambda_D, (1-D_{CL}^{(\alpha)}).\lambda_D] \quad (16)$$

avec λ_D le taux de défaillance dangereuse du $i^{ème}$ composant, sera représenté par un nombre flou singulier.

Les paramètres $\tilde{\lambda}_{DD}$ et $\tilde{\lambda}_{DU}$ intègrent alors directement la matrice de transition caractéristique du système étudié. Nous sommes en présence d'une chaîne de Markov multi-phases à nombres flous, ce qui nécessite la réécriture des équations 3 et 6 avec des nombres flous et adapter leur traitement. Nous sommes donc en présence d'une chaîne de Markov floues multi-phases. Les probabilités supérieure et inférieure des différents états sont obtenues grâces aux équations suivantes :

$$p_L^{(t_2),(\alpha)} = p_L^{(t_1),(\alpha)}.M \quad (17)$$

$$p_R^{(t_2),(\alpha)} = p_R^{(t_1),(\alpha)}.M \quad (18)$$

Il s'agit alors d'utiliser (17) et (18) pour calculer la performance moyenne par intégration dans le temps et qualifier le SIS.

Rappelons simplement que dans la norme CEI 61508 [1], les différentes configurations des systèmes instrumentés de sécurité étudiés sont composées de canaux. Chaque canal peut avoir plusieurs types de configuration architecturale (architecture 1oo1, 1oo2, …) et, chaque canal peut avoir, des défaillances détectables par les tests de diagnostic, avec un taux λ_{DD} et des défaillances non détectées avec un taux λ_{DU} .

D. Architecture 1oo2

Cette architecture proposée à la figure 2 se compose de deux canaux identiques fonctionnant en redondance chaude. Il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande.

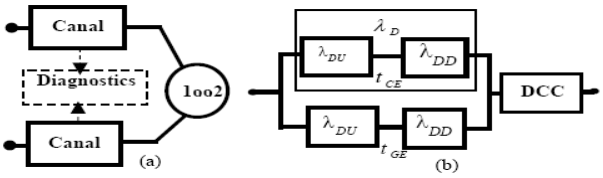

Fig. 2. Blocs-diagramme physique (a) et de fiabilité (b) de l'architecture 1oo2

Le bloc-diagramme de fiabilité (figure 2b) montre que le système 1oo2 possède deux modes de défaillance mutuellement exclusifs (dangereux détecté DD et dangereux non détecté DU).

Le sous-système étant testé à intervalle régulier T_1, son comportement au cours d'une mission de durée donnée est correctement décrit par un modèle markovien multi-phases, tenant compte à la fois du comportement propre sans défaillance de causes communes (DCC) de l'architecture 1oo2 (états 1 à 6) et du comportement avec DCC (états 7 et 8) est représentée à la figure 3.

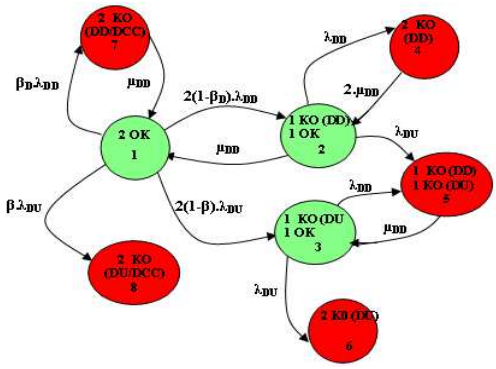

Fig. 3. Modèle markovien multi-phases de l'architecture 1oo2

Dans ce modèle, β et β_D représentent respectivement la proportion de défaillances de causes communes détectées et non détectées liée au taux de couverture de diagnostic.
Les liens entre les probabilités d'occupation des états en fin de phase (i-1) et en début de phase i sont définis comme suit [4] :

$$P_1(d_i) = P_1(f_{i-1}) \; ; \; P_2(d_i) = P_2(f_{i-1}) + P_3(f_{i-1}) \; ; \quad P_4(d_i) = P_4(f_{i-1}) + P_5(f_{i-1}) \tag{19}$$

$$P_7(d_i) = P_6(f_{i-1}) + P_7(f_{i-1}) + P_8(f_{i-1}) \; ; \quad P_3(d_i) = P_5(d_i) = P_6(d_i) = P_8(d_i) = 0 \tag{20}$$

