7e Conférence Internationale de MOdélisation et SIMulation - MOSIM'08 - du 31 mars au 2 avril 2008 – Paris- France

« Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination.».

IMPACT DE L'UTILISATION D'UN RESEAU DE COMMUNICATION SUR LES PERFORMANCES EN SECURITE D'UN SYSTEME INSTRUMENTE DE SECURITE

A. MKHIDA

Centre de Recherche en Automatique de Nancy
CRAN CNRS UMR 7039
Ecole Nationale Supérieure d'Arts et Métiers Université Moulay Ismaïl
Marjane II, 50000 Meknès, Maroc
mkhida@hotmail.com

J.M.THIRIET

GIPSA-Lab (Grenoble Images Parole Signal Automatique) UMR 5216
Université Joseph Fourier Grenoble
38402 Saint Martin d'Hères,
jean-marc.thiriet@ujf-grenoble.fr

J.F.AUBRY

Centre de Recherche en Automatique de Nancy
CRAN CNRS UMR 7039
ENSEM
54500 Vandoeuvre, France
jean-francois.aubry@isi.u-nancy.fr

RESUME : *Dans ce papier, la modélisation et l'évaluation des performances relatives à la sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) sont traitées pour des structures classiques. La contribution de la fonctionnalité communication est ensuite évaluée après l'introduction d'un réseau de communication dans les systèmes instrumentés de sécurité. Une approche dynamique utilisant les réseaux d'activité stochastiques est proposée. Les paramètres utilisés pour l'évaluation de la sûreté de fonctionnement des SIS se réfèrent à deux modes de défaillances mentionnés par les normes de sécurité relatives aux systèmes instrumentés de sécurité CEI 61508 et CEI 61511. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres.*

MOTS-CLES : *Réseau de communication, Système Instrumenté de Sécurité, Probabilité de défaillances dangereuses, Probabilité de défaillances sûres, SAN (Réseaux à activité stochastique), Evaluation de performances*

1. INTRODUCTION

L'évolution des équipements d'automatisation entraîne d'une part l'utilisation des instruments dans des équipements sécuritaires qui deviennent plus "intelligents" et aptes à communiquer avec les équipements de production moyennant des réseaux de communication typiquement des réseaux de terrain. D'autre part, il est devenu possible d'intégrer aux équipements "intelligents" une fonction sécuritaire apte à appréhender son environnement et à réagir localement en fonction du rôle de l'équipement auquel elle est associée. Avec cette tendance moderne de traiter les données numériques, il est naturellement nécessaire de convertir les valeurs électriques sous des formes de représentations aptes à être traitée par un logiciel. Ceci exige une complexité de matériel et de logiciel bien au-dessus de celle qui existait dans ce type d'instruments classiques (Dobbing et al., 1998). Les nouvelles fonctions incorporées dans les instruments intelligents sont fortement complexes et intégrées (Mekid, 2006). Ceci rend l'analyse de sécurité difficile, de même que la nature fortement interactive des interfaces, particulièrement quand un réseau de communication est partagé entre plusieurs dispositifs.

L'introduction des réseaux de communication dans des applications sécuritaires basées sur les systèmes instrumentés de sécurité affecte les performances en sécurité.

La norme CEI 61508 (IEC, 2000) spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux indicateurs sont la probabilité de défaillance dangereuse (PFD) et la probabilité de défaillance en sécurité (PFS). Leur évaluation comme l'exige la norme CEI 61508 pose quelques problèmes liés à leur spécificité. En effet, les systèmes instrumentés de sécurité intègrent de manière obligatoire en fonction du niveau de sécurité requis, des auto-tests systématiques et des redondances permettant la détection et/ou la tolérance à certaines défaillances afin de garantir l'effectivité de la fonction de sécurité.

Dans cet article, nous nous intéressons à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant un réseau de communication par l'utilisation de réseaux d'activité stochastiques qui sont une extension des réseaux de Petri stochastiques.

Nous nous intéresserons plus particulièrement à l'influence de la fonctionnalité communication sur la probabilité de défaillance dangereuse (PFD) et la probabilité de défaillances sûres des systèmes instrumentés de sécurité et donc sur le niveau de SIL de ces systèmes.

2. RESEAU DE COMMUNICATION ET EVALUATION DE LA SURETE DE FONCTIONNEMENT

2.1. Problématique

Les systèmes d'automatisation comportant un réseau de communication sont une extension des systèmes d'automatisation classiques. L'intégration du réseau fait en sorte qu'il y a interaction constante avec les autres composants du système.

