Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Probabilité de Défaillance à la Demande moyenne et Tests longs par Réseaux Bayésiens Dynamiques
Mean Probability of Failure on Demand and Long Time Test by Dynamic Bayesian Network

Christophe SIMON
Université de Lorraine, CNRS, CRAN
F-54000 Nancy, France
christophe.simon@univ-lorraine.fr

Walid MECHRI
Université de Tunis El Manar
Tunis, Tunisie
walid.mechri@isim.rnu.tu

Philippe WEBER
Université de Lorraine, CNRS, CRAN
F-54000 Nancy, France
philippe.weber@univ-lorraine.fr

***Résumé* — Cet article étudie la modélisation de l'indisponibilité des systèmes instrumentés de sécurité (SIS) par les réseaux bayésiens dynamiques (RBD) dans le cas particulier de tests de durée importante. La durée augmente la complexité du modèle lorsque l'on considère l'indisponibilité des composants étant donné le test, mais elle est plus réaliste.**

Mots Clés — SIS, indisponibilité moyenne, test d'inspection, durée de test, stratégie de test.

***Abstract* — This paper studies the modelling of the unavailability of instrumented security instrumented systems (SIS) by dynamic Bayesian networks (DBNs) in the case of large tests duration. Duration increases the complexity of the model when considering the unavailability of components given the test but is more realistic.**

Keywords- SIS, Mean availability, Proof Test, Test duration, Test strategy

I. INTRODUCTION

Dans de nombreux secteurs industriels des Systèmes Instrumentés de Sécurité (SIS) sont installés pour réduire les risques à un niveau admissible en détectant les précurseurs d'événements dangereux. Un SIS est utilisé pour effectuer une ou plusieurs fonctions de sécurité (SIF) [1], mais il est souvent question d'étudier chacune de ces fonctions. Le but d'une SIF est de détecter les événements dangereux, d'effectuer les actions de sécurité requises et de maintenir ou d'amener l'entité sous contrôle (EUC) dans une situation sûre.

Les exigences relatives à la fonction de sécurité exposées dans les normes [2], [3] introduisent l'évaluation quantitative de la performance du SIS et sa classification selon les niveaux de performance visés (SIL) [4, p. 7]. La performance du SIS est calculée sur la base de l'évaluation de l'indisponibilité de la SIF qu'il assure [5]. Deux concepts particuliers sont utilisés pour exprimer la performance en matière de sécurité. La probabilité moyenne de défaillance à la demande (PFD_{avg}) pour les SIF exploitées en mode de faible demande, et la probabilité de défaillance par heure (PFH) pour les SIF exploitées en mode de demande élevée (ou continue) [6].

Le mode faible demande est un cas particulier pour les systèmes de sécurité qui sont en fonctionnement permanent, mais qui ne sont sollicités que si les paramètres de l'EUC dépassent les valeurs seuils [7]. Ce cas d'usage amène à la notion de défaillances latentes qui ne peuvent être découvertes que si une demande se produit ou si on vérifie leur absence. Les défaillances latentes sont donc un problème clé des SIS en mode de faible demande. Pour le résoudre, des diagnostics intégrés sont réalisés et des tests répétés sont mis en œuvre. Même si un SIS a généralement une structure peu complexe, son étude peut être plus complexe que prévu en raison de la présence ces défaillances latentes [8].

L'évaluation de la performance d'un SIS peut être déterminée par plusieurs méthodes et modèles. Il est à noter qu'aucune technique particulière n'est recommandée dans la CEI 61508 [2]. Néanmoins, certaines d'entre elles sont mentionnées dans leurs annexes. Certains modèles sont statiques (les blocs diagrammes de fiabilité [9] et les arbres de défaillance [5]) qui supposent des hypothèses fortes sur la durée et la stratégie des tests, tandis que d'autres peuvent décrire des caractéristiques dynamiques (tels les chaînes de Markov [10], les réseaux de Petri [11] et réseaux bayésiens dynamiques (RBD) [12]).

Dutuit et al. [5] fait valoir que l'analyse par arbre de défaillance est facile à manipuler par les praticiens, mais donne parfois des résultats approximatifs en raison des hypothèses sur les tests. Catelani et al. [13] évalue la PFD_{avg} d'un système de sécurité par une méthode des blocs diagrammes de fiabilité avec peu de considérations sur les tests. Hokstad [14] donne de nouvelles approximations pour l'évaluation PFD_{avg} et montre l'impact du taux de sollicitation pour le SIS travaillant en mode de demande faible ou élevée. Zhang et al. [15] propose un réseau bayésien pour évaluer le PFD_{avg} en tenant compte des facteurs d'influence de la fiabilité dus au contexte des applications sous-marines [8].

Mechri et al. [16] propose une approche par réseaux de fiabilité pour concevoir une architecture optimale par allocation de la fiabilité des composants. Pour une intention

similaire, Chebila et al. [10] présente de nouvelles formulations analytiques génériques permettant l'évaluation de la performance de SIS en termes d'intégrité de sécurité. Cela permet de travailler sur l'optimisation de la conception de l'architecture SIS. Pour ces deux travaux, peu de paramètres concernant les caractéristiques des tests sont pris en compte.

Shu et al. [17] applique l'analyse de Markov pour évaluer le SIL du SIS où ils considèrent un modèle simplifié et une structure générique k/n avec des facteurs β de causes communes (DCC) et des défaillances sûres non détectées. Dutuit et al. [5] propose d'appliquer des chaînes de Markov multi-phases pour traiter les effets des dépendances dues aux tests de preuve, DCC, etc. Signoret et al. [11] utilise des réseaux de Petri pour qualifier les SIS. Les réseaux de Petri permettent de calculer très finement les performances et d'analyser l'impact de plusieurs paramètres, mais nécessitent des simulations de Monte-Carlo couteuses en temps de calcul.

Hokstad et al. [18] discute de la contribution significative du modèle particulier de DCC dans l'analyse de fiabilité de SIS pour l'industrie du pétrole et du gaz. Mechri et al. [8] intègre plusieurs paramètres de performance des tests. Innal et al. [7] envisage des tests de preuve partielle et complète avec une chaîne de Markov à commutations. Wu et al. [19] intègre la contribution temporelle des réparations imparfaites et des tests de preuve. Dans tous ces travaux, la performance des tests ne tient pas compte de la durée des tests, ce qui introduit des dépendances et peut avoir un impact important sur les performances du système.

Torres-Echeverria et al. [20] accorde plus d'attention aux stratégies de test et à la manière d'évaluer les performances des SIS par le biais d'un arbre de défaillance pour les couches SIS redondantes ou de type k/n. Ils proposent d'utiliser un modèle compact qui prend en compte plusieurs paramètres tels que DCC, le taux de couverture de diagnostic (DC), les instants des tests de preuve, etc. Brissaud et al. [21] analyse l'impact des tests partiels et développe une formule générale pour évaluer la performance de SIS pour les systèmes à composants multiples. Liu et al. [22] envisage un test d'inspection apériodique basé sur les états des composants et la modélisation des réseaux de Petri.

Pour intégrer les stratégies de test, il est nécessaire de mettre au point une formule générale pour évaluer les performances des systèmes à composants multiples.

II. SYSTEMES INSTRUMENTES DE SECURITE ET LEUR EVALUATION

A. Principes du SIS

Les SIS sont largement utilisés dans les industries de transformation pour prévenir les situations dangereuses impliquant des risques réels pour les personnes ou l'environnement (tel que feu, gaz toxique, surpression, etc.) [2]. L'objectif du SIS est de fournir une ou plusieurs fonctions pour protéger et maintenir un état sûr d'une EUC en fonction d'un événement dangereux [2], [3].

