Prise en compte de la performance des proof tests sur celle des systèmes instrumentés de sécurité

Walid Mechri, Christophe Simon, Frédérique Bicking, Kamel Ben Othman

Prise en compte de la performance des proof tests sur celle des systèmes instrumentés de sécurité

Christophe Simon, Frédérique Bicking
Centre de Recherche en Automatique de Nancy,
Université de Lorraine, CNRS UMR 7039,
Bd des Aiguillettes, 54506, Vandœuvre lès Nancy, France
@ : {christophe.simon ;frederique.bicking}@univ-lorraine.fr

Walid Mechri, Kamel Ben Othman
Ecole Nationale d'Ingénieurs de Tunis,
LARA-Automatique, LR-11-ES18,
Le Belvédère, 1002 Tunis, Tunisie
@ : walid.mechri@isim.rnu.tn, kamel.benothman@enim.tn

***Résumé*—Cet article propose une approche pour analyser l'effet des proof tests dans l'évaluation de la performance des systèmes instrumentés de sécurité (SIS). L'analyse est basée sur les chaînes de Markov multiphases intégrant plusieurs paramètres tels que les défaillances de causes communes (DCC), le taux de couverture de diagnostic, les proofs tests, etc. Nous accordons une attention particulière à la performance et à l'efficacité des proof tests. Les concepts de base des chaînes de Markov multiphases sont introduits et appliquées. Un modèle de calcul d'indisponibilité pour une étude de cas est présenté montrant l'effet de la performance des proof tests sur celle du système de sécurité.**

I. Introduction

Dans plusieurs domaines d'application, il est nécessaire de réduire les conséquences des évènements dangereux qui pourraient générer des sources potentielles de dangers pour l'environnement ou la santé des personnes. L'objectif des systèmes de sécurité est de couvrir ces risques potentiels. Un système de sécurité doit fournir une couche indépendante de protection par la mise en œuvre de fonctions de sécurité à l'aide de différentes techniques. Dans ce contexte, la norme IEC 61508 [1] est un guide pour la conception, la validation et la vérification de la fonction de sécurité réalisée par un système Electrique/Electronique/Electronique Programmable (E/E/PES). Un E/E/PES est utilisé comme un SIS pour mettre en œuvre la Fonction Instrumentée de Sécurité (SIF) [2].

La performance du SIS s'apparente à un calcul d'indisponibilité de la fonction de sécurité lors de sa sollicitation. Cette performance est définie par 4 niveaux d'intégrité de sécurité (SIL) [3] grâce au calcul d'un paramètre probabiliste. Deux principaux indices sont utilisés pour la qualification des SIS. La probabilité moyenne de défaillance à la demande (PFD_{avg}) est utilisé en mode faible demande [3], [4] et la probabilité de défaillance par heure (PFH) est utilisé pour un SIS en mode de forte demande [5]. Les SIS en mode faible demande font l'objet de cet article.

L'indisponibilité des SIS doit être prouvée préférentiellement par des modèles quantitatifs à partir de méthodes référencées telles que les arbres de défaillance [3], les blocs diagrammes de fiabilité [6] ainsi que les chaînes de Markov [7], [8] ou les réseaux de Petri [9] par exemple. La performance ainsi calculée permet la classification/qualification selon les SIL définis dans la norme IEC 61508 [1]. Dans ce cadre, la méthode des chaînes de Markov apporte une bonne formalisation de tous les états que peuvent prendre ces systèmes faiblement sollicités en fonction des événements rencontrés et des paramètres étudiés. Cette méthode apporte une finesse de modélisation pertinente au regard du comportement des SIS étudiés. En outre, l'explosion combinatoire des états qui est l'inconvénient majeure des chaînes de Markov est généralement surmontable compte tenu de la relative complexité des SIS mais requiert une attention soutenue relative aux nombreuses transitions. Par ailleurs, l'emploi d'une chaîne de Markov à temps discret est pertinent vis à vis de la prise en compte des instants de test. L'utilisation d'une méthode simulation de la chaîne de Markov pour obtenir l'évaluation de performance requise est fort utile.

Dans cet article, nous proposons d'utiliser l'approche des chaînes de Markov multiphases pour analyser les systèmes de sécurité en faible demande pour tenir compte des proof tests. L'article propose notamment l'intégration des paramètres suivants : les défaillances dangereuses, les défaillances de cause commune, l'intervalle de test, la probabilité de défaillance à cause du test γ, ou la probabilité de ne pas détecter une panne lors d'un test ξ, en une seule équation afin d'évaluer la performance des SIS périodiquement testés par simulation. Dans la section II, nous rappelons les éléments de base des SIS et leurs paramètres caractéristiques. La section III est consacrée aux modèles de Markov et leurs extensions aux chaînes de Markov multiphases afin de calculer la PFD_{avg} des SIS. La section IV est dédiée à une illustration par l'étude d'un SIS supervisant un réacteur chimique [8].

II. Système Instrumenté de sécurité

Un SIS est un système visant à mettre le procédé qu'il surveille en position de repli de sécurité, c'est-à-dire 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. Un SIS est composé de trois parties, une partie capteur, une partie unité logique de traitement et une partie actionneur. Un SIS est en mode faible demande si sa sollicitation est inférieure ou égale à 1 an^{-1} et en mode demande élevée sinon [1], [10].