La présence d'un réseau de communication apporte quelques avantages pour les systèmes d'automatisation tels que la réduction du câblage, l'amélioration de la reconfigurabilité, la facilité de la maintenance mais néanmoins complexifie la conception et l'analyse de ce type de systèmes (Zhang et al., 2002). De nouveaux paramètres entrent en considération par rapport aux systèmes classiques, tels que le délai de transmission qui peut être constant ou variable suivant le type de réseau. Ce délai est représentatif du temps écoulé pendant la transmission des informations via le réseau. L'impact de ce délai sur le bon fonctionnement du système peut être important de sorte que les performances peuvent être dégradées et le système peut être déstabilisé (Garcia-Rivera & Barreiro, 2007). Les données transmises par le réseau peuvent être altérées en partie ou en totalité pendant la transmission affectant ainsi les performances de ce type de systèmes.

La norme CEI 61508 exige un certain nombre de recommandations et de prescriptions relatives à l'utilisation des moyens de communication de données pour réaliser des fonctions de sécurité. Notamment lorsqu'une forme quelconque de communication de données est utilisée dans la réalisation d'une fonction de sécurité, la probabilité de défaillance de la fonction de sécurité due au processus de communication doit être estimée en prenant en compte les erreurs de transmission, les répétitions, les suppressions, les insertions, les modifications du séquencement, la corruption, le retard et le masquage. Cette probabilité doit être prise en compte lors de l'estimation de la probabilité de défaillance dangereuse de la fonction de sécurité, due à une défaillance aléatoire du matériel.

Le modèle du réseau de communication doit s'attacher à tous les délais significatifs qui peuvent se produire au cours de la transmission de l'information. La difficulté inhérente à toute modélisation est la détermination du niveau de détail que le modèle doit atteindre.

2.2. Réseau de terrain et sûreté de fonctionnement

Les architectures distribuées comportant un réseau de communication ne peuvent être traitées d'un point de vue de sûreté de fonctionnement comme les architectures classiques centralisées. En effet, la modélisation du réseau ne doit pas se contenter de décrire structurellement le canal de communication mais elle doit incorporer les caractéristiques relatives à la sûreté de fonctionnement.

Les modèles statiques ne permettent pas de faire apparaître les aspects dynamiques relatifs aux transmissions de données entre différents interlocuteurs ainsi que les différents politiques d'accès au médium et les différents algorithmes mis en place.

Plusieurs techniques d'évaluation de la sûreté de fonctionnement de systèmes d'automatisation comportant un réseau de communication existent et peuvent concerner soit le réseau uniquement ou le système entier. Ces techniques peuvent concerner l'analyse quantitative (injection de fautes, diagrammes de fiabilité…), les méthodes qualitatives inductives (comme l'analyse des modes de défaillances et de leurs effets AMDE) ou encore les méthodes quantitatives déductives (comme les arbres de défaillances) (Geffroy, et al., 2002).

(Cauffriez et al., 2004) s'est basé sur le standard ISO/OSI qui est composé de sept couches en les réduisant aux trois couches habituellement prises en compte dans les réseaux de terrain, ce sont des couches qui peuvent affecter les contraintes temporelles du système. L'identification des modes de défaillances a été assurée par l'utilisation de la méthode d'évaluation AMDE. (Moncelet et al., 1997) a étudié la sûreté de fonctionnement par une évaluation quantitative utilisant la simulation de Monte Carlo. La focalisation est faite sur le système entier et non sur le réseau.

L'approche utilisée pour l'étude de la sûreté de fonctionnement est celle qui concerne l'étude du système complet et non pas l'approche qui se focalise entièrement et explicitement au réseau.

3. PERFORMANCE EN SECURITE D'UN SYSTEME INSTRUMENTE DE SECURITE (SIS)

Un système instrumenté de sécurité est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…). Un SIS est composé d'un ensemble de capteurs, d'unités de traitement et d'éléments finaux.

Les normes CEI 61508 (IEC, 2000) et CEI 61511 (IEC, 2003) définissent le niveau d'intégrité de sécurité (Safety Integrity Level : SIL) pour définir le niveau de réduction du risque, c'est-à-dire le niveau d'intégrité de sécurité que doit avoir le système de protection. Plus le SIL à une valeur élevée, plus la réduction du risque est importante. Par exemple un système de SIL 4 apporte une réduction de risque entre 10000 à 100000 alors qu'un système de SIL 1 comporte un facteur de réduction de risque compris entre 10 à 100 seulement.

Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisée par des systèmes E/E/EP relatifs à la sécurité selon la norme CEI 61508 (IEC, 2000) ou des fonctions instrumentés de sécurité selon la norme CEI 61511 (IEC, 2003). L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux événements dangereux identifiés pendant l'analyse de risque (Beugin, 2006). Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances dangereuses uniquement sans tenir compte des défaillances en sécurité ou défaillances sûres.

A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité faiblement sollicitée, la moyenne de la probabilité de défaillance à la demande PFD_{avg} (*Average Probability of Failure on Demand*) est évaluée sur un intervalle [0, t].

La performance d'une fonction de sécurité peut être exprimée comme la probabilité de défaillance à la demande (PFD), et la probabilité de défaillances sûres ou de déclenchements intempestifs. Ces deux attributs sont importants dans le monde de la sécurité et leurs valeurs représentent respectivement une mesure pour le niveau de sécurité atteint et coût financier causé par le système de sécurité en raison de déclenchements intempestifs. La valeur de la PFD est une exigence pour répondre à l'intégrité de la sécurité au niveau de la norme CEI 61508 (IEC, 2000). Pour la valeur PFS il n'ya pas actuellement de prescriptions internationales en matière de sécurité dans le monde, même si les utilisateurs finaux du système de sécurité exigent une valeur de PFS aussi faible que possible (Wolfgang & Houtermans, 2005).

Plusieurs utilisateurs sont à la recherche de systèmes qui soient à la fois fiables et sûrs. Un système est fiable s'il ne tombe pas en panne fréquemment. Un système est sûr si ses défaillances ne sont pas dangereuses.

La figure 1 montre le diagramme de Venn d'un système incluant le bon fonctionnement et les deux modes primaires de défaillances, le mode de défaillances sûres et le mode de défaillances dangereuses (Marszal & Goble, 2001).

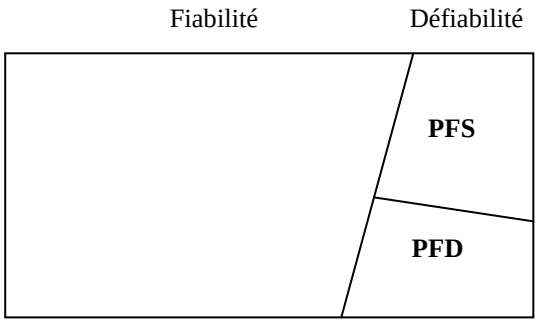

Figure 1: Système avec modes de défaillances

La fiabilité n'est pas suffisante à elle seule. Dans plusieurs applications, il est aussi important que le système tombe en panne d'une manière prévisible (défaillance sûre).

Pour les deux modes de défaillances, les défaillances dangereuses sont beaucoup plus graves puisque les systèmes de protection ne peuvent assurer la mise en sécurité du processus et les défaillances ne peuvent être révélées.

4. MODELISATION DU COMPORTEMENT

4.1. Limites des méthodes classiques

Les méthodes classiques de la sûreté de fonctionnement, sont statiques. Ces méthodes basées sur la logique booléenne pour représenter le système étudié sont adaptées à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées dans le temps.

Dans le cadre de nos travaux, la prise en compte des mécanismes de reconfiguration dans les systèmes pilotés par calculateurs est essentielle. Cet aspect n'est pas pris en compte par les méthodes classiques de sûreté de fonctionnement ce qui les rend inappropriées pour ce type de système (Mkhida et, al, 2006). Par exemple la méthode des Arbres de Défaillance ne tient pas compte de l'ordre d'apparition des événements dans un scénario. En effet, une séquence d'événements peut conduire à un événement redouté alors que les mêmes événements se produisant dans un ordre différent ou à des dates différentes peuvent l'éviter. Le temps séparant deux événements n'est pas pris en compte dans la méthode des Arbres de Défaillance, les reconfigurations ne peuvent donc pas être représentées. Les défaillances temporaires ne sont pas non plus prises en compte.

La limitation du pouvoir d'expression et de capacité d'analyse des méthodes classiques nous impose l'utilisation de méthodes où les aspects dynamiques sont modélisés tels que l'évolution déterministe des variables physiques du processus et les défaillances à caractère stochastique des composants.