En général, un SIS est un système qui consiste en une combinaison quelconque de trois parties : un sous-système capteurs, un sous-système unité logique et un sous-système éléments finaux. Le sous-système capteur surveille la dérive des paramètres (pression, température, etc.) vers un niveau dangereux. Ce sous-système est constitué de capteurs, de détecteurs ou de transmetteurs. Le sous-système unité logique collecte le signal du sous-système capteur, interprète ces signaux et décide des actions à entreprendre. Le sous-système éléments finaux, constitué d'un ou plusieurs éléments d'actionnement (par exemple vannes, électrovannes, alarmes) met le processus dans sa position de sécurité et l'y maintien pour éviter tout dommage.

La norme IEC 61508 [2] peut désormais être considérée comme la norme principale pour la spécification et la conception des SIS. Sa déclinaison sectorielle pour l'industrie de transformation [3] est destinée aux intégrateurs et aux utilisateurs de ce domaine. Les exigences de la fonction de sûreté exposées dans [2], [3] introduisent également une approche probabiliste pour l'évaluation quantitative des performances de sécurité. L'introduction de la probabilité dans l'évaluation du SIL a impliqué l'évaluation particulière de la PFD_{avg} pour les systèmes à faible demande. La qualification de cette performance est déterminée par des niveaux référencés (SIL). Ainsi, le PFD_{avg} est en fait évalué par l'indisponibilité moyenne du SIS pour assurer la fonction de sécurité à la demande [20]. La norme CEI 61508 [2] établit quatre niveaux de classification basés sur le PFD_{avg} où SIL 4 représente l'exigence la plus stricte, et SIL 1 la moins stricte. Les différents niveaux de SIL sont définis dans le tableau 1 pour le mode de faible demande.

TABLE I. SIL POUR LE MODE FAIBLE DEMANDE [2]

SIL	PFD_{avg}
4	$]10^{-4}, 10^{-5}]$
3	$]10^{-3}, 10^{-4}$
2	$]10^{-2}, 10^{-4}]$
1	$]10^{-1}, 10^{-2}]$

L'évaluation de la PFD_{avg} doit prendre en compte plusieurs caractéristiques comme : les taux de défaillance, DCC, les performances des tests, les temps de réparation, DC, les fréquences des tests, les stratégies de test et la durée des tests.

B. Détection et diagnostic des défaillances

Le PFD_{avg} est une mesure d'indisponibilité par rapport à une défaillance dangereuse. Ce type de défaillance peut mettre le SIS dans un état dangereux. Une caractéristique des SIS est que les défaillances sont normalement cachées. Pour la vérification du SIS, plusieurs tests ont été définis. Les tests de preuve et les tests de diagnostic sont les deux principales techniques appliquées pour détecter les défaillances dangereuses.

- Les tests de preuve (test hors ligne) sont des tests d'inspection réguliers avec un intervalle entre plusieurs mois et plusieurs années. Ils sont effectués pour détecter les défaillances latentes d'un système cible. Après un test d'inspection, le SIS peut être restauré dans un état "comme neuf", mais d'autres niveaux de restauration peuvent être considérés [19].
- Les tests de diagnostic (tests en ligne) sont effectués plus souvent que les tests de preuve, généralement avec un intervalle entre quelques secondes et quelques heures. Le diagnostic peut détecter des défaillances essentiellement aléatoires d'un composant ou d'un

module SIS [23]. L'état "aussi bon que neuf" ne peut être supposé, car seule une fraction des défaillances dangereuses peut être détectée.

C. *Défaillances des composants*

Selon la norme [2], les défaillances des SIS sont classées en dangereuses ou sûres. Les défaillances dangereuses (λ_D) provoquent des conséquences dangereuses, c'est-à-dire l'incapacité à remplir la fonction de sécurité, tandis que les défaillances sûres (λ_S) entraînent des déclenchements intempestifs [24].

Les défaillances des composants SIS sont généralement révélées par les tests de diagnostic, qui ont un effet important sur l'évaluation de la PFD_{avg} . L'efficacité d'un test de diagnostic ou le taux de couverture de diagnostic (DC) est mesuré par le pourcentage du taux total de défaillances détectées. DC divise les fractions dangereuses et sûres en modes de défaillance détectés (λ_{DD})et (λ_{SD}) et non détectés (λ_{DU}) et (λ_{SU}) . Compte tenu du paramètre, le taux de défaillance total d'un composant (λ_T) est donné par Eq. (1).

$$\lambda_T = DC * \lambda_D + (1 - DC) * \lambda_D + DC * \lambda_S + (1 - DC)\lambda_S \quad (1)$$

Notez que nous nous concentrons principalement sur les défaillances dangereuses et que λ_S n'est généralement pas pris en compte. Certains chercheurs expliquent que toutes les défaillances sont dangereuses en choisissant correctement la fraction de défaillances sûres [25].

D. *Contribution des défaillances de cause commune*

Les défaillances de causes communes (DCC) sont importantes dans l'analyse des performances des SIS [26]. Dans la plupart des analyses de fiabilité, les DCC sont modélisées par le modèle du facteur β en raison de sa complexité raisonnable et de l'initiative internationale visant à évaluer ses valeurs [27]. En outre, le modèle du facteur β est régulièrement introduit dans les modélisation [23]. Le modèle du facteur β est une façon de quantifier les DCC où le facteur β exprime la fraction de DCC parmi toutes les défaillances d'un composant [8].

En outre, le facteur β divise le taux de défaillance total en deux modes de défaillance : indépendant λ_I et de cause commune λ_{DCC} comme précisé par l'équation 2 :

$$\lambda_T = (1 - \beta) * \lambda_T + \beta * \lambda_T \quad (2)$$

En incluant la quantification des DCC modélisée par le facteur β (Eq. 2) dans l'expression du taux de défaillance total (Eq. 1), les modes de défaillance détectées et non détectées sont divisés en défaillances indépendantes et de causes communes. Il est alors possible de détailler l'ensemble de tous les types de défaillance.

E. *Tests et stratégies de tests*

Un test est par essence une activité répétitive. Il peut être classé comme partiel ou complet, c'est-à-dire s'appliquer sur tout ou partie des éléments. Un test de tous les composants rendra la SIF non disponible pendant toute la durée du test, mais permettra la recherche d'une défaillance latente sur chacun des composants. On privilégiera l'arrêt de l'EUC lors d'une telle stratégie de test, ce qui donne un test de durée négligeable.

Un test partiel permet de tester des composants tout en gardant la disponibilité de la SIF, mais avec une performance temporairement dégradée. La stratégie de test consiste à choisir les composants à tester selon un protocole temporel donné pour conserver la disponibilité de la SIF. On retrouve des séquences de tests régulières, étagées, aléatoires, etc.

Un test peut être partiel en ce sens qu'il n'est destiné qu'à la détection de certaines défaillances [28] grâce à un protocole spécifique. C'est généralement dans un objectif précis d'optimisation du ratio temps/performance. Il a donc une performance propre.