La norme IEC 61508 [1] est devenue la norme de référence pour la spécification et la conception des systèmes instru-

mentés de sécurité (SIS). Sa déclinaison sectorielle dans le domaine du process industriel est destinée aux concepteurs et utilisateurs de ce domaine. Ces normes de sécurité fonctionnelle [1] introduisent une approche probabiliste pour l'évaluation quantitative de la performance du système instrumenté de sécurité et la qualification de cette performance par des niveaux de sécurité référencés. L'introduction de probabilités dans l'évaluation du niveau d'intégrité a entraîné la mise en place de concepts tels que les notions de calculs de la probabilité de défaillance à la sollicitation (PFD_{avg}).

La norme IEC 61508 [1] relative à l'évaluation de performance des systèmes instrumentés de sécurité établit la classification des systèmes étudiés selon 4 niveaux définis dans le tableau I à partir du calcul de la probabilité moyenne de défaillance à demande PFD_{avg} (en faible sollicitation).

TABLE I: Niveau de SIL pour le mode faible demande [1]

SIL	PFD_{avg}
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

La norme IEC 61508 [1] permet de donner les principaux éléments pour estimer la PFD_{avg} due aux défaillances aléatoires du matériel. Les calculs d'évaluation de la performance peuvent considérer un grand nombre de paramètres tels que les taux de défaillance des composants, intervalle de test, le temps moyen de réparation (MTTR), le taux *DC*, le facteur DCC et les caractéristiques des proof tests.

A. Couverture de diagnostic

La norme IEC 61508[1] définit le taux de couverture pour les tests de diagnostic comme étant le rapport du taux de défaillance des pannes dangereuses détectées λ_{DD} (par un test de diagnostic) sur le taux de défaillance total des pannes dangereuses λ_D (détectées et non détectées). Ainsi, l'équation 1 peut être formulée.

$$DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \tag{1}$$

Comme l'objectif est de déterminer la probabilité de défaillance dangereuse, seuls les taux de défaillances dangereuses des modules des composants des architectures étudiées seront étudiés. Le taux de couverture intervient dans la détermination des taux de défaillances dangereuses détectées λ_{DD} et dangereuses non détectées λ_{DU} connaissant le taux de défaillance du composant. D'après 1, il vient :

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

Par ailleurs, le calcul de la PFD_{avg} doit tenir compte du taux de défaillance des composants et du facteur de défaillance de cause commune (DCC) [7]. L'importance des DCC a été mentionnée dans de nombreux travaux. Par exemple, [11], [12] discute de cette importance dans l'évaluation de performance des SIS [13], [5].

B. Défaillances de Cause Commune

Les défaillances de cause commune ou de mode commun peuvent être introduites dans les calculs de probabilité de défaillance de façon directe. Les paramètres de calcul sont obtenus à partir de données de retour d'expérience ou dans des bases de données. Toutefois, ce dernier cas ne concerne que le domaine du nucléaire. Ces données sont assez difficiles à obtenir aussi des modèles paramétriques ont été développés. Plusieurs modèles sont envisageables notamment le modèle β [14], la méthode PDS de chez syntex [15], le modèle des multiples lettres grecques (MLG), ou encore le modèle α [16]. Dans cet article, nous avons privilégié le modèle β en raison de sa complexité raisonnable et sa faible exigence en paramètres mais aussi parce qu'il est cité dans la norme.

Selon le modèle β, le taux de défaillance total (λ_T) d'un composant est la somme de ses taux de défaillances indépendantes (λ^I) et de DCCs (λ^C). Ainsi, il vient l'équation 3 :

$$\lambda^T = \lambda^I + \lambda^C = (1 - \beta).\lambda^T + \beta.\lambda^T \tag{3}$$

où β est défini comme la probabilité d'une défaillance de cause commune, sachant la présence d'une défaillance [12], [13]. L'expression du facteur β est donné comme suit :

$$\beta = \frac{\lambda^C}{\lambda^C + \lambda^I} = \frac{\lambda^C}{\lambda^T} \tag{4}$$

Comme l'objectif est de déterminer la valeur de PFD_{avg}, seuls les taux de défaillances dangereuses des composants seront considérés. Ainsi, les différents taux de défaillances dangereuses détectées et non détectées s'écrivent :

$$\begin{cases} \lambda^I_{DD} = (1 - \beta_D).\lambda_{DD} = (1 - \beta_D).DC.\lambda_D \\ \lambda^C_{DD} = \beta_D.\lambda_{DD} = \beta_D.DC.\lambda_D \\ \lambda^I_{DU} = (1 - \beta_U).\lambda_{DU} = (1 - \beta_U).(1 - DC).\lambda_D \\ \lambda^C_{DU} = \beta_U.\lambda_{DU} = \beta_U.(1 - DC).\lambda_D \end{cases} \tag{5}$$

où β_D et β_U représentent respectivement la proportion de DCC détectées et non détectées liée au taux *DC* [17].

C. Stratégies de proof tests

Pour la vérification des SIS plusieurs types de tests ont été définis et peuvent être classés en fonction de leur mode de réalisation (*i.e.* en ligne ou hors ligne). Les tests de diagnostic sont des tests en ligne qui permettent de détecter essentiellement les défaillances aléatoires d'un composant ou un module de système. Elles sont caractérisées par le taux de couverture *DC*. L'hypothèse est faite que la détection est immédiate [5]. Les proof test (tests hors ligne), qui eux sont des tests d'inspection périodiques sont effectuées pour détecter les défaillances latentes d'un système en fonctionnement *i.e.* non détectées. Lorsque les défaillances latentes sont détectées, nous considérons que le système est rétabli dans un état de fonctionnement 'aussi bon que neuf' ou aussi proche que possible de celui-ci [1].