4.2. Réseaux d'activité stochastiques

Les méthodes classiques ne répondent pas à notre étude puisqu'il y a des difficultés à exprimer les caractéristiques temporelles et dynamiques. Nous avons choisi de travailler avec les réseaux de Petri (dans leur variante intitulée réseaux d'activités stochastiques) pour plusieurs raisons. Citons par exemple que les réseaux de Petri disposent d'une représentation graphique, la conception est hiérarchique et modulaire, ce qui permet la réutilisation de sous-modèles à plusieurs reprises, l'évaluation des performances et l'évaluation des caractéristiques de la sûreté de fonctionnement sont des domaines d'application des réseaux de Petri…

Les méthodes fondées sur les graphes de Markov sont limités par l'explosion combinatoire qui peut aussi affecter les réseaux de Petri mais uniquement dans les graphes d'accessibilité et non pas dans les réseaux de Petri originaux.

La modélisation est donc traitée sous la forme d'une approche stochastique utilisant les SAN (*Stochastic Activity Network*). Les SAN sont un formalisme de modélisation puissant et sont une extension des réseaux de Petri stochastiques (Movaghar & Meyer, 1984). Ce formalisme permet la représentation formelle du comportement en ayant un pouvoir d'expression et un pouvoir d'analyse. Le pouvoir d'expression doit permettre le parallélisme, la synchronisation et le pouvoir d'analyse doit permettre une analyse qualitative et une analyse quantitative par évaluation des performances.

Le haut niveau de constructions de modèles est offert par les "portes d'entrée" et les "portes de sortie" qui permettent des commandes spécifiques dans l'exécution du réseau et permettent aussi des constructions hiérarchiques pour le modèle. Les modèles composés sont basés sur des sous-modèles plus simples qui peuvent être développés indépendamment et joints à d'autres sous-modèles. L'outil utilisé pour les SAN est Möbius (Deavours et al., 2002).

Dans cette méthodologie, parallèlement aux modèles fonctionnels, les modèles dysfonctionnels sont développés en même temps en exprimant les différents modes de défaillances relatifs aux différents composants. Ainsi, les modèles fonctionnels et dysfonctionnels seront intégrés dans un seul modèle. L'expression des différents modes de défaillances pour chaque composant est élaborée.

Les modèles sont ensuite interconnectés. La jonction des différents composants permet la construction de tous les sous-modèles et constitue l'étape ultime de la modélisation.

L'étape suivante consiste à spécifier les critères d'évaluation de la sûreté de fonctionnement. Les performances de sécurité ou de disponibilité s'expriment par la probabilité de se trouver dans un état dangereux (PFD) ou dans un état de repli intempestif (PFS). Cette quantification est rendue possible par la connaissance du taux de défaillance, du taux de couverture de diagnostic de chaque composant, ainsi que de l'architecture du système. Cette étape définit les critères d'évaluation nécessaires pour notre étude.

4.3. Modélisation d'un système instrumenté de sécurité

Nous allons nous intéresser à une architecture 1oo1 (un parmi un) dans laquelle toute défaillance dangereuse entraîne la défaillance du système, et une défaillance sûre se traduit par la mise dans une position de repli prédéfinie ou par une exécution intempestive de la fonction de sécurité.

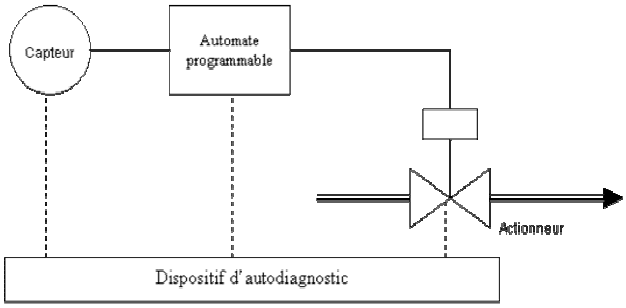

Figure 2 : Système instrumenté de sécurité

Le SIS est composé d'un capteur, d'un automate programmable et d'un actionneur. La détection des défaillances par autodiagnostic des dispositifs a pour objectif d'atteindre la fiabilité des équipements requise par le niveau d'intégrité des fonctions (de sécurité).

Nous présentons le détail des descriptions de quelques composants de notre système.