A partir des équations 19 et 20, on détermine la matrice de passage M . La probabilité de défaillance sur demande de l'architecture 1oo2 est calculée en utilisant les équations 17 et 18.
En considérant un taux de couverture D_C imprécis, nous pouvons mesurer l'influence de cette imprécision sur la performance de l'architecture 1oo2. Le paramètre D_C est décrit par un nombre flou caractérisé par ces trois paramètres caractéristiques $< m_i, a_i, b_i >$ (fournis par les experts). Considérons les données numériques suivantes : T_1=1460h, λ_D= 4,66.10^{-5} h^{-1}; D_C = <0.2, 0.1, 0.4> ; μ_{DD}= 1/MTTR ; MTTR=8h.
L'évolution de la probabilité de défaillance au cours du temps $\tilde{P}(t)$ de l'architecture 1oo2 ainsi que sa valeur moyenne, $\tilde{P}_{avg}$ représentée en pointillés, pour (α=0 et α=1) sont fournies à la figure 4.

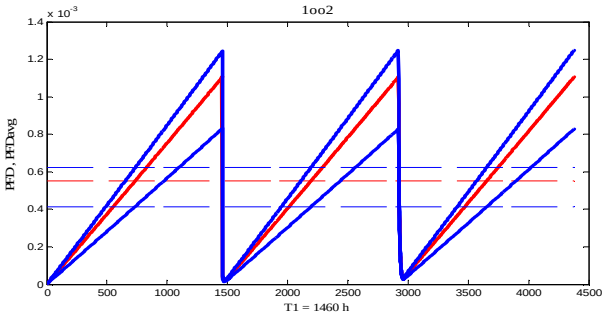

Fig. 4. Variation de la $\tilde{P}(t)$ et $\tilde{P}_{avg}(t)$ de l'architecture 1oo2, pour α=0 et α=1

La $\tilde{P}(t)$ du sous-système est encadrée par des bornes supérieure et inférieure liées à l'intervalle défini par l' α-coupe de niveau 0. La propriété de monotonie dans l'inclusion de la fonction disponibilité associée à ce système permet de garantir que les intervalles des α-coupes de niveau supérieur à 0 sont strictement inclus dans le support donné à la figure 4.

VI. Application

Un HIPS *(High Integrity Protection System*) est un système instrumenté de sécurité à haut niveau d'intégrité de sécurité. Il comporte 3 couches (capteurs, unités logiques, actionneurs) formées par des architectures selon une redondance choisie en fonction du niveau de réduction de risque que le concepteur souhaite amener. Le système proposé à la figure 5 a été proposé dans [5] et sera utilisé comme exemple.

Le SIS étudié, est destiné à protéger un circuit aval d'une surpression émanant d'un puits W1. Son fonctionnement est le suivant : quand la valeur de la pression dans la canalisation dépasse un certain seuil, elle est détectée par les trois capteurs de pression PTi qui envoient l'information à l'unité logique qui contrôle son caractère majoritaire 2/3 (2oo3).

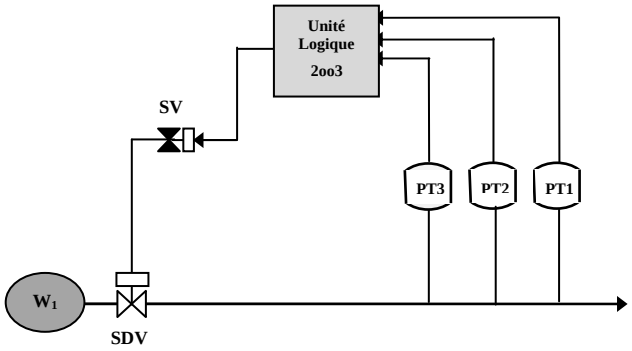

Fig. 5. Le SIS à étudier

Si au moins deux des trois signaux reçus des capteurs confirme la présence d'une surpression dans la canalisation, l'unité logique commande l'ouverture de la vanne solénoïde SV, ce qui à pour conséquence de couper l'alimentation hydraulique qui maintenait ouverte la vanne SDV. Celles-ci se ferment alors et suppriment le risque de surpression dans le circuit aval. L'événement redouté auquel on s'intéresse est justement l'inhibition du SIS, qui se traduit par la non fermeture des deux vannes de secours. Cet exemple est utilisé ici comme un cas-test destiné à juger de l'applicabilité des chaînes de Markov floues multi-phases proposées.
Les paramètres caractéristiques des composants du SIS étudié sont des nombres flous du type $L-R$. On propose d'étudier l'impact de l'imprécision de taux de couverture sur la performance du SIS. On choisit le taux de défaillance dangereuse $\lambda_{D,i}$ comme étant un nombre flou singulier. Le taux de couverture de chaque ensemble de composants est décrit par un triplet de paramètres $< m_i, a_i, b_i >$, fournis par les experts. Les données numériques sont regroupées dans le tableau 2, nous donnons les valeurs de ces 3 paramètres pour chaque sous systèmes du SIS, ainsi que les autres paramètres caractéristiques.