Généralement le proof test est considéré comme parfait. Cela signifie que toutes les défaillances latentes non détectées

sont révélées et réparées. En outre, l'hypothèse est faite que la réparation est réalisée pendant le test. Mais la réalité nous fait dire que le test peut être imparfait, c'est-à-dire qu'il n'est pas capable de révéler tous les types de défaillances non détectées, ou il est effectué sous des conditions qui diffèrent d'une situation de demande réelle. Dans ce cas, nous définissons ξ comme la probabilité conditionnelle qu'une défaillance non détectée ne soit pas détectée par le proof test étant donné que le défaut se produit lors du lancement du proof test. Par conséquent $(1-\xi)$ représente la capacité du proof test à révéler les défaillances latentes. Un proof test est parfait si $\xi = 0$ puisque toutes les défaillances non détectées sont révélées, et un proof test est imparfait si $\xi > 0$. Certains analystes fournissent une estimation de ξ dans le manuel de sécurité. Cette estimation est obtenue par exemple en effectuant une AMDEC détaillée afin d'évaluer la capacité du proof test à révéler les défaillances latentes.

Par ailleurs, beaucoup d'autres paramètres peuvent être pris en compte pour évaluer plus précisément la PFD_{avg} pour un SIS périodiquement testé. Nous trouvons, par exemple :

- μ, le taux de réparation.
- γ, la probabilité de défaillance due au test. Ce paramètre représente l'innocuité du proof test.
- π, la durée du test. Ce paramètre n'est pas considéré dans ce travail car il requiert une modélisation encore plus complexe que celle proposée ici.

Pour évaluer la PFD_{avg} des SIS, nous nous appuyons sur la méthode des chaînes de Markov pour représenter tous les états que peuvent prendre ces SIS en fonction des évènements rencontrés et des paramètres étudiés. Par exemple, il est possible de modéliser différents modes de défaillance des composants, des stratégies de test, des opérations de réparation, le taux *DC* et le facteur de DCC. Mais, la méthode des chaînes de Markov est fortement limitée par l'explosion combinatoire du nombre d'états, notamment parce que le processus de modélisation implique le recensement de tous les états accessibles et toutes les transitions entre ces états. Toutefois il est possible de faire des hypothèses raisonnables pour simplifier l'analyse.

D. Considérations et hypothèses de travail

Afin d'évaluer la PFD_{avg} pour les SIS périodiquement testés nous prenons en compte les considérations et hypothèses suivantes :

- Tous les composants des SIS ont des taux de défaillance λ constants [3].
- Les architectures d'un système de type M parmi N (MooN) sont soumises à des proof tests partiels ou complets [18], [19].
- Les proof tests complets permettent de détecter toutes les défaillances [19].
- Les proof tests partiels ne permettent de détecter que certaines défaillances [19].
- Tous les composants du système sont testés simultanément lors de chaque test. Cela signifie que nous n'exploitons qu'une stratégie de test.
- La probabilité de ne pas détecter une défaillance lors du test ξ (test de couverture) est considérée.
- La probabilité de défaillance à cause du test γ, (innocuité) est considérée.
- La durée du test est négligée [18].
- Le temps de réparation d'une défaillance relevée par un proof test est supposé négligeable car inclut dans la durée du proof test.
- Les défaillances détectées au cours d'un proof test sont réparées immédiatement et des mesures sont prises afin de maintenir l'EUC dans un état sûr, de telle sorte que les durées de tests ou de maintenances ne sont pas inclues dans la quantification de la PFD.
- Après chaque proof test/réparation, tous les composants du SIS sont dans une condition "aussi bon que neuf". [18].
- La défaillance de cause commune est représentée par le modèle du facteur β [11], [12].
- Les défaillances sont supposées rares et les trois couches d'un SIS sont supposées indépendantes.

III. ÉVALUATION DE L'INDISPONIBILITÉ

L'indisponibilité d'un SIS doit être quantitativement prouvée en utilisant des modèles adaptés. Aucun modèle particulier n'est recommandé dans la norme IEC 61508 ou dans la IEC 61511 [2]. Néanmoins, certains modèles bien connus sont cités dans les annexes. Parmi ces modèles, on trouve les arbres de défaillances [20], les blocs diagramme fiabilité [21] ainsi que les chaînes de Markov [3], [22], [19]. Dans ce contexte, les chaînes de Markov sont un modèle formel intéressant, où il faut identifier les différents états du système en tenant compte de tous les événements rencontrés ainsi que leurs paramètres caractéristiques [17], [7]. Les chaînes de Markov peuvent modéliser les effets dynamiques associés à des tests et opérations de maintenance. Les étapes de modélisation peuvent être lourdes et nécessitent une bonne compréhension du mécanisme de transition. L'emploi d'une chaîne de Markov à temps discret est pertinent vis à vis de la prise en compte des instants de test et l'utilisation d'une méthode simulation de la chaîne d'une Markov pour obtenir l'évaluation de performance requise est fort utile.

A. Chaînes de Markov

La modélisation par chaînes de Markov évoquées dans la norme IEC 61511 [2] est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants à taux de défaillance constant et réparable (pour la prise en compte des taux de réparation) [17]. Dans ce travail, les probabilités de transition de la chaîne de Markov sont considérées comme indépendantes du temps (processus homogène). Cette hypothèse est conforme lorsque l'on travaille dans la durée de vie utile (phase de maturité) des composants. Lors de l'utilisation des chaînes de Markov, il est également possible de tenir compte des dépendances et de faire une analyse dynamique du système [13].