Parallèlement à la stratégie de test, un test présente une certaine efficacité. En général, il est considéré comme parfait. Cela signifie que toutes les défaillances non détectées sont révélées lors d'un test et réparées. La restauration est également généralement considérée comme parfaite. Le SIS est restauré dans un état aussi bon que neuf. En situation réelle, le test peut être imparfait, c'est-à-dire qu'il peut ne pas révéler tous les types de défaillances non détectées, ou qu'il est effectué dans des conditions différentes de celles d'une situation de demande réelle. Pour modéliser cette performance relative, le facteur $1 - \xi_i$ représente la probabilité conditionnelle qu'une défaillance non détectée ne soit pas détectée par le test étant donné que la défaillance s'est produite avant le lancement du test [8]. ξ_i représente l'incapacité du test à révéler les défaillances non détectées. Un test est parfait si $\xi_i = 0$ et imparfait si $\xi_i > 0$.

Outre l'incapacité du test, d'autres paramètres sont caractéristiques comme :

- la probabilité de défaillance due au test (γ) ou l'innocuité du test,
- la durée du test (π),
- le taux de réparation/restauration (μ).

Chacun de ces paramètres va avoir une incidence caractéristique sur l'indisponibilité instantanée. La Fig. 1 montre l'effet des paramètres sur l'indisponibilité d'un seul composant/bloc-système lorsque les tests sont effectués à une fréquence donnée.

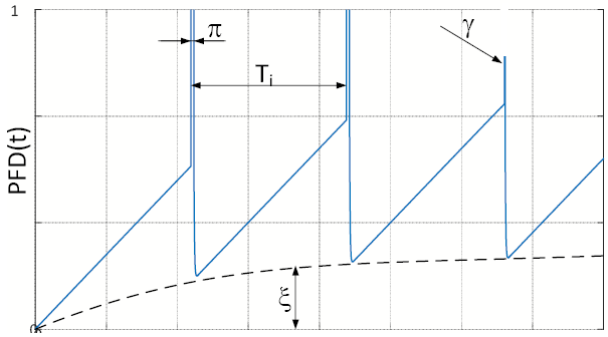


Fig. 1. PFD d'un système 1 parmi 1

F. *hypothèses d'évaluation des performances*

Rappelons que pour qualifier la SIF assurée par un SIS, si les contraintes architecturales sont vérifiées, il est nécessaire de calculer la valeur de la PFD_{avg}. Cette évaluation nécessite une modélisation précise et détaillée. Pour cela, nous faisons les hypothèses suivantes :

- Tous les composants de SIS ont des taux d'échec supposés constants λ, c'est-à-dire les temps avant l'échec sont considérés comme des distributions exponentielles [5].

- Les structures de type k/n sont soumises à des tests partiel ou complet [21], [28]. Si $k = 1$ la structure modélisée est un système parallèle et si $k = n$ le système modélisé est un système en série.
- Les tests complets peuvent détecter toutes les défaillances et les tests partiels ne peuvent détecter que certaines défaillances [28].
- Tous les composants sont testés ensemble lors de n'importe quel test (c'est-à-dire pas de tests échelonnés).
- Une stratégie de tests échelonnés signifie que les canaux redondants sont testés à des moments différents, mais en même temps un intervalle de test constant est maintenu.
- La probabilité ξ de ne pas détecter une défaillance pendant un test est prise en compte.
- La probabilité de défaillance γ due au test est prise en compte.
- La durée du test π est considérée.
- Le temps de restauration d'une défaillance détectée est supposé négligeable.
- Si les défaillances dangereuses détectées sont révélées immédiatement, une action de réparation est immédiatement lancée (c'est-à-dire que les défaillances détectées sont supprimées). Lors des tests et des réparations, des mesures sont prises pour maintenir un état sûr de l'EUC de telle sorte que toute durée de test ou de maintenance n'est pas incluse dans la quantification de la PFD.
- Après chaque essai/restauration, tous les composants du SIS sont dans leur état initial [21].
- Le facteur β est utilisé pour modéliser les DCC [20].
- Les défaillances de sécurité ne sont pas prises en compte.

Les hypothèses présentées ont pour but de développer un modèle détaillé. Ce modèle est appliqué pour l'évaluation précise des performances du SIS. Dans ce contexte, toutes les composantes du SIS ont des taux de défaillance constants λ c'est-à-dire que des distributions exponentielles sont prises en compte. Cette hypothèse est habituelle même si les applications d'ingénierie réelles avec un mécanisme de défaillance variable dans le temps comme le vieillissement, la fatigue, la corrosion, la dégradation, etc. nécessitent l'application de distributions de taux de défaillance variables dans le temps comme les lois log-normale et Weibull.

La prise en compte de tous les paramètres, c'est-à-dire les états des composants redondants peut s'avérer lourde lorsqu'il s'agit d'une chaîne de Markov. Murphy [29] fait valoir que les RBD sont une forme compacte de chaînes de Markov. Un RBD peut donc être un outil puissant pour modéliser la structure des SIS en considérant les tests comme des variables exogènes et ainsi que pour les calculs d'indisponibilité. S'il est fait référence à des structures types k/n alors l'emploi des RBD ou RBD orientés objets (RBDOO) faciliteraient la construction de modèles et l'évaluation de la PFD_{avg}.

III. RESEAU BAYESIEN POUR LA MODELISATION DE L'INDISPONIBILITE DES SIS

Les RB sont des modèles graphiques [30] qui combinent la théorie des graphes avec la théorie bayésienne pour fournir un cadre général de modélisation graphique intuitive et claire des problèmes du monde réel. Ils offrent de nombreux avantages en matière de modélisation :

- Représentation compacte [31].
- Prise en compte de variables exogènes pour les processus de conditionnement (RBD) à temps variants [32].
- Calcul par inférence en tenant compte des observations (états connus des composants) [32].

A. Modèles graphiques statiques dirigés

Un réseau bayésien statique se compose de deux parties distinctes : la partie qualitative et la partie quantitative. La partie qualitative est représentée par un graphe acyclique dirigé dont les nœuds représentent les variables aléatoires du problème et les arcs représentent la dépendance conditionnelle entre les variables. Pour la modélisation des SIS, les nœuds représentent les états des composants, des sous-systèmes et des états du système. La partie quantitative est exprimée par un ensemble de fonctions locales associées à chaque variable du graphique selon le cadre de modélisation bayésien.

Pour chaque nœud racine X, une distribution a priori $P(X)$ doit être définie sur les états de la variable X. Pour les autres nœuds, une fonction conditionnelle $P(X|Pa(X))$ est spécifiée pour chaque état possible de X connaissant les états de ses parents désignés par $Pa(X)$.

Fondamentalement, les RB statiques ne permettent pas de gérer les connaissances variables dans le temps, car elles ne représentent pas la dimension temporelle. Néanmoins, divers RBD ont été proposés [32].

B. Réseaux Bayésiens Dynamiques

Un RBD est un modèle graphique dirigé prenant en compte la dimension temporelle. A chaque pas de temps $k\,\Delta T$ avec $k \geq 0$, une variable aléatoire X est représentée par un nœud X_k. Ainsi, à chaque pas de temps $k\,\Delta T$, un ensemble de nœuds caractérise toutes les variables à cette tranche de temps [32]. La dépendance entre deux pas de temps est directement liée à une relation causale entre variables. Ainsi, si un nœud X_k caractérise l'état d'un composant et X_{k+1} son état futur alors la probabilité conditionnelle $P(X_k|X_{k+1})$ est directement liée au taux de défaillance du composant X. Si maintenant X est un ensemble de composants alors il est possible de modéliser les états de l'ensemble comme pour une chaine de Markov. Il est important de rappeler que le processus modélisé est :

- Stationnaire : $P(X_k|X_{k-1})$ ne dépend pas de k.
- Markovien : $P(X_k)$ ne dépend que des distributions de ses nœuds parents. Ainsi, le pas de temps futur est conditionnellement indépendant du passé étant donné la tranche de temps actuelle [29].