4.3.1 Modèle de capteur

Dans le modèle du capteur de la figure 3, un certain nombre de défaillances sont exprimées. Il s'agit des défaillances sûres (place ***Sur***) et défaillances dangereuses (place ***Danger***). Un taux de couverture de diagnostic DC est alloué au capteur (***Coverage***). Ce taux de couverture exprime le rapport entre le taux de défaillances détectées et le taux de défaillances totales. Après l'occurrence d'une défaillance sûre, il y a possibilité de restaurer le système par le franchissement de la transition déterministe (***restore***) dont la durée est égale au temps nécessaire à la restauration complète du système après un déclenchement intempestif par exemple.

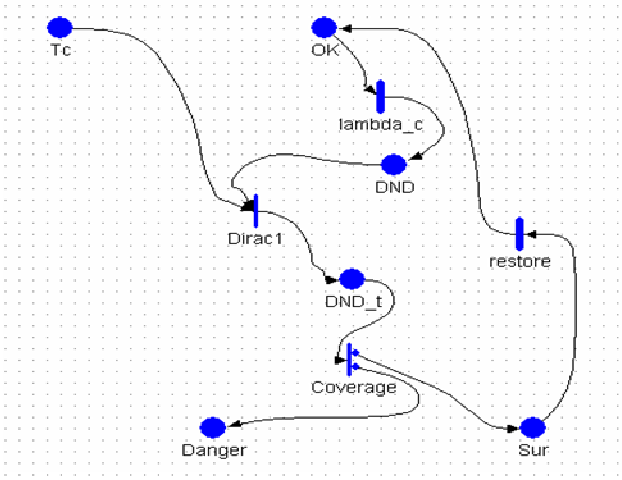

Figure 3 : Modèle du capteur

La présence d'une marque dans la place ***Tc*** autorise un autotest du capteur géré par l'automate. Les défaillances non détectées ***DND*** peuvent être qualifiées de sûres ou de dangereuses suite à l'exécution de l'autotest. (Notons que l'autotest n'est pas source de défaillances par hypoyhèse).

4.3.2 Modèle de l'automate

Le modèle de l'automate de la figure 4 montre une disposition de deux parties, l'une fonctionnelle et l'autre dysfonctionnelle. Dans la partie fonctionnelle (à gauche), les cycles de l'automate sont exécutés par une horloge périodique (***periode***).

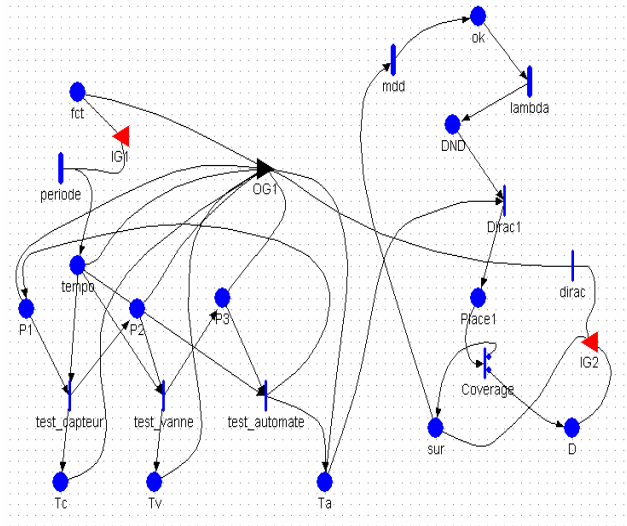

Figure 4 : Modèle de l'automate

Les autotests des différents dispositifs sont gérés localement suivant une politique de test qui consiste à allouer la même durée de test pour les différents dispositifs et à commencer par le test du capteur (***Tc***), puis l'actionneur (***Tv***) et enfin l'automate (***Ta***). Cette politique n'est pas la seule possible à être exécutée par l'automate et d'autres politiques peuvent être éventuellement implantées. Pour la partie dysfonctionnelle, il faut s'assurer que le jeton est soutiré de la partie fonctionnelle là où il se trouve lorsque le système tombe en panne sûre ou dangereuse. L'automate peut être également restauré en cas de défaillance sûre et il dispose également d'un taux de couverture de diagnostic qui lui est propre.

4.4. Modèle du réseau de communication

L'introduction des réseaux dans les applications distribuées offre de la flexibilité mais introduit aussi quelques problèmes nouveaux. Les délais, la perte de trames, les retards éventuellement non bornés, la gigue…

Nous allons nous intéresser à un modèle de système instrumenté de sécurité (SIS) avec un réseau de terrain type CAN.