Une chaîne de Markov est un modèle qui transite de l'état i à l'état j avec une probabilité q_{ij} qui ne dépend que des états i et j. La matrice $Q = (q_{ij})$ de dimension $(r \times r)$, représente la matrice de transition définie à partir des taux de transition q_{ij}. Soit $P(t) = (P_1(t), \ldots, P_r(t))$ le vecteur de probabilités des différents états où $P_j(t)$ représente la probabilité du système d'être dans l'état j à l'instant t. La loi de transition d'une chaîne de Markov est définie par l'équation suivante :

$$P(t) = P(t-1).Q \tag{6}$$

La matrice de transition Q est caractérisée par le fait que la somme de chacune de ses lignes est égale à un et chaque coefficient $q_{ij} \geq 0$. La probabilité d'être dans l'état j à l'instant t est calculée à partir de :

$$P_j(t) = \sum_i P_i(t-1).q_{ij} \tag{7}$$

L'indisponibilité du SIS est calculée par la somme des probabilités d'être dans l'état j à l'instant t à partir de l'équation 8. j correspondent aux états où le système de sécurité n'est pas en mesure de répondre à la demande.

$$PFD(t) = \sum_j P_j(t) \tag{8}$$

Mais, les SIS sont périodiquement testés et l'équation 7 ne convient pas à ce cas particulier. Les test provoquent une rupture de transition et génèrent des phases. L'équation 8 n'est valable que durant ces phases. Dans ce contexte, les chaînes de Markov multi-phases doivent leur être préférées.

B. Chaînes de Markov multi-phases

A l'aide d'un test, nous connaissons l'état des composants testés. L'état d'un SIS est connu ou partiellement connu à l'instant de test et donc, les probabilités des différents états sont connus. Le comportement du SIS testé périodiquement et partiellement, avec plusieurs périodes peut être facilement modélisé par une chaîne de Markov multi-phases [3].

Les chaînes de Markov multi-phases sont utiles lorsque la structure des états change à un instant connu ou lorsque l'état de certaines parties du système est connu à certains instants. Il s'agit d'une chaîne de Markov homogène par morceaux. Les phases de test modifie la structure de la matrice de transition ce qui réfute l'emploi de chaînes de Markov non homogènes. En outre, les chaînes de Markov multiphases conviennent parfaitement à la simulation et non à une résolution analytique.

Ainsi, les proof tests créent une nouvelle phase dans l'évolution de la chaîne de Markov. Généralement, un intervalle de test unique pour vérifier la fonction de sécurité de l'ensemble du système est considéré. Il est généralement supposé que les sous-systèmes sont fonctionnellement testés indépendamment les uns des autres [13]. Le SIS est alors considéré comme complètement arrêté pendant la période du test quel que soit le sous-système testé. Mais, certaines applications nécessitent l'utilisation des intervalles de test différents propres à chaque sous système du SIS et une chaîne de Markov multi-phases plus complexes doit alors être définie.

Un test parfait donne l'état exact des composants et donc celui du système. Ainsi, la répartition des états du système devrait être réaffectée selon cette connaissance [7] grâce à une matrice dite de passage. Si on considère un intervalle de test dans une stratégie de test unique, il existe donc une seule matrice de passage permettant l'affectation de la distribution de probabilités d'être dans les différents états aux instants d'inspection $(k.t_i)$ vers la distribution de probabilités aux instants $(k.t_i + \Delta t)$ [7].

$$P(k.T_i + \Delta T) = P(k.T_i).M \tag{9}$$

avec

— $k \in \mathbb{N}^+$, $T_i \in \mathbb{R}^+$ définissent les temps d'inspection et ΔT est la période de la chaîne de Markov.

— M est la matrice de passage entre deux phases consécutives à chaque instant de test $k.T_i$. Quand un test est effectué, M permet d'enchaîner les états en fonction de l'effet du test. Les paramètres ξ et γ sont impliqués dans la définition des coefficients de la matrice M. Les probabilités des états de la phase i sont utilisées pour calculer les probabilités initiales de la phase suivante $(i+1)$.

La fonction de la matrice de passage de la phase i à la phase $(i+1)$ est de spécifier la probabilité que l'état j à la fin de la phase i donnera un état k au début de phase $(i+1)$.

Comme le SIS est composé de plusieurs sous-systèmes et composants, et selon la stratégie de test choisi, il est possible que plusieurs matrices de transition M_i soient utilisés pendant le temps de la mission du SIS même si les inspections sont normalement répétées avec des intervalles de temps constants. Grâce aux précédentes équations 7 & 9 nous pouvons déterminer la probabilité de défaillance du SIS modélisé par une chaîne de Markov multi-phases en utilisant l'équation 10.

$$P(t) = \delta(t).P(t-1).M + (1-\delta(t)).\sum_i P_i(t-1).q_{ij} \tag{10}$$

avec $i, j, = 1, \ldots, r$ et $\delta(t) = \begin{cases} 1 & \text{if} \quad t = k.T_i \\ 0 & \text{if} \quad t \neq k.T_i \end{cases}$