Ainsi, le test est une variable exogène qui modifie la matrice de transition de la chaîne de Markov modélisée par le réseau bayésien dynamique. Si le test est connu à chaque instant $k\,\Delta T$, alors il est possible de conditionner la transition à la valeur du test $P(X_k|X_{k-1}, T_k)$. Le RBD est alors équivalent à une chaîne de Markov commutée telle que proposée par [5]. Pour calculer l'indisponibilité instantanée de X, il suffit alors de sommer les probabilités sur les états de X_k selon la phase de test. Un nœud dédié à chaque pas de temps permet ce calcul. En revanche, la PFD_{avg} est l'intégrale de l'indisponibilité sous forme discrète et doit être évaluée séparément.

C. RBD, chaine de Markov commutée

L'activité du test est donc une variable exogène qui introduit une commutation entre deux chaines de Markov. La

Fig. 2 illustre le principe de fonctionnement. Selon la nature du système (architecture), la nature du test et ses caractéristiques, il est possible de définir un modèle RBD générique (cf. Fig. 3) dont on peut assurer la simulation.

L'activité du test et donc l'état de la variable exogène *T* se comporte comme un sélecteur de matrices de probabilités conditionnelles. Lorsque le test est inactif alors $P(X_k|X_{k-1}, T_k = 0)$ correspond à la chaine de Markov du bloc de composants étudiés. Pendant le test, $P(X_k|X_{k-1}, T_k = 1)$ modélise la nouvelle structure du système liée à la stratégie de test. La nouvelle chaine de Markov tiendra compte de la structure fonctionnelle choisie selon ce qui est testé. C'est la durée du test et le fait que le SIS assure tout de même sa fonction en situation dégradée qui nécessite cette structure. Le passage d'une situation à une autre demande à ce que les probabilités soient correctement redistribuées.

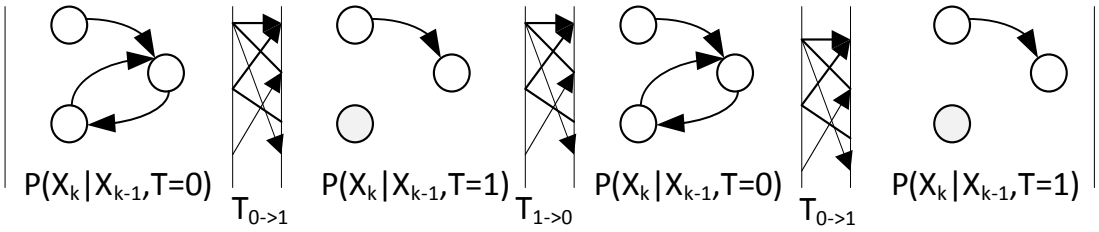


Fig. 2. Principe d'une chaine de Markov commutée et Test

Selon le type de test (partiel, efficace …) il peut y avoir plusieurs manières de redistribuer les probabilités entre les phases. Il est donc nécessaire de définir les matrices pour chacun des passages entre phases liées au test ($T_k = 0$, $T_k = 0 -> 1$, $T_k = 1$, $T_k = 0 -> 1$). Ce travail laborieux peut être avantageusement préparé avec des modèles de RBD caractéristiques des structures et des tests. Le modèle complet d'un système peut alors se faire par composition de modèles élémentaires instanciés au problème (RBDOO).

Cas 1oo1 : Le composant ne peut avoir que 3 états : fonctionnel (OK), en défaillance détectée (DD) ou en défaillance non détectée (DU). Le schéma de la Fig. 3 montre les différentes phases pour une structure 1oo1.

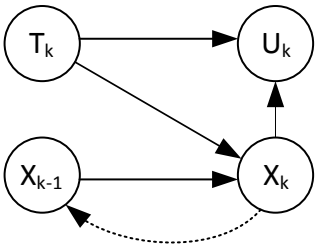


Fig. 3. RBD générique

On a donc :

$$P(X_k|X_{k-1}, T_k = 0) = \begin{bmatrix} 1-(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & 1-\mu_{DD} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (3)$$

$$P(X_k|X_{k-1}, T_k = 0 \to 1) = \begin{bmatrix} 1-\gamma & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (4)$$

$$P(X_k|X_{k-1}, T_k = 1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (5)$$

$$P(X_k|X_{k-1}, T_k = 1 \to 0) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1-\xi & \xi \end{bmatrix} \quad (6)$$

Où $T_k = 0$ précise que le test n'est pas effectif, $T_k = 1$ précise qu'il est effectif, $T_k = 0 \to 1$ indique la phase de démarrage du test et $T_k = 1 \to 0$ indique sa phase d'arrêt.

Cas 1oo2 : Une architecture de type 1oo2 présente 9 états, mais on peut les agréger pour réduire la taille de la chaine à 6 états. Ceci n'est pas une obligation, mais peut s'avérer plus simple à élaborer. Le test d'un composant sur 2 lorsqu'une stratégie de tests alternés est proposée donnera la chaine de Markov commutée ci-dessous :

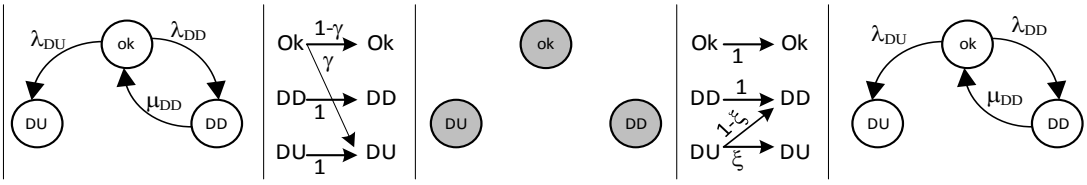


Fig. 4. Chaine de Markov commutée d'un 1oo1

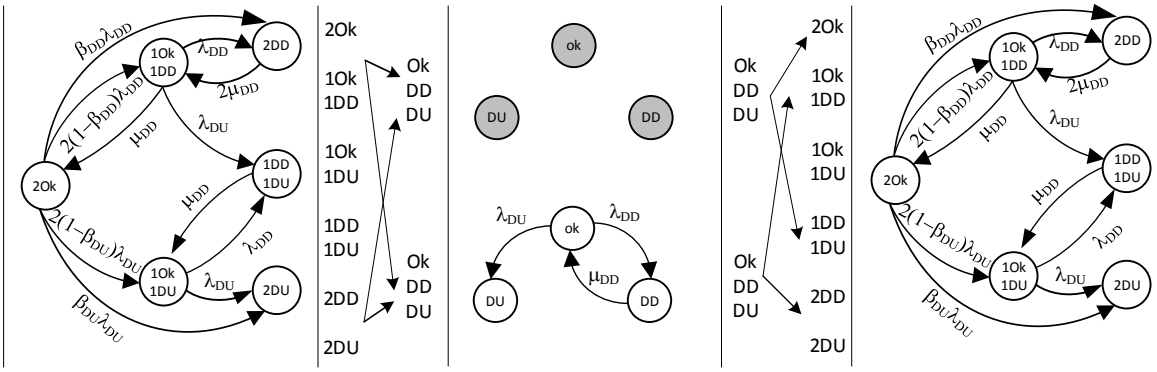


Fig. 5. Chaine de Markov commutée d'un 1oo2

Les 4 matrices liées aux 4 états du test peuvent être formulées ainsi :