TABLE II
DONNEES NUMERIQUES

Composants du SIS	λ_D (h^{-1})	D_C	β (%) CCF	MTTR (h)	Ti (h)
PT1	7.00E-7	<0.5, 0.3, 0.6>	5	10	T_1 = 730
SDV	4.66E-6	<0.2, 0.1, 0.4>	10	8	T_2 = 1460
SV	4.66E-6	<0.2, 0.1, 0.4>	10	8	T_2 = 1460
LS	2.25E-6	<0.8, 0.7, 0.9>	-	10	T_3 = 2190

La probabilité moyenne de défaillance à la demande de la fonction de sécurité est calculée par la combinaison de la probabilité moyenne de défaillance de tous les sous systèmes assurant ensemble la fonction de sécurité. Elle est exprimée par les formules suivantes [1] sous l'hypothèse d'évènement rares:

$$\tilde{PFD}_{HIPS} = \tilde{P}_{cap} + \tilde{P}_{UL} + \tilde{P}_{ac} \quad (21)$$

$$\tilde{PFD}_{HIPS} = \tilde{P}_{2oo3} + \tilde{P}_{1oo1} + \tilde{P}_{1oo2} \quad (22)$$

La figure 6 montre la courbe en fonction du temps de l'indisponibilité instantanée $\tilde{PFD}$ du SIS étudié pour α=0 et α=1, ainsi que sa valeur moyenne $\tilde{PFD}_{avg}$, lorsque tous les composants du système sont testés simultanément. On détermine, pour chaque α-coupe, les bornes supérieure et inférieure de la probabilité de défaillance moyenne PFD_{avg} du SIS.

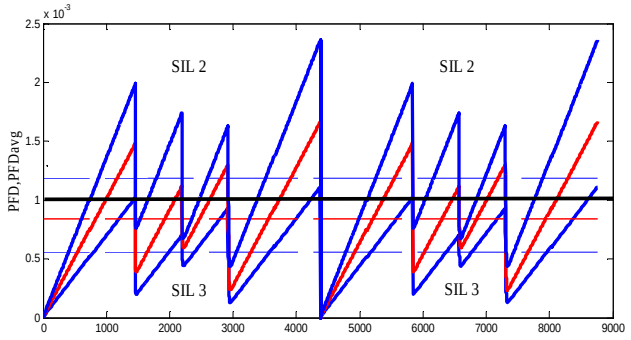

Fig. 6. Variation de la $\tilde{PFD}$ et $\tilde{PFD}_{avg}$ du SIS, pour α=0 et α=1.

En utilisant la méthode des chaînes de Markov floues multi-phases proposée dans cet article et celle des α-coupes, la probabilité de défaillance à la demande du SIS est déterminée à partir des valeurs des paramètres caractéristiques de ses composants.

La figure 7 montre le nombre flou de type triangulaire représentant l'imprécision sur la probabilité moyenne de défaillance à la demande du système instrumenté de sécurité induite par l'imprécision des taux de couverture de diagnostic D_C modélisée par des nombres flous triangulaires.

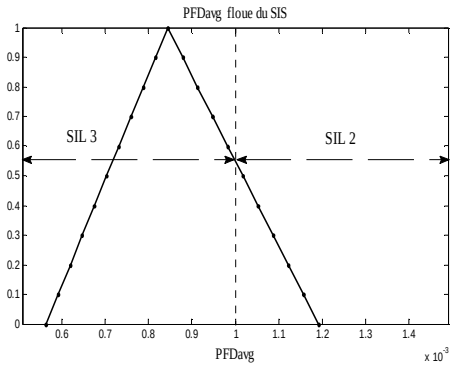

Fig. 7. $\tilde{PFD}_{avg}$ floue du SIS étudié

Le support du nombre flou caractéristique de la probabilité moyenne de défaillance à la demande varie de 0.564×10^{-3} jusqu'à 1.192×10^{-3}, ce qui donne pour le SIS étudié un niveau de SIL3 ($PFD_{avg} \in [10^{-4},10^{-3}]$) ou un niveau SIL2 ($PFD_{avg,} \in [10^{-3},10^{-2}]$) sachant que $\tilde{PFD}_{avg}$ est un ensemble disjonctif.