$\delta(t)$ est une fonction indicatrice qui assure la commutation entre les matrices Q et M à l'instant du test $k.T_i$. La PFD du SIS est calculée selon l'équation 8, où j représente les probabilités des états où le système de sécurité n'est pas en mesure de répondre à la demande. A l'aide de l'équation 10, nous pouvons simuler la chaîne de Markov et déterminer la PFD instantanée [7]. La PFD_{avg} est ensuite calculée par une intégration en temps discret à l'aide de l'équation 11 :

$$PFD_{avg}(k.\Delta T) = \frac{1}{k.\Delta T}.\sum_{n=0}^{k}\sum_j P_j(n.\Delta T).\Delta T \tag{11}$$

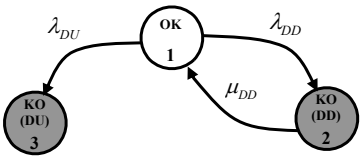
avec $k.\Delta T \in [0, T_M]$, T_M le temps de mission, j les états de défaillances dangereuses, et $P_j(n)$ la probabilité d'être dans un de ces états à l'instant $n.\Delta T$. La qualification de

la performance du SIS est alors obtenue par référence aux données du tableau I.

C. Analyse du système 1oo1

A titre d'illustration, nous utilisons un système 1oo1 et nous ne donnerons pas l'ensemble des matrices et graphes de Markov pour des systèmes plus compliqués (cf. [23]).

Le système 1oo1 est modélisé par une chaîne de Markov multi-phases présentée à la figure 1. La signification des nœuds est également jointe.



état	Description
1	OK
2	Défaillance détectées
3	Défaillance non détectées

FIGURE 1: Modèle de Markov multi-phases relatif au système 1oo1

Chaque intervalle de test constitue une phase au cours de laquelle le fonctionnement du système 1oo1 est décrit par le processus de Markov à 3 états dont la matrice de transition est donnée à l'équation 12. Compte tenu des faibles valeurs des taux utilisés dans cette matrice de transition, il est possible d'utiliser l'approximation usuelle $\lambda \approx e^{-\lambda.\Delta T}$. La matrice Q est ainsi valable.

$$Q = \begin{bmatrix} 1-(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & 1-\mu_{DD} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (12)$$

Au moment du test, les phases sont enchaînées comme cela est illustré à la figure 2.

- Considérons le système dans l'état 1 (*i.e.* état de marche) avant le test (phase i), alors :
  - il reste à l'état 1 avec une probabilité égale à $(1-\gamma)$, *i.e.* que le test n'a pas causé la défaillance du système.
  - il passe à l'état 2, avec une probabilité égale à $\gamma.(1-\xi)$, *i.e.* que le test a provoqué la défaillance du système, et cette défaillance a été détectée. Une fois détectée, elle sera réparée.
  - il passe à l'état 3, avec une probabilité égale à $\gamma.\xi$, *i.e.* que le test a provoqué la défaillance du système, et cette défaillance n'a pas été détectée.
- Si le système était dans l'état 2 (état de panne) avant le test. Le système reste en panne et les défaillances sont immédiatement détectées (DD), puis réparées. La probabilité de rester dans l'état 2 est donc égale à 1.
- Si le système était dans l'état 3 (état de panne) avant le test. Le système reste en panne. Les défaillances restent cachées et ne seront détectées (DU) qu'à l'occasion du prochain test périodique ou d'une demande. Dans ce cas :

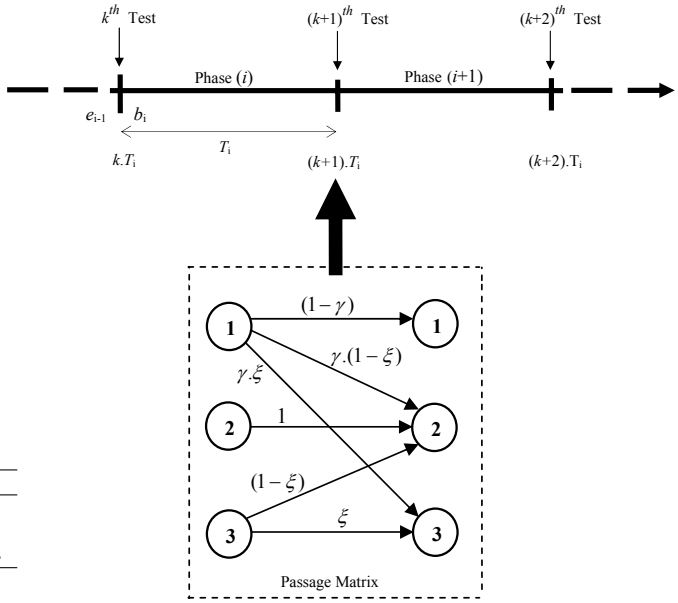


FIGURE 2: Principe du modèle de Markov multi-phases

- soit la chaîne de Markov passe dans l'état 2, avec une probabilité égale à $(1-\xi)$, *i.e.* que le test effectué permet de détecter la défaillance, puis réparée.
- soit elle reste dans l'état 3 avec une probabilité égale à ξ, *i.e.* que le test effectué n'a pas détecté la défaillance.