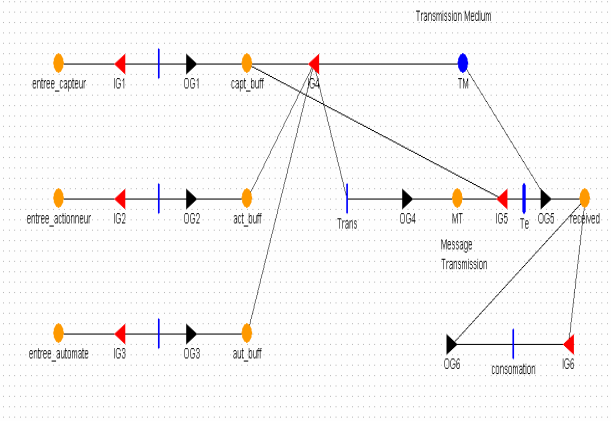

Figure 5: Modèle du réseau de terrain avec l'outil Möbius

La modélisation du réseau de communication représente le modèle le fonctionnement d'un réseau CAN (Controller Area Network). Le réseau est constitué dans cet exemple de trois stations émettrices qui vont pouvoir envoyer des messages (trames) sur un médium partagé (canal de transmission). Les messages envoyés sont placés dans des places tampons (***buffer***) qui sont des places étendues, les messages ensuite attendent la libération du canal pour être transmis vers leur destination. La manière d'accéder au canal est celle d'une transmission basée sur des niveaux de priorité des messages. Ceci signifie que chaque abonné sera affecté d'une priorité lui permettant ou non d'envoyer ces caractéristiques via le canal, pour éviter les collisions sur le canal.

Le medium (canal) est affecté d'un retard représentant le délai de transmission des messages. Le message en sortie du canal est prêt à être envoyé et il est disponible dans la place *"received"*.

Lorsque le bus est libre, n'importe quel émetteur qui dispose de son propre identificateur peut commencer à transmettre une information sur le canal. Lorsque deux nœuds tentent d'accéder simultanément au medium, le nœud qui dispose de la plus haute priorité gagne

l'arbitrage et accède au bus, son information est envoyée sans perte de temps alors que le nœud affecté d'une priorité moindre attend la libération du medium pour émettre.

Il faut noter que l'introduction du réseau de communication provoque le changement des modèles des composants qui constituent le système pour tenir compte des informations échangées entre les différents interlocuteurs.

4.5. Composition hiérarchique

La figure 6 montre la composition hiérarchique du système auquel le réseau de terrain a été introduit. Ce modèle composé est une combinaison de modèles de sous-systèmes de la boucle de sécurité, d'un modèle permettant le calcul des métriques relatives à l'évaluation des performances du système en terme de sécurité et du réseau de communication.

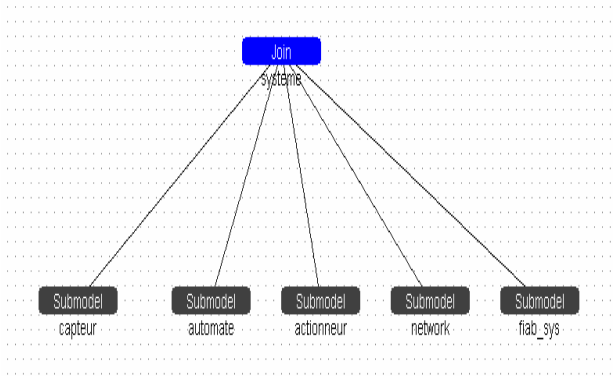

Figure 6: Composition hiérarchique du système avec réseau de terrain

L'introduction du réseau a pour conséquence quelques modifications dans les modèles de base des constituants de la boucle de sécurité afin de tenir compte des mécanismes de transmission de données via le réseau.

5. RESULTATS DE SIMULATION

5.1 Evaluation des performances du système sans réseau de communication

La procédure utilisée pour le calcul de la probabilité des défaillances dangereuses PFD et de la probabilité de défaillances sûres PFS consiste en la présence de jetons dans les places qui décrivent les défaillances sûres et les défaillances dangereuses pour l'ensemble du système.

La figure 7 montre l'évolution des deux métriques principales des performances en sécurité PFD et PFS pour une durée de 10000 heures qui est un peu supérieure à une année (8670 heures). Les deux courbes font état d'allures exponentielles. Ceci est justifié par le fait que l'ensemble des composants disposent