Nous constatons très rapidement que l'imprécision sur le taux de couverture de diagnostic amène à une variation du niveau de SIL du SIS alors qu'une valeur précise mais incertaine nous aurait fournie un niveau unique de SIL 3 correspond à $\tilde{PFD}^{(\alpha=1)}$. L'imprécision sur la $\tilde{PFD}_{avg}$ induit donc une incertitude sur la qualification de performance du SIS.

V. Conclusion

Dans cet article, nous avons proposé une approche basée sur l'utilisation des nombres flous au sein des chaines de Markov multi-phases pour évaluer la performance imprécise des systèmes instrumentés de sécurité. Le choix de nombres flous triangulaire correspond bien à la formulation linguistique de l'imprécision par les experts mais peut être largement étendu à toutes autres formes. En outre, le taux de couverture de diagnostic est généralement mal connu et une valeur imprécise est plus certaine (intervalle, nombre flou…). L'approche permet d'estimer l'impact de l'imprécision de D_C sur l'imprécision de la performance du système. L'arithmétique floue contrainte proposée par Buckley permet ce calcul de façon efficace en garantissant le plus petit support final. Nous avons ainsi montré que l'imprécision induite par une connaissance imparfaite pouvait entraîner des variations de qualification de performance d'un SIS et placer le concepteur dans une situation de risque. Compte tenu de ce constat, il semble crucial d'étudier les effets des imprécisions affectant l'ensemble des paramètres et, les chaînes de Markov floues multi-phases sont des modèles pertinents dans ce contexte.

Références

[1] IEC61508. *Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems*. International Electrotechnical Commission (IEC), 1998.

[2] IEC61511. *Functional safety: Safety Instrumented Systems for the process industry sector*. International Electrotechnical Commission (IEC), 2000.

[3] Lanternier B., Dranguet J.-M, *Maintenance optimization of sensors for certification in compliance with the IEC 61511 standard*, European Safety and Reliability Conference ESREL07, Stavanger, Norvège, 25-27 Juin 2007.

[4] Dutuit Y., Innal F., Rauzy A., Signoret, J.-P., Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. *Reliability Engineering and System Safety*, vol.93, pp.1867–1876, 2008

[5] Signoret J.-P., Methodology SIL evaluations related to HIPS – Total Draft Memo, April 27- 2005.

[6] Kozine I., Utkin L., Interval valued Finite Markov Chains, *Reliable computing*, vol. 8, pp. 97- 113, 2002.

[7] Buckley JJ., Eslami E., Fuzzy Markov chains: Uncertainty Probabilities, *MathWare and soft computing*, vol. 9, pp 33-41, 2002.

[8] Huang J-J., Tzeng G-H., A Constrained Fuzzy Arithmetic Method for the Fuzzy Analytic Network Process, Fourth International Conference on Fuzzy Systems and Knowledge Discovery FSKD, Chine, 2007.

[9] Kruse R., Buck-Emden R., Cordes R., Processor power considerations an application of fuzzy Markov chains. *Journal of intelligent and Fuzzy Systems*, vol. 6, pp. 223-235, 1998.

[10] Sallak M, Simon Ch ., Aubry J-F., A Fuzzy Probabilistic Approach for Determining Safety Integrity Level, *IEEE Transactions on Fuzzy Systems*, vol. 16, n°1, pp. 239-248, 2008.

[11] Zadeh L,. Fuzzy sets. *Information and Control*, pp. 338–353, 1965.

[12] Buckley JJ,. *Fuzzy Probabilities: New approach and applications*, Spinger 2005.

[13] Moore R.E,. *Methods and applications of interval analysis. Studies in Applied Mathematics*, SIAM, Philadelphia, 1979.

[14] Baudri C,. Représentation et propagation de connaissances imprécises et incertaines : Application des risques liés aux sites et aux sols pollués. Thèse de Doctorat de l'université de Toulouse III, PAUL SABATIER, 19 Octobre 2005.