Les valeurs des probabilités d'occupation des états au début d_i de la phase i sont déduites de celles obtenues au terme f_{i-1} de la phase $(i-1)$ de la manière suivante :

$$\begin{aligned} P_1(b_i) &= (1-\gamma).P_1(e_{i-1}) \\ P_2(b_i) &= \gamma.(1-\xi).P_1(e_{i-1}) + P_2(e_{i-1}) + (1-\xi).P_3(e_{i-1}) \\ P_3(b_i) &= \gamma.\xi.P_1(e_{i-1}) + \xi.P_3(e_{i-1}) \end{aligned} \quad (13)$$

La matrice de passage M entre phases est donnée par l'équation 14 :

$$M = \begin{bmatrix} 1-\gamma & \gamma.(1-\xi) & \gamma.\xi \\ 0 & 1 & 0 \\ 0 & 1-\xi & \xi \end{bmatrix} \quad (14)$$

M est la matrice de passage utilisée uniquement à chaque instant de temps $k.T_i$, telle que la somme de chacune de ses lignes est égale à un et chaque coefficient m_{ij} est supérieur ou égale à 0.

La démarche d'analyse menée sur une architecture 1oo1 et conduisant aux équations 10 et 14 peut être étendue à d'autres configuration des systèmes relatif à la sécurité, tels que les architectures 1oo2 et 1oo3 [23]. Selon la stratégie de test choisi, il est possible d'associer à chaque configuration architecturale sa propre matrice de passage M pendant le temps de la mission du SIS, en tenant compte du fonctionnement de chaque architecture.

IV. APPLICATION : ÉTUDE D'UN SYSTÈME DE SÉCURITÉ

Le système présenté à la figure 3 a été étudié dans [8] et est utilisé comme illustration de l'approche proposée. Les chaînes de Markov multi-phases sont appliquées à un système de protection contre la sur-pression et l'excès de température d'un réacteur chimique. Le système est composé de quatre sous-systèmes : Transmetteur de température (TT), transmetteur de pression (PT), unité logique (LS) et l'élément de contrôle final (FC). Lors de la détection d'un dépassement de température ou de pression, le système de sécurité coupe l'alimentation du réacteur pour éviter une réaction d'emballement [8].

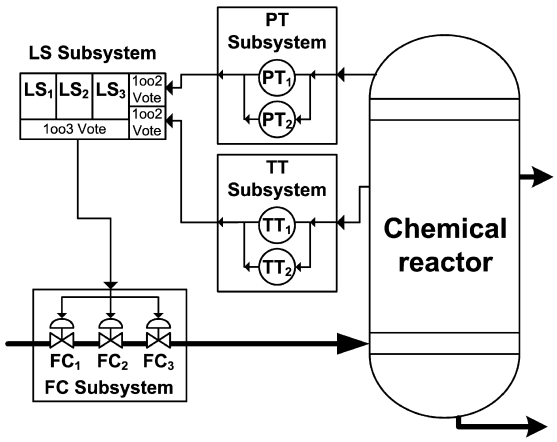


FIGURE 3: Système de protection d'un réacteur chimique

Le système étudié est composé ainsi de :

— La partie capteur constituée de deux transmetteurs : Transmetteur de température (TT) et transmetteur de pression (PT) structurés en 1oo2.

— La partie unité logique (Logic Solver) structurée en architecture 1oo3.

— La partie actionneur en architecture 1oo3 constituée de trois vannes.

Le bloc-diagramme de fiabilité du SIS est donné à la figure 4.

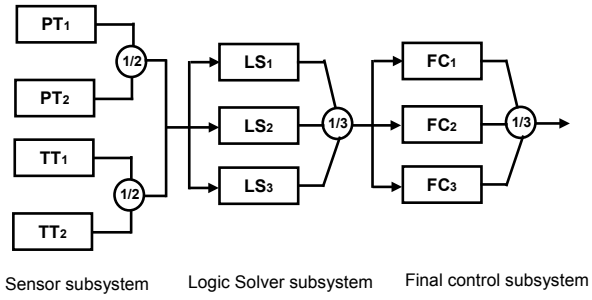


FIGURE 4: Bloc-diagramme de fiabilité du SIS

Chaque sous-système peut avoir un ou plusieurs canaux. Un canal est une structure d'un ou de plusieurs composants et peut exécuter indépendamment une fonction de sécurité de canal. En utilisant la méthode des chaînes de Markov multi-phases proposée dans cet article, la PFD_{avg} du SIS est déterminée à partir des paramètres caractéristiques des composants. T_i (interval de proof test), λ_D (taux de défaillance), DC, β_D (proportion de DCC détectées), β_U (proportion de DCC non détectées), MTTR, ξ et γ. Les valeurs numériques des paramètres caractéristiques des composants du SIS sont donnés dans le tableau II.

TABLE II: Données numériques

Parameters \ Components	PT_i	TT_i	LS_i	FC_i
$\lambda_D(\times 10^{-6}/h)$	5.00	5.00	4.60	5.00
DC	0.3	0.3	0.4	0.5
$\beta_U(\%)$	20	20	10	10
MTTR (h)	8	8	10	10
$\text{T}_i(h)$	730	730	1460	2190
ξ	0.4	0.4	0.5	0.3
γ	0.03	0.03	0.04	0.05
Others data :				
$\beta_D = \frac{1}{2}.\beta_U$				
$\mu_{DD} = \frac{1}{MTTR}$				

La PFD du SIS est calculée par la combinaison de la probabilité de défaillance de tous les sous-systèmes assurant ensemble la fonction de sécurité (cf. eq.15). Elle est exprimée par la formule suivante sous l'hypothèse d'événements rares :

$$PFD = PFD_{LS} + (PFD_{TT}.PFD_{PT}) + PFD_{FC} \qquad (15)$$

où PFD_{LS}, PFD_{TT}, PFD_{PT} et PFD_{FC} sont respectivement la probabilité de défaillance de l'unité logique, du système de transmetteurs de température, du système de transmetteurs de pression et du système d'actionnement.