$$P(X_k|X_{k-1}, T_k = 0) = \begin{bmatrix} - & 2(1-\beta_{DD})\lambda_{DD} & 2(1-\beta_{DU})\lambda_{DU} & \beta_{DD}\lambda_{DD} & 0 & \beta_{DU}\lambda_{DU} \\ \mu_{DD} & - & 0 & \lambda_{DD} & \lambda_{DU} & 0 \\ 0 & 0 & - & 0 & \lambda_{DD} & \lambda_{DU} \\ 0 & 2\mu_{DD} & 0 & - & 0 & 0 \\ 0 & 0 & \mu_{DD} & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (7)$$

$$P(X_k|X_{k-1}, T_k = 0 \to 1) = \begin{bmatrix} 1/2 & 0 & 0 & 1/2 & 0 & 0 \\ 1/4 & 1/4 & 0 & 1/4 & 1/4 & 0 \\ 1/4 & 0 & 1/4 & 1/4 & 0 & 1/4 \\ 0 & 1/2 & 0 & 0 & 1/2 & 0 \\ 0 & 1/4 & 1/4 & 0 & 1/4 & 1/4 \\ 0 & 0 & 1/2 & 0 & 0 & 1/2 \end{bmatrix} \quad (8)$$

$$P(X_k|X_{k-1}, T_k = 1) = \begin{bmatrix} 1-(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & \lambda_{DU} & 0 & 0 & 0 \\ \mu_{DD} & 1-\mu_{DD} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ 0 & 0 & 0 & \mu_{DD} & 1-\mu_{DD} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (9)$$

$$P(X_k|X_{k-1}, T_k = 1 \to 0) = \begin{bmatrix} 1-\gamma & \gamma(1-\xi) & \gamma\xi & 0 & 0 & 0 \\ 0 & 1-\gamma & 0 & \gamma(1-\xi) & \gamma\xi & 0 \\ 0 & 0 & 1-\gamma & 0 & \gamma(1-\xi) & \gamma\xi \\ 1-\gamma & (1-\gamma)\xi & \gamma\xi & 0 & 0 & 0 \\ 0 & 1-\gamma & 0 & \gamma(1-\xi) & \gamma\xi & 0 \\ 0 & 0 & 1-\gamma & 0 & \gamma(1-\xi) & \gamma\xi \end{bmatrix} \quad (10)$$

Pour un modèle k/3, le problème devient très complexe, mais reste abordable. Nous rappelons que l'objectif est d'élaborer des modèles génériques qui seront assemblés sous forme de briques de modèles.

D. Modélisation SIS avec RBD

La structure fonctionnelle d'un SIS peut être représentée par un bloc-diagramme de fiabilité à au moins 3 couches. Chaque couche ou sous-système indépendant peut être modélisé par un RBD générique ou une composition de RBD génériques modélisant les structures k/n suivant la structure de la Fig. 4.

L'organisation fonctionnelle se réduit alors à une mise en série/parallèle des modèles des couches qualifiant ainsi l'état de disponibilité du système à partir de celui des couches. La structuration du réseau bayésien passe par la définition des tables de probabilités conditionnelles spécifiant l'état de la couche à partir de l'état des composants qui la constitue. La composition de la structure est intégrée dans un nœud spécifique dont la table de probabilité conditionnelle est déterministe. La modélisation d'un SIS suit alors le schéma de la Fig.6.

L'indisponibilité instantanée à la demande (PFD) du système est alors obtenue pour être intégrée afin de vérifier le niveau de SIL

IV. CAS PRATIQUES

Cette section est consacrée à deux exemples afin de montrer comment l'approche est appliquée pour évaluer le SIL d'un SIS.

Le premier exemple concerne la simulation d'un système simple avec un système 1 parmi 1 (1oo1) pour calculer son indisponibilité à la demande, sa PFD_{avg} et sa sensibilité aux paramètres des tests.

Le second exemple est un modèle de SIS défini sur la base d'un bloc-diagramme de fiabilité tiré de l'exemple industriel proposé dans [24].

A. Modélisation d'un composant/architecture 1oo1

Afin de représenter l'équivalent RBD d'une architecture 1oo1, on considère une variable aléatoire discrète X à trois états $\{s_1, s_2, s_3\}$. Ces états représentent respectivement l'état opérationnel (OK), la défaillance dangereuse détectée (DD) et la défaillance dangereuse non détectée (DU).

Le modèle RBD de ce cas est donné à la Fig. 4. La table de probabilités conditionnelles résulte de la composition des équations 3 à 6.

La Fig. 8 montre l'évolution de l'indisponibilité instantanée pour différentes valeurs de ξ, γ et π. 6 cas de simulation sont considérés. Les valeurs des paramètres de fiabilité pour la simulation du RBD sont : $T_i = 2190\,h$ (intervalle des tests), $\lambda_D = 1.40\,10^{-5}h^{-1}$ (taux de défaillance global), DC = 60% et MTTR = 8 h [Mechri2015].

Dans les cas 5 et 6, c'est la durée du test qui est modifiée. La PFD instantanée présente un motif répétitif avec une indisponibilité de 1 pendant la période du test. Cela influence grandement la PFD_{avg} et nous oblige à une représentation semi-logarithmique.

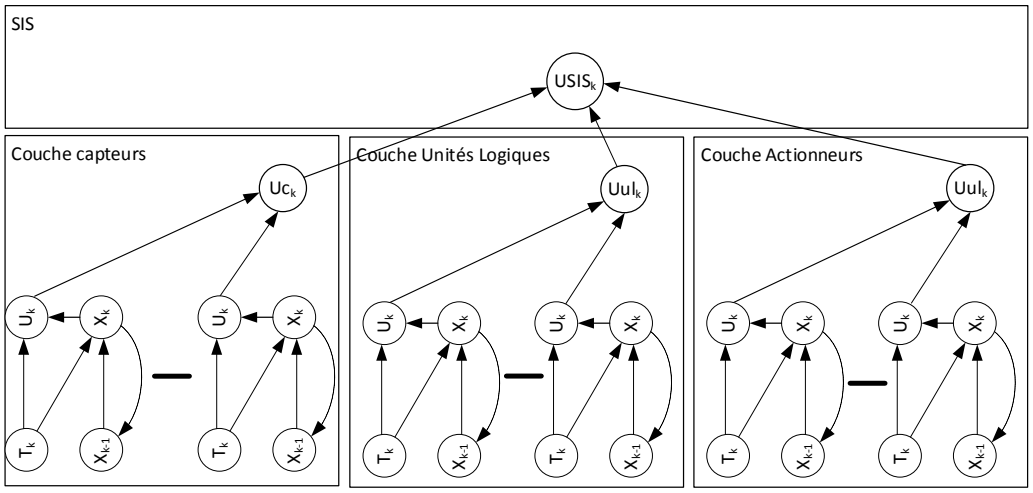


Fig. 6. Structure générique d'un RBD de SIS

La valeur de PFD_{avg} varie de $0.621\ 10^{-2}$ (cas 1) à $2.05\ 10^{-2}$ (cas 6). Le SIL du système 1 parmi 1 varie d'un niveau SIL 2 ($PFD_{avg} \in [10^{-3}, 10^{-2}]$) à un niveau SIL 1 ($PFD_{avg} \in [10^{-2}, 10^{-1}]$) selon le tableau I. Ces résultats sont exactement les mêmes que ceux proposés dans [8], mais calculés avec une chaine de Markov multi-phase.

