

CHAINES DE MARKOV MULTIPHASES A INTERVALLES POUR L'EVALUATION DE PERFORMANCE IMPRECISE DES SIS

MECHRI Walid.¹, SIMON Christophe.², BEN OTHMAN Kamel.¹, AUBRY J-Francois.², BENREJEB Mohamed.¹

1 LARA Tunis, Ecole National d'Ingénieurs de Tunis, BP37 le Belvédère, 1002 Tunis, Tunisie

2 CRAN Nancy Université CNRS, 2 Rue Jean Lamour, Vandoeuvre les Nancy, France

Résumé :

Dans cet article, nous traitons le problème d'imprécision dans l'évaluation de la performance des systèmes instrumentés de sécurité à l'aide de chaîne de Markov multi-phases à intervalles. Nous montrons comment l'imprécision sur la valeur d'un unique paramètre induit des variations particulièrement significatives sur la qualification du niveau d'intégrité de sécurité d'un SIS.

Abstract:

In this article, we deal with the problem of imprecision in performance evaluation of the safety instrumented systems by the use of multi-phase intervals Markov chains. We show how the imprecision on the value of a single parameter causes significant variations on the safety integrity level qualification of a given safety instrumented system.

Mots clés : Chaînes de Markov multi-phases, intervalles de probabilités, Systèmes Instrumentés de Sécurité, chaînes de Markov à Intervalles.

Key words: multi-phase Markov chains, probabilities intervals, Safety Instrumented Systems, intervals Markov chains.

1. Introduction

L'application de la norme IEC61508 et des normes filles, notamment la 61511 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 [Dut 08]. Dans ce cadre, les chaînes de Markov ont été largement utilisées avec les avantages et inconvénients qu'on leur connaît.

Si 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 [Utk 07]. Ce problème de précision dans la connaissance des valeurs de probabilités est connu et appréhendé de diverses manières. La modélisation des probabilités par un intervalle est une forme simple et séduisante de l'imprécision. Kozine l'a proposée pour l'étude de l'imprécision dans les chaînes de Markov [Koz 02].

Dans ce travail, nous proposons d'utiliser ces travaux dans le cadre de l'évaluation de la performance des SIS en modélisant l'imprécision sur la connaissance des taux de défaillance des composants et autres

paramètres caractéristique d'un SIS par des intervalles de probabilités. La première section de cet article est consacrée aux paramètres imprécis des SIS. La seconde section concerne la modélisation de l'indisponibilité des SIS par les chaînes de Markov multi-phases. En particulier, deux architectures types sont étudiées lorsque le taux de couverture de diagnostic est imprécis. La dernière section de cet article est consacrée à l'évaluation de la performance d'un système instrumenté de sécurité à haut niveau d'intégrité dédié à une application de sécurité process.

2. Paramètres imprécis des SIS

La norme CEI 61508 [CEI 98] relative à l'évaluation de 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 ($PF_{D_{avg}}$ en faible sollicitation) ou de la probabilité de défaillance par heure (PFH en forte sollicitation)

Sollicitation	Demande faible	Demande élevée
SIL	$PF_{D_{avg}}$	Défaillances/heure
4	$10^{-5} \leq PF_{D_{avg}} \leq 10^{-4}$	$10^{-9} \leq PFH \leq 10^{-8}$
3	$10^{-4} \leq PF_{D_{avg}} \leq 10^{-3}$	$10^{-8} \leq PFH \leq 10^{-7}$
2	$10^{-3} \leq PF_{D_{avg}} \leq 10^{-2}$	$10^{-7} \leq PFH \leq 10^{-6}$
1	$10^{-2} \leq PF_{D_{avg}} \leq 10^{-1}$	$10^{-6} \leq PFH \leq 10^{-5}$

Tableau 1. Définition des niveaux de SIL

Le calcul de l'indice de performance se base sur les hypothèses suivantes :

1. L'évaluation probabiliste des boucles de sécurité s'applique à des composants ayant des défaillances aléatoires et modélisés par une distribution exponentielle [Lan 07]. Les taux de défaillance sont présumés être constants et indépendants du temps.
2. Les pannes sont classées en quatre catégories. Sont distinguées les défaillances sûres des défaillances dangereuses, chacune de ces catégories étant divisée en défaillances détectées et non détectées.
3. Le taux de couverture (DC) est défini comme étant la probabilité qu'une panne soit détectée :

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

Lorsque les systèmes instrumentés de sécurité sont faiblement sollicités, le retour d'expérience est faible et les probabilités en jeu sont souvent imprécises. Le problème de précision sur les taux de défaillance ou de réparation existe également lorsque l'on travaille avec de nouveaux composants. Dans ce dernier cas, les experts ou les concepteurs fournissent des estimations des taux caractéristiques des composants. L'imprécision existe également avec des SIS fortement sollicités où le retour d'expérience est beaucoup plus important. Les bases de données fournissent des données statistiques descriptives (min, max, moyenne) et la distribution réelle reste inaccessible. Dans tous les cas, il faut tenir compte du fait que les conditions d'exploitation (environnement) des SIS sont souvent différentes des conditions de la base de données. En ce qui concerne le taux de couverture de diagnostic, il résulte dans la plupart des cas d'un travail d'expertise, pouvant être guidée par l'expérience ou par estimation, d'où l'imprécision. C'est également le cas pour le taux de défaillance de cause commune.

Pour tenir compte de l'imprécision, la valeur du taux de couverture DC peut être représentée par un intervalle : $DC \in [DC_{min}, DC_{max}]$.

De ce fait, les différents taux de défaillance dangereuse deviennent :

$$\lambda_{DDmin} = DC_{min} \cdot \lambda_D \quad \text{et} \quad \lambda_{DDmax} = DC_{max} \cdot \lambda_D$$

$$\lambda_{DUmin} = (1 - DC_{max}) \lambda_D \quad \text{et} \quad \lambda_{DUmax} = (1 - DC_{min}) \lambda_D$$

$$D'o\grave{u} \lambda_{DD} \in [\lambda_{DDmin}, \lambda_{DDmax}] \quad \text{et} \quad \lambda_{DU} \in [\lambda_{DUmin}, \lambda_{DUmax}]$$

L'objectif \u00e9tant de d\u00e9terminer l'indice de performance du SIS, pour d\u00e9terminer son niveau d'int\u00e9grit\u00e9, nous ne consid\u00e9rons que les taux de d\u00e9faillances dangereuses λ_D des modules composant les architectures \u00e9tudi\u00e9es. Ce taux est le r\u00e9sultat des d\u00e9faillances dangereuses ; d\u00e9tect\u00e9es par les tests de diagnostic ayant un taux λ_{DD} et non d\u00e9tect\u00e9es ayant un taux λ_{DU} .

3. Cha\u00eene de Markov multi-phases \u00e0 Intervalles

L'approche markovienne apporte une bonne formalisation des \u00e9tats que peuvent prendre les SIS en fonction des \u00e9v\u00e9nements rencontr\u00e9s (d\u00e9faillance, test, maintenance ...) et des param\u00e8tres \u00e9tudi\u00e9s (taux de d\u00e9faillance, d\u00e9faillance de cause commune ...).

3.1. Cha\u00eene de Markov \u00e0 Intervalles

La loi de transition d'une cha\u00eene de Markov classique est d\u00e9finie par : $b_j(k) = \sum_{i=1}^n b_i(k-1) \alpha_{ij}$, avec $b_j(k)$

la probabilit\u00e9 \u00e0 l'instant k de l'\u00e9tat $s_j, j=1, \dots, n$ et α_{ij} la probabilit\u00e9 de transition de l'\u00e9tat s_i vers l'\u00e9tat s_j . α_{ij} et $b_i(0)$ sont connus pour $i, j=1, \dots, n$.

Supposons maintenant que α_{ij} et $b_i(0)$ ne soient pas connus avec pr\u00e9cision mais appartiennent avec certitude \u00e0 des intervalles. C'est-\u00e0-dire $\underline{b}_i(0) \leq b_i(0) \leq \bar{b}_i(0)$ et $\underline{\alpha}_{ij} \leq \alpha_{ij} \leq \bar{\alpha}_{ij}$ pour $i, j=1, \dots, n$ o\u00f9 \underline{b}_i (resp. \bar{b}_i) est la borne inf\u00e9rieure de b_i (resp. sup\u00e9rieure) et $\underline{\alpha}_{ij}$ (resp. $\bar{\alpha}_{ij}$) est la borne inf\u00e9rieure de α_{ij} (resp. sup\u00e9rieure).

Les probabilit\u00e9s sup\u00e9rieure et inf\u00e9rieure des diff\u00e9rents \u00e9tats sont obtenues comme solutions du probl\u00e8me suivant [Koz 02]:

$$\bar{b}_j(k) = \sup_{b_i} \sum_{i=1}^n b_i(k-1) \bar{\alpha}_{ij}, \quad j=1, \dots, n \quad (2)$$

$$\underline{b}_j(k) = \inf_{b_i} \sum_{i=1}^n b_i(k-1) \underline{\alpha}_{ij}, \quad j=1, \dots, n \quad (3)$$

Il s'agit donc d'utiliser les \u00e9quations 2 et 3 pour \u00e9valuer les performances des SIS \u00e9tudi\u00e9s. Rappelons simplement que dans la norme CEI 61508 [CEI 98], les diff\u00e9rentes configurations des syst\u00e8mes instrument\u00e9s de s\u00e9curit\u00e9 \u00e9tudi\u00e9s sont compos\u00e9es de canaux. Chaque canal peut avoir plusieurs types de configuration architecturale (architecture 1oo1 : un parmi un, 1oo2 : au moins un parmi deux, ...). Un canal peut avoir, des d\u00e9faillances d\u00e9tectables par les tests de diagnostic, avec un taux λ_{DD} et des d\u00e9faillances non d\u00e9tect\u00e9es avec un taux λ_{DU} .

3.2. Architecture 1oo1

Cette architecture de base est compos\u00e9e d'un seul canal (figure 1). En cons\u00e9quence, toute d\u00e9faillance dangereuse induit la perte de la fonction de s\u00e9curit\u00e9 [CEI 98].

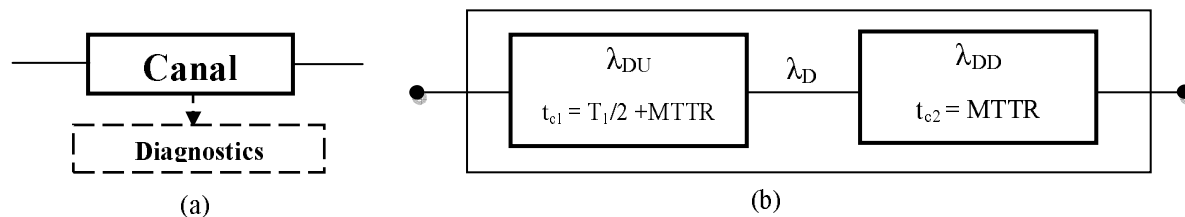


Figure 1 : Blocs-diagrammes physique (a) et de fiabilit\u00e9 (b) de l'architecture 1oo1

Le bloc-diagramme de fiabilité (figure 1b) montre que le système 1oo1 possède deux modes de défaillance mutuellement exclusifs (dangereux détecté DD et dangereux non détecté DU). Le système étant périodiquement 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, comme l'indique la figure 2 [Inn 06].

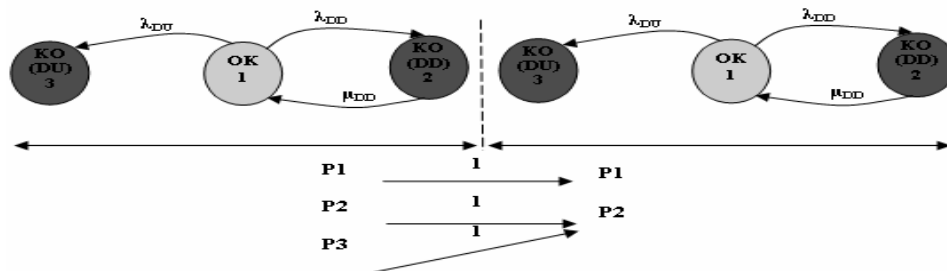


Figure 2 : Modèle markovien multi-phases relatif à l'architecture 1oo1

Dans ce modèle, μ_{DD} représente le taux de réparation spécifiques aux défaillances dangereuses détectées par le test de diagnostic.

Pour exploiter ce modèle, il faut veiller à ce que les valeurs des probabilités d'occupation des états au début de la phase i (d_i) soient déterminées à partir de celles obtenues au terme de la période précédente (f_{i-1}) [Inn 06]. Sur l'architecture étudiée, l'ensemble de relations inter-phases est déterminé:

$$P_1(d_i) = P_1(f_{i-1}); P_2(d_i) = P_2(f_{i-1}) + P_3(f_{i-1}); P_3(d_i) = 0. \quad (4)$$

Etude quantitative :

Si nous considérons les données numériques suivantes :

- MTTR = 8h ; $T_1=4380h$; $\lambda_D=2,5 \cdot 10^{-5} h^{-1}$; $\mu_{DD}=\text{MTTR}$;
- $DC \in [0.4, 0.6]$

Les probabilités de défaillances dangereuses sur demande $PF_{D_{min}}$ et $PF_{D_{max}}$ en fonction du temps, correspondant respectivement aux taux de couverture DC_{min} et DC_{max} des tests de diagnostic sont fournies à la figure 3, à partir des équations 2, 3 et 4.

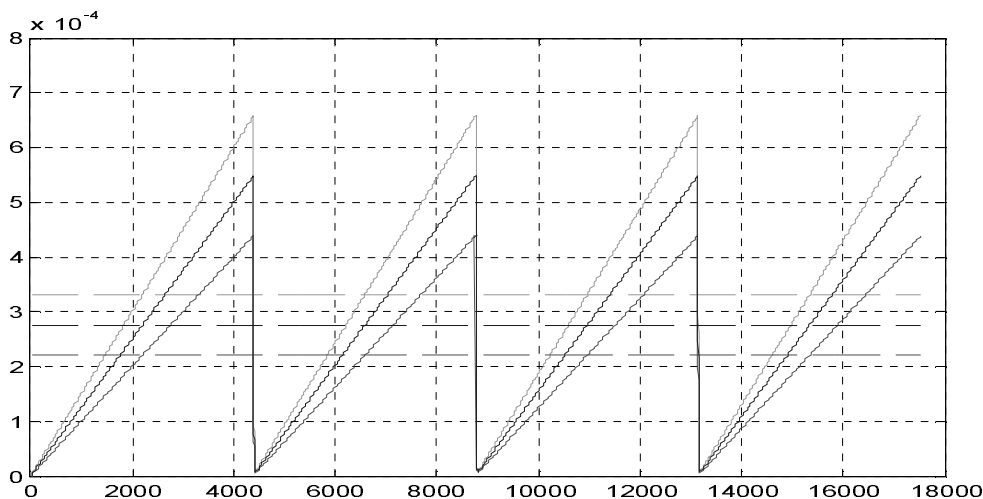


Figure 3 – Valeur moyenne et indisponibilité instantanée de l'architecture 1oo1 pour les différentes valeurs de DC : ---- DC=0.4 ; - - - - DC= 0.5 ; - · - · - DC= 0.6

La figure 3 montre que la probabilité de défaillance dangereuse de l'architecture 1oo1 reste encadrée par les probabilités supérieures et inférieures de défaillance sur demande correspondant aux valeurs

maximum et minimum que peut prendre le taux de couverture. Cette propriété est liée à la cohérence du système au regard de la disponibilité.

3.3. Architecture 1oo2

Cette architecture proposée à la figure 4 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.

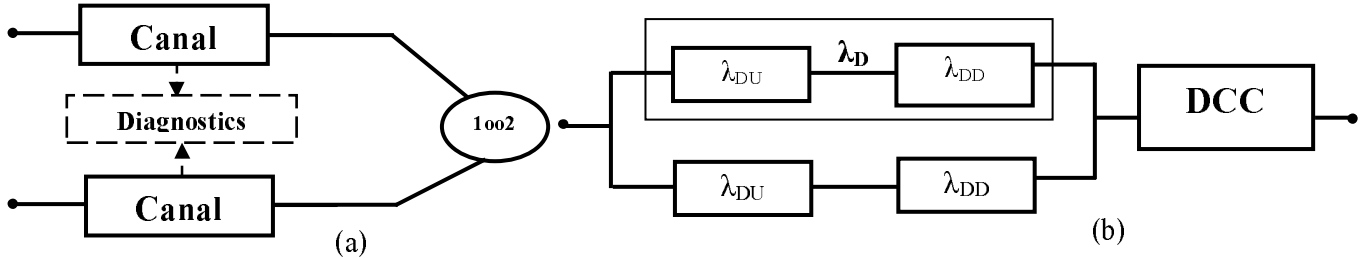


Figure 4 : Blocs-diagrammes physique (a) et de fiabilité (b) de l'architecture 1oo2

Le modèle multi-phases [Inn 06] 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 5.

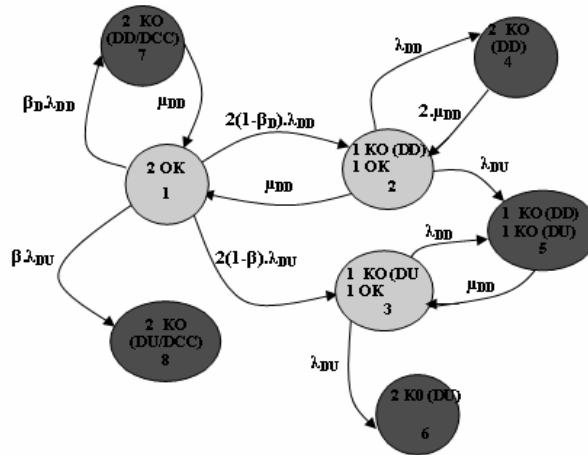


Figure 5 : Modèle markovien multi-phases de l'architecture 1oo2

Dans ce modèle, β_D et β représente 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 [Inn 06] sont définis comme suit :

$$P_1(d_i) = P_1(f_{i-1}); P_2(d_i) = P_2(f_{i-1}) + P_3(f_{i-1}); P_4(d_i) = P_4(f_{i-1}) + P_5(f_{i-1}); \quad (5)$$

$$P_7(d_i) = P_6(f_{i-1}) + P_7(f_{i-1}) + P_8(f_{i-1}); P_3(d_i) = P_5(d_i) = P_6(d_i) = P_8(d_i) = 0. \quad (6)$$

Etude quantitative :

Si nous considérons les données numériques suivantes :

- MTTR = 8h ; $T_1=4380h$; $\lambda_D=2,5 \cdot 10^{-5} h^{-1}$; $\mu_{DD}=\text{MTTR}$; $\beta=\beta_D=20\%$;
- $DC \in [0.4, 0.6]$

L'évolution de l'indisponibilité au cours du temps pour les différentes valeurs du taux de couverture de diagnostic est fournie à la figure 6, à partir des équations 2,3, 5 et 6 :

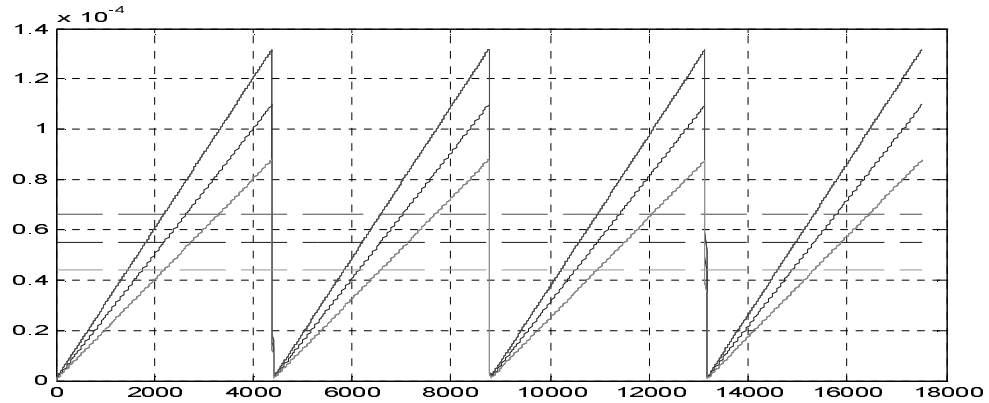


Figure 6 – Valeur moyenne et indisponibilité instantanée de l'architecture 1oo2 pour les différentes valeurs de DC : --- DC=0.4 ; --- DC= 0.5 ; --- DC= 0.6

Comme dans le cas précédent, l'indisponibilité instantanée du système est encadrée par des bornes supérieure et inférieure liées à l'intervalle défini pour le taux de couverture de diagnostic grâce à la monotonie de la fonction disponibilité associée à ce système.

4. Application à un HIPS

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 7 a été proposé dans [Sig 05] et sera utilisé comme exemple.

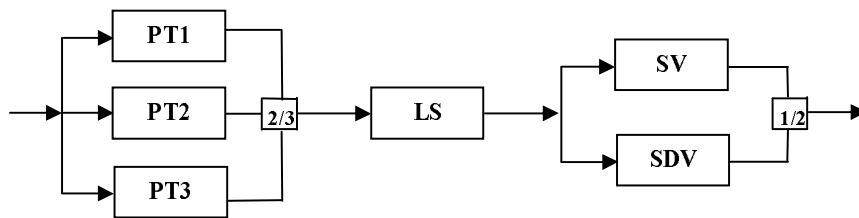


Figure 7 – Bloc- diagramme de fiabilité du HIPS étudié

Le HIPS étudié est composé de :

- la partie capteur en architecture 2oo3, constitué de trois capteurs de pression PT_i .
- la partie unité logique (Logic Solver) en architecture 1oo1.
- la partie actionneur en architecture 2oo1, composés par les vannes SV et SDV.

La probabilité moyenne de défaillance sur 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 [CEI 98]:

$$PFD_{HIPS} = PFD_{Cap} + PFD_{UL} + PFD_{AC} \quad (4)$$

$$PFD_{HIPS} = PFD_{2oo3} + PFD_{1oo1} + PFD_{1oo2} \quad (5)$$

Etude quantitative :

Deux cas sont distingués selon que les tests de diagnostic des composants soient réalisés simultanément ou non. L'ensemble des données numériques pour les deux cas est fourni dans le tableau 2.

Paramètre	$\lambda_D (h^{-1})$	DC	Ti (h)	Ti (h)	MTTR (h)	β (%)
Composant			Cas 1	Cas2		DCC
PT1	17.5E-7	[0.4, 0.6]	T1 = 4380	T1 = 1460	8	20
SDV	10.25E-7	[0.4, 0.6]	T2 = 4380	T2 = 4380	8	20
SV	10.25E-7	[0.4, 0.6]	T2 = 4380	T2 = 4380	8	20
Logic Solver	2.5E-7	[0.4, 0.6]	T3 = 4380	T3 = 2920	8	0

Tableau 2 : Données numériques

1^{er} Cas : tous les composants du système sont testés simultanément.

La figure 8 montre l'évolution de la probabilité de défaillance dangereuse instantanée en fonction des valeurs de $DC \in [DC_{min}, DC_{max}]$.

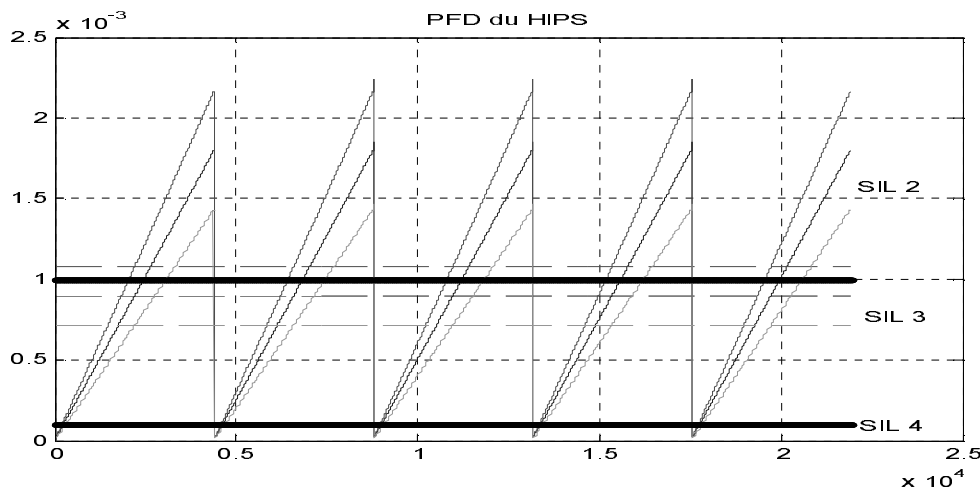


Figure 8 – Valeur moyenne et indisponibilité instantanée de HIPS pour les différentes valeurs de DC : ---- $DC=0.4$; ---- $DC=0.5$; ---- $DC=0.6$

Ainsi, sachant $0,4 \leq DC \leq 0,6$ la probabilité moyenne de défaillance sur demande est $7,15 \cdot 10^{-4} \leq PFD_{avg} \leq 1,07 \cdot 10^{-3}$. Dans le cas où DC est maximum, le SIS passe plus de 60% de son temps dans le domaine de SIL 2, ce qui explique l'obtention d'une valeur moyenne qui est égale à $1,07 \cdot 10^{-3}$ et classe ce $HIPS$ de niveau SIL 2. Lorsque DC est minimum, la probabilité moyenne de défaillance sur demande est égale à $0,715 \cdot 10^{-3}$ et classe le $HIPS$ de SIL3.

Nous constatons très rapidement que l'imprécision sur le taux de couverture de diagnostic amène très rapidement une variation du niveau de SIL du $HIPS$ alors qu'une valeur précise mais incertaine nous aurait fourni un niveau unique de SIL. L'importance de l'imprécision sur la qualification des systèmes de sécurité n'est pas négligeable et mérite une attention toute particulière.

2^{ème} Cas : les composants du système sont testés à des intervalles de temps différents.

Dans les résultats de cette simulation (figure 9), l'encadrement de la probabilité instantanée de défaillance sur demande est conservé. Pour $0,4 \leq DC \leq 0,6$ nous obtenons $4,32 \cdot 10^{-4} \leq PFD_{avg} \leq 6,48 \cdot 10^{-4}$ ce qui place ce $HIPS$ sur un SIL 3 quelle que soit la valeur de DC dans l'intervalle fourni.

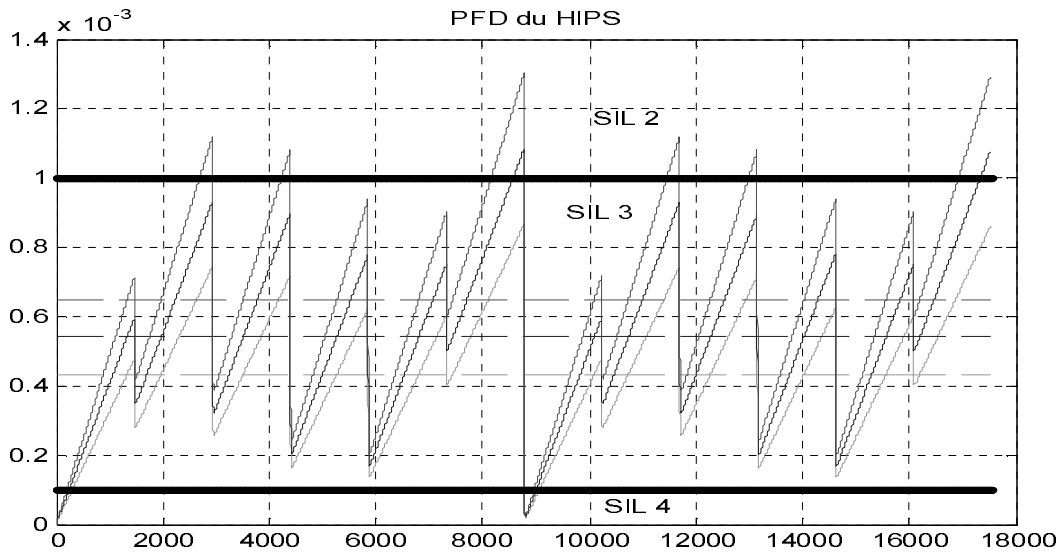


Figure 9 – Valeur moyenne et indisponibilité instantanée de HIPS pour les différentes valeurs de DC : -
 --- DC=0.4 ; ---- DC= 0.5 ; -.-.- DC= 0.6

5. Conclusions

L'imprécision dans les études de fiabilité et disponibilité des systèmes est un problème significatif souvent minoré. Nous avons proposé dans cet article l'étude des effets de l'imprécision sur un seul paramètre caractéristique d'un système instrumenté de sécurité et nous avons montré que cela pouvait entraîner des variations de qualification de son niveau de sécurité. Compte tenu de ce constat, il semble crucial d'étudier les effets des imprécisions affectant l'ensemble des paramètres et, les chaînes de Markov multi-phases à intervalles sont des modèles pertinents dans ce contexte.

Références

- [Lan 07] B. Lanternier et J.-M. Dranguet, Maintenance optimization of sensors for certification in compliance with the IEC 61511 standard, ESREL07, 2007.
- [CEI 98] Norme internationale CEI 61508. Sécurité fonctionnelles des systèmes électriques/ électroniques/ électroniques programmables relatifs à la sécurité ; parties 1 à 7; octobre 1998-mai 2000 ; Genève, Suisse.
- [Inn 06] F. Innal, Y. Dutuit, and A. Rauzy. Quelques interrogations et commentaires relatifs à la norme cei 61508. In Proceedings of the Lambda Mu 2006 Conference, Lille, France, 2006.
- [Sig 05] J.-P. Signoret, Methodology SIL evaluations related to HIPS – Total Draft Memo, April 27-2005.
- [Dut 08] Y. Dutuit, F. Innal, A. Rauzy, J.-P. Signoret, Probabilistic assessments in relationship with safety integrity levels by using fault trees. RESS, 2008.
- [Koz 02] I. Kozine, L. Utkin, Interval valued Finite Markov Chains , Reliable computing, vol. 8, p. 97-113, 2002.
- [Utk 07] L. Utkin, F. Coolen, New metaheuristics, neural & fuzzy techniques in reliability, vol. 2 of Computational intelligence in reliability engineering, G. Levitin, Chapter 10 Imprecise reliability: An introductory overview., pp. 261-306, 2007.