Pour calculer la PFD_{avg}, un intervalle de temps T_i lié à la fréquence de test du SIS est défini pour chaque sous-système. Nous supposons que l'on teste fonctionnellement chaque sous-système indépendamment les uns des autres. Ainsi, la complexité du problème de modélisation n'augmente pas puisque chaque sous-système peut être étudié indépendamment.

En utilisant la méthode des chaînes de Markov multi-phases proposée, la PFD instantanée est déterminée à partir des paramètres caractéristiques de ses composants, en utilisant l'équation 15. Alors, la PFD_{avg} est obtenue en calculant la moyenne des valeurs de points de la PFD, comme indiqué par l'équation 11.

La figure 5 montre l'évolution de l'indisponibilité du SIS étudié, ainsi que sa valeur moyenne PFD_{avg}. Deux cas de simulation ont été considérés pour montrer l'influence des paramètres γ et ξ. Dans le premier cas (cf.Fig. 5), les deux paramètres sont négligés. Le deuxième cas (cf. Fig. 6) décrit la contribution des paramètres proposés.

Ces figures montrent l'évolution de l'indisponibilité instantanée du SIS (en bleu) ainsi que sa valeur moyenne PFD_{avg} (en rouge). Les instants de test sont reconnaissables sur la PFD instantanée où des changements de valeurs brutales sont mis en évidence. La valeur de la PFD_{avg} varie de 0.955×10^{-3} (1^{er} cas) à 1.253×10^{-3} ($2^{ème}$ cas).

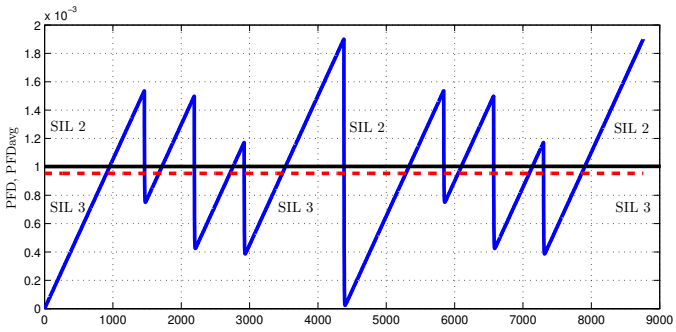


FIGURE 5: La PFD(t) et la PFD_{avg} du SIS dans le 1^{er} cas

Le SIL correspondant du SIS étudié varie d'un niveau SIL 3 ($\text{PFD}_{avg} \in [10^{-3}, 10^{-2}[$) à un niveau de SIL 2 ($\text{PFD}_{avg} \in [10^{-2}, 10^{-1}[$) selon le tableau I. La variation des paramètres ξ et γ amène donc à un changement significatif sur la qualification du niveau de SIL du SIS.

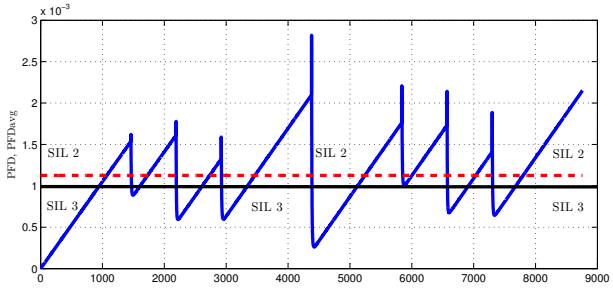


FIGURE 6: La PFD et la PFD_{avg} du SIS dans le $2^{ème}$ cas

L'approche proposée montre comment l'efficacité et la performance des proof tests a une influence significative sur la valeur moyenne de l'indisponibilité du système et la qualification du SIS alors que ces paramètres sont souvent négligés en pratique car ils sont difficiles à quantifier.

V. CONCLUSION

Dans cette étude, une nouvelle application des chaînes de Markov multi-phases pour la modélisation et l'analyse des systèmes instrumentés de sécurité est proposée. Il s'agit d'une approche holistique en mesure de tenir compte de nombreux paramètres et notamment des proofs tests dont l'influence sur la performance du SIS ne doivent pas être négligée. Toutefois, elle nécessite beaucoup d'efforts pour l'analyste afin d'éviter les erreurs de modélisation.

L'originalité de cet article réside dans le fait que la performance du SIS est modélisée par une unique équation en tenant compte de nombreux paramètres, tels que, les défaillances dangereuses, la couverture de diagnostic, les défaillances de cause communes, les proof tests, le taux de réparation, la probabilité de défaillance due au test et la probabilité de ne pas détecter une défaillance lors d'un test. La chaînes de Markov multi-phases est simulée pour évaluer la performance des systèmes de sécurité fonctionnant en mode faible demande.

Nous attachons une attention particulière à la performance des proof tests (performace γ et l'innocuité ξ). Les paramètres γ et ξ s'intègrent directement dans la matrice de passage des chaînes de Markov multi-phases pour former des matrices types réutilisables selon l'architecture choisie.

L'approche développée produit des estimations fines de l'indisponibilité, puisque les taux de défaillance de tous les composants du système ainsi que les effets des proofs tests sont pris en compte dans le processus d'évaluation. La nature complexe de ces paramètres rend cependant leur quantification plus difficile et incertaine. Les simulations montrent clairement que les deux paramètres γ et ξ influencent les résultats du niveau de SIL du SIS.