Si l'on considère $\pi \neq 0$, l'indisponibilité du système 1oo1 passe à 1 pour toutes les périodes de test (l'intervalle de test du système 1oo1), cela s'explique par le fait que le système 1oo1 est indisponible pendant toute la durée du test π. Les cas 5 et 6 de la Fig. 6 montrent les indisponibilités en considérant les durées de test (8h et 20h) en représentation normale et semi-logarithmique.

Ainsi, l'augmentation de la valeur de π entraîne une augmentation de la valeur de PFD_{avg} qui peut elle-même induire une variation du SIL.

B. Modèlisation d'un SIS

Dans cet exemple, nous allons considérer un SIS dont la structure fonctionnelle est donnée à la Fig. 7.

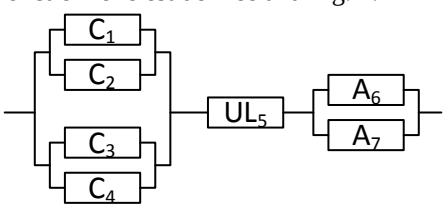


Fig. 7. Bloc-diagramme de fiabilité d'un SIS

Comme on peut le constater, le SIS est architecturé en 3 couches dont la couche capteurs est formée de deux blocs de 2 capteurs (C_1, C_2, C_3, C_4) en structure 1oo2. La couche Unité Logique (UL5) est en structure 1oo1 dont nous avons déjà donné le comportement à la section précédente. Enfin, la couche actionneurs (A_6, A_7) est en structure 1oo2. En suivant la proposition de la Fig. 6, on peut formuler le modèle RBD de la Fig. 9.

Le modèle générique principal est un RBD d'une structure 1oo2. Il suit le modèle générique proposé (cf. Fig.4) avec une table de probabilités conditionnelles composée à partir des équations 7 à 10.

En évaluant les distributions de probabilités du RBD avec le logiciel Bayesialab, la PFD instantanée du SIS est calculée par inférences successives. Ce calcul d'inférence est exact mais couteux. Il est toutefois possible d'approcher le résultat par simulation. Ensuite, la PFD_{avg} est déterminée en calculant la moyenne des valeurs ponctuelles par intégration numérique. La Fig.10 présente les résultats obtenus sur une échelle semi-logarithmique.

C. Analyse des résultats

Le modèle complet du RBD est simulé sur une période de 12000 heures. Les valeurs des caractéristiques de chaque composant sont données dans le tableau II.

La Fig. 10 montre l'évolution de l'indisponibilité instantanée de chaque bloc. On constate les motifs répétitifs sur chaque courbe dû aux tests. Le composant C_5 est indisponible à chaque test pendant la durée du test. Aussi, la PFD du SIS est à 1 à ces mêmes instants.

Comme les valeurs caractéristiques sont influentes et que certaines sont difficiles à estimer (DC, β, γ et ξ), il est important d'analyser la robustesse de la décision à leur valeur. Cette analyse de robustesse peut être réalisée via une analyse de sensibilité.

L'indisponibilité moyenne de chaque bloc de composants converge vers une valeur stationnaire, ce qui va induire le même comportement pour l'indisponibilité du SIS. C'est un comportement classique qui avait été montré dans [5], [8]. La PFD_{avg} nous indique que le SIS est de SIL1 ce qui s'accorde avec l'architecture de SIS qui a été proposée.

V. CONCLUSION

Dans cette étude, une application de RBD pour évaluer le SIL de SIS en mode de faible demande est proposée. La prise en compte des durées de test a nécessité une modélisation particulière avec des modèles markoviens commutés.

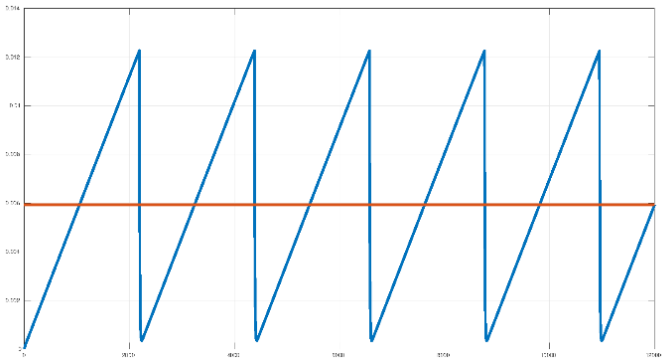
Une structure générique de RBD est proposée et peut être instanciée selon les structures fonctionnelles du SIS étudié dans l'esprit d'une approche orientée objet. Les RBD offrent donc une construction simplifiée du modèle global pour l'évaluation de la performance du SIS.

Sur le plan numérique, la comparaison des résultats peut être faite en analysant [8] et [33]. On trouve que sur des modèles complexes mais sans l'introduction de tous les paramètres d'un test, ces résultats sont les mêmes. L'inférence dans les réseaux bayésiens peut être exacte selon le niveau de charge de calcul et d'empreinte mémoire que l'on tolère. Il est possible de recourir à des inférences approximatives lorsque la complexité devient trop grande.

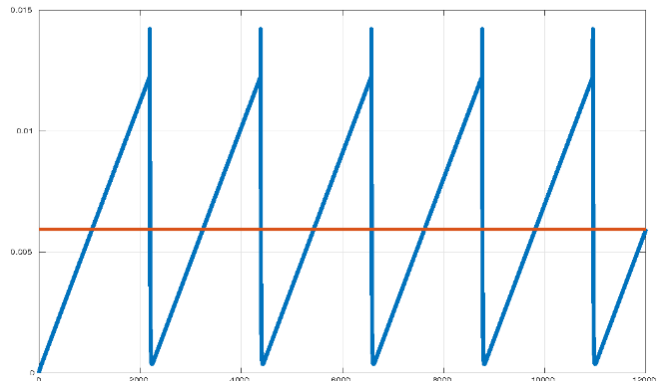
L'intégration de la durée de test n'a de réel sens que si les tests ne rendent pas indisponible l'ensemble du SIS. Toutefois, cela nous a contraints à formuler le comportement du bloc de composants pendant le test et donc de paramétrer l'effet du test sur les composants.

Il est important de préciser qu'il est possible d'aborder le problème avec d'autres outils de modélisation. L'équivalence entre les modèles markoviens et les RBD à variables exogènes ayant été montrés, il parait évident que les chaines de Markov sont un modèle valable.

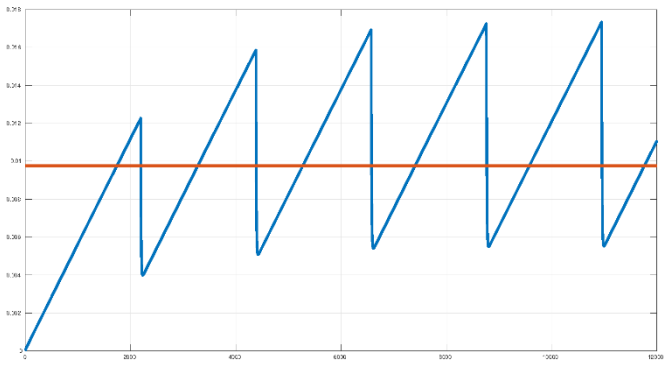
Les réseaux de Petri sont également des modèles parfaitement utilisables. Ils permettraient d'autres possibilités de modélisation bien connues. Ils permettent notamment de lever les contraintes des propriétés Markoviennes (Mémoire).



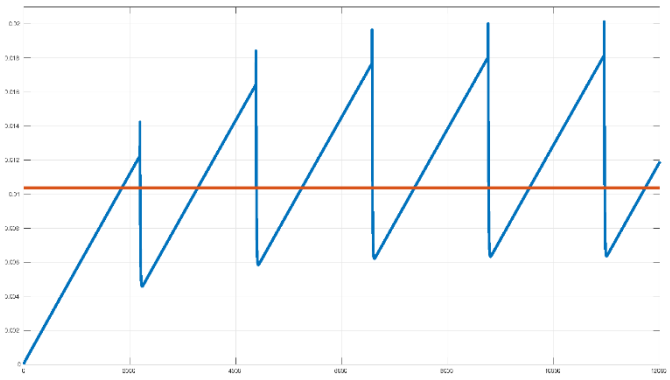
Case 1 : ξ=0; γ=0; π =0



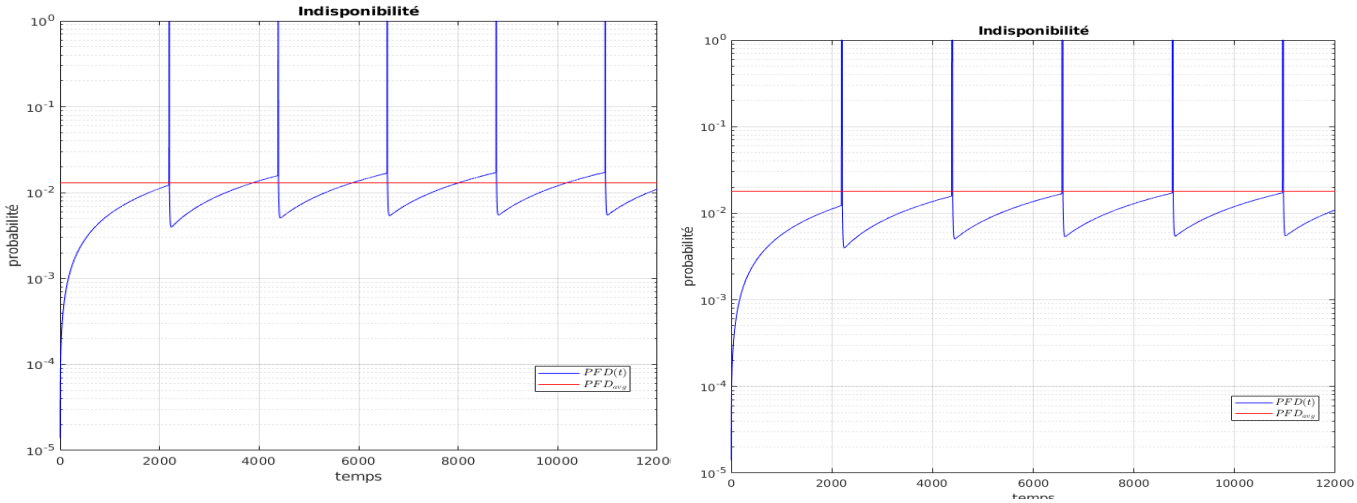
Case 2 : ξ =0; γ =0.002; π =0



Case 3 : ξ =0.3; γ =0; π =0



Case 4 : ξ=0.3; γ =0.002; π =0



Case 5 : ξ=0.3; γ =0.002; π=8 Case 6 : ξ=0.3; γ =0.002; π=20

Fig. 8. $PFD(t)$ and PFD_{avg} of 1oo1 system

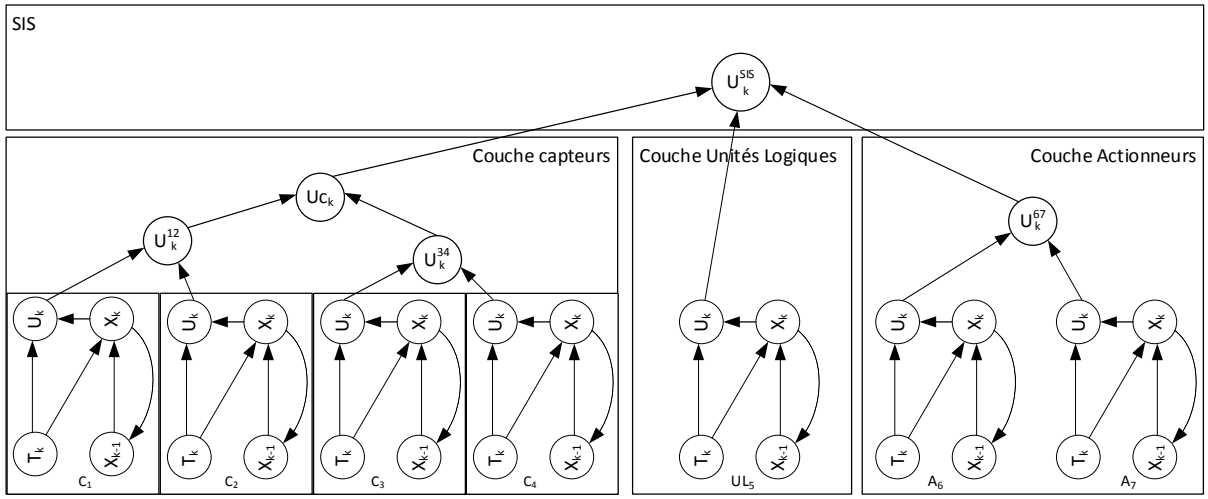


Fig. 9. RBD pour le calcul de la PFD du SIS

TABLE II. PARAMÈTRES CARACTERISTIQUES DES COMPOSANTS

Composantes \ Paramètres	C_1-C_2	C_3-C_4	UL_5	A_6-A_7
$\lambda_D * 10^{-6}$	5.00	5.00	4.60	5.00
DC	0.3	0.3	0.4	0.5
β_{DU}(%)	20	20		10
MTTR (h)	8	8	10	10
T_i(h)	730	730	1460	2190
ξ	0.4	0.4	0.5	0.3
γ	0.03	0.03	0.04	0.05
π(h)$	8	12	10	20

Autres données :

$$\beta_{DD} = \beta_{DU}$$

$$\mu_{DD} = 1/MTTR$$

BIBLIOGRAPHIE

[1] F. Wang, O. Yang, R. Zhang, et L. Shi, « Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database », *J. Loss Prev. Process Ind.*, vol. 44, n° Supplement C, p. 212- 222, 2016.

[2] « IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems ». 2010.

[3] « IEC 61511: Functional safety – Safety instrumented systems for the process industry sector ». 2016.

[4] D. J. Satur, J. Kim, M. Bae, S.-Y. Kim, et Y. Lee, « Cost effective alternative in meeting the required Safety Integrity Level (SIL) », *J. Loss Prev. Process Ind.*, vol. 40, n° Supplement C, p. 406- 418, 2016.

[5] Y. Dutuit, F. Innal, A. Rauzy, et J.-P. Signoret, « Probabilistic assessments in relationship with safety integrity levels by using Fault Trees », *Reliab. Eng. Syst. Saf.*, vol. 93, n° 12, p. 1867- 1876, 2008.

[6] Y. Liu et M. Rausand, « Reliability assessment of safety instrumented systems subject to different demand modes », *J. Loss Prev. Process Ind.*, vol. 24, n° 1, p. 49- 56, 2011.

[7] F. Innal, M. A. Lundteigen, Y. Liu, et A. Barros, « A PFDavg generalized formulas for SIS subject to partial and full periodic test based on multi-phase Markov Chain Models », *Reliab. Eng. Saf. Syst.*, vol. 150, p. 160- 170, 2016.

[8] W. Mechri, C. Simon, et K. BenOthman, « Switching Markov chains for a holistic modeling of SIS unavailability », *Reliab. Eng. Syst. Saf.*, vol. 133, p. 212‑ 222, janv. 2015, doi: 10.1016/j.ress.2014.09.005.
[9] G. Kaczor, S. Mlynarski, et M. Szkoda, « Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams », *J. Loss Prev. Process Ind.*, vol. 41, n° Supplement C, p. 31‑ 39, 2016.
[10] M. Chebila et F. Innal, « Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH », *J. Loss Prev. Process Ind.*, vol. 34, n° Supplement C, p. 167‑ 176, 2015.
[11] J.-P. Signoret, Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, et P. Thomas, « Make your Petri nets understandable: Reliability block diagrams driven Petri nets », *Reliab. Eng. Syst. Saf.*, vol. 113, n° 0, p. 61‑ 75, 2013.
[12] S. Barua, X. Gao, H. Pasman, et M. S. Mannan, « Bayesian network based dynamic operational risk assessment », *J. Loss Prev. Process Ind.*, vol. 41, n° Supplement C, p. 399‑ 410, 2016.
[13] M. Catelani, L. Ciani, et V. Luongo, « A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application », *Microelectron. Reliab.*, vol. 51, p. 1503‑ 1507, 2011.
[14] P. Hokstad, « Demand rate and risk reduction for safety instrumented systems », *Reliab. Eng. Syst. Saf.*, vol. 127, n° 0, p. 12‑ 20, 2014.

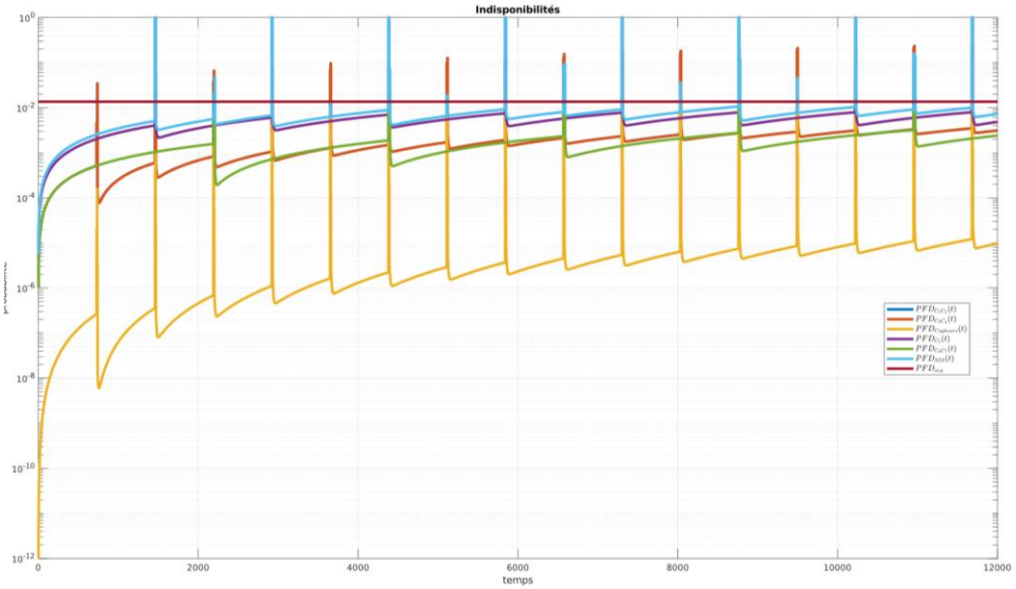


Fig. 10. Insponibilité instantanée du système et des différents éléments

[15] J. Zhang, Y. Liu, M. A. Lundteigen, et L. Bouillaut, « Using Bayesian networks to quantify the reliability of a subsea system in the early design », in *ESREL 2016 - Risk, Reliability and Safety: Innovating Theory and Practice*, Glasgow, Scotland, 2016, p. 404‑ 411.
[16] W. Mechri, C. Simon, F. Bicking, et K. Ben Othman, « Probability of failure on demand of safety systems by Multiphase Markov Chains », in *2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, oct. 2013, p. 98‑ 103, doi: 10.1109/SysTol.2013.6693839.
[17] Y. Shu et J. Zhao, « A simplified Markov-based Approach for Safety Integrity level verification », *J. Loss Prev. Process Ind.*, vol. 29, p. 262‑ 266, mai 2014.
[18] P. Hokstad et M. Rausand, « Common cause failure modeling : status and trends », in *Handbook of Performability Engineering*, K. B. Misra, Éd. Springer London, 2008, p. 621‑ 640.
[19] S. Wu, L. Zhang, M. A. Lundteigen, Y. Liu, et W. Zheng, « Reliability assessment for final elements of {SISs} with time dependent failures », *J. Loss Prev. Process Ind.*, p., 2017.
[20] A. C. Torres-Echeverria, S. Martorell, et H. A. Thompson, « Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm », *Reliab. Eng. Syst. Saf.*, vol. 106, p. 45‑ 60, 2012.
[21] F. Brissaud, A. Barros, et C. Bérenguer, « Probability of failure on demand of safety systems: impact of partial test distribution », *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 226, n° 4, p. 426‑ 436, 2012.
[22] Y. Liu et M. Rausand, « Proof testing strategies induced by dangerous detected failures of safety Instrumented systems », *Reliab. Eng. Syst. Saf.*, vol. 145, p. 366‑ 372, 2016.
[23] Y. Wang et M. Rausand, « Reliability analysis of safety-instrumented systems operated in high-demand mode », *J. Loss Prev. Process Ind.*, vol. 32, n° Supplement C, p. 254‑ 264, 2014.
[24] A. C. Torres-Echeverria, S. Martorell, et H. A. Thompson, « Modelling and optimization of proof testing policies for safety instrumented systems », *Reliab. Eng. Syst. Saf.*, vol. 94, n° 4, p. 838‑ 854, avr. 2009.
[25] F. Brissaud et D. Turcinovic, « Functional Safety for Safety-Related Systems: 10 Common Mistakes. », in *25th European Safety and Reliability Conference*, Zurich, Switzerland, 2015, vol. Safety and Reliability of Complex Engineered Systems.
[26] W. Mechri, C. Simon, et K. B. Othman, « Uncertainty analysis of common cause failure in Safety Instrumented Systems », *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 225, n° 4, p. 450‑ 460, 2012.
[27] W. Mechri, C. Simon, K. B. Othman, et M. Benrejeb, « Uncertainty evaluation of Safety Instrumented Systems by using Markov chains », in *Proceedings of 18th IFAC World Congress, Milano, Italy*, 2011, p. 7719‑ 7724.
[28] J. L. Rouvroye et J. A. M. Wiegerinck, « Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations », *ISA Trans.*, vol. 45, n° 4, p. 611‑ 621, 2006.
[29] K. Murphy, « Dynamic Bayesian Networks: Representation, Inference and Learning », PhD Thesis, Dept. Computer Science. UC, Berkeley, 2002.
[30] J. Pearl, *Probabilistic reasoning in intelligent systems: networks of plausible inference*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1988.
[31] H. Boudali et J. B. Dugan, « A discrete-time Bayesian network reliability modeling and analysis framework », *Reliab. Eng. Syst. Saf.*, vol. 87, p. 337–349, 2005.
[32] P. Weber et C. Simon, *Benefits of Bayesian networks Models*. ISTE-Wiley, 2016.
[33] C. Simon, W. Mechri, et G. Capizzi, « Assessment of Safety Integrity Level by simulation of Dynamic Bayesian Networks considering test duration », *JLPPI*, vol. 57, p. 101‑ 113, 2019.