La méthode des chaînes de Markov multi-phases a été appliquée à un exemple simple de type 1001 à titre de l'illustration puis à un SIS d'une complexité certaine. L'analyse a été relativement compliquée et à demander un effort et un vigilance accrue. Dans le cas de la modélisation des systèmes complexes, le nombre d'états du modèle de Markov augmente avec le nombre de composants du système et nous devons donc essayer de réduire le nombre d'états chaque fois que possible. Pour éviter ce problème, le système de sécurité complexes peut être découpé en sous-systèmes dans l'esprit de ce qui a été fait ici lorsque cela est possible.

RÉFÉRENCES

[1] IEC61508, *Functional safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. Part 1-7*, International Electrotechnical Commission Std., 2010.

[2] IEC61511, *Functional safety Safety instrumented systems for the process industry sector*, IEC Std., 2000.

[3] Y. Dutuit, F. Innal, A. Rauzy, and J.-P. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using fault trees," *Reliability Engineering & System Safety*, vol. 93, no. 12, pp. 1867 – 1876, 2008, 17th European Safety and Reliability Conference.

[4] A. Torres-Echeverria, S. Martorell, and H. Thompson, "Multi-objective optimization of design and testing of safety instrumented systems with moon voting architectures using a genetic algorithm," *Reliability Engineering & System Safety*, vol. 106, no. 0, pp. 45 – 60, 2012.

[5] H. Jin, M. A. Lundteigen, and M. Rausand, "New pfh-formulas for k-out-of-n :f-systems," *Reliability Engineering and Safety System*, vol. 111, no. 0, pp. 112 – 118, 2013.

[6] M. Catelani, L. Ciani, and V. Luongo, "A simplified procedure for the analysis of safety instrumented systems in the process industry application," *Microelectronics Reliability*, vol. 51, pp. 1503 – 1507, 2011.

[7] W. Mechri, C. Simon, F. Bicking, and K. B. Othman, "Fuzzy multiphase markov chains to handle uncertainties in safety systems performance assessment," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 4, pp. 594–604, 2013.

[8] A. Torres-Echeveria, S. Martorell, and H. Thompson, "Modeling safety instrumented systems with moon voting architectures addressing system reconfiguration for testing," *Reliability Engineering and System Safety*, vol. 96, no. 5, pp. 545 – 563, 2011.

[9] J.-P. Signoret, Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, and P. Thomas, "Make your petri nets understandable : Reliability block diagrams driven petri nets," *Reliability Engineering and Safety System*, vol. 113, no. 0, pp. 61–75, 2013.

[10] J. Bukowski, "Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems," *IEEE Transactions on Reliability*, vol. 50, no. 3, pp. 321–329, 2001.

[11] P. Hokstad and M. Rausand, "Common cause failure modeling : status and trends," in *Handbook of Performability Engineering*, K. B. Misra, Ed. Springer London, 2008, ch. 39, pp. 621–640.

[12] M. A. Lundteigen and M. Rausand, "Common cause failures in safety instrumented systems on oil and gas installations : Implementing defense measures through function testing," *Journal of Loss Prevention in the Process Industries*, vol. 20, no. 3, pp. 218 – 229, 2007.

[13] W. Mechri, C. Simon, K. BenOthman, and M. Benrejeb, "Uncertainty evaluation of safety instrumented systems by using markov chains," in *Proceedings of 18th IFAC World Congress, Milano, Italy*, 2011, pp. 7719–7724.

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

[15] S. Hauge, P. Hokstad, H. Langseth, and K. Oien, *Reliability Prediction Method for Safety Instrumented Systems*. SINTEF, 2006.

[16] A. Mosleh and N. Siu, "A multiparameter event based common cause failure model," *Proceedings of the 9th international conference on structural mechanics in reactor technology*, no. 2, pp. 147–152, 1987.

[17] Y. Langeron, A. Barros, A. Grall, and C. Bérenguer, "Combination of safety integrity levels (sils) : A study of iec61508 merging rules," *Journal of Loss Prevention in the Process Industries*, vol. 21, no. 4, pp. 437 – 449, 2008.

[18] F. Brissaud, A. Barros, C. Bérenguer, and D. Charpentier, "Reliability analysis for new technology-based transmitters," *Reliability Engineering and System Safety*, vol. 96, no. 2, pp. 299 – 313, 2011.

[19] J. L. Rouvroye and J. A. Wiegerinck, "Minimizing costs while meeting safety requirements : Modeling deterministic (imperfect) staggered tests using standard markov models for sil calculations," *ISA Transactions*, vol. 45, no. 4, pp. 611 – 621, 2006.

[20] W. Mechri, C. Simon, and K. BenOthman, "Uncertainty analysis of common cause failure in safety instrumented systems," *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, vol. 225, no. 4, pp. 450–460, 2012.

[21] H. Guo and X. Yang, "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering and System Safety*, vol. 92, no. 9, pp. 1267 – 1273, 2007.

[22] H. Jin, M. A. Lundteigen, and M. Rausand, "Reliability performance of safety instrumented systems : A common approach for both low- and high-demand mode of operation," *Reliability Engineering and System Safety*, vol. 96, no. 3, pp. 365 – 373, 2011.

[23] W. Mechri, C. Simon, and K. Ben Othman, "Switching Markov chains for a holistic modeling of SIS unavailability," *Reliability Engineering and System Safety*, vol. 133, pp. 212–222, Jan. 2015. [Online]. Available : https ://hal.archives-ouvertes.fr/hal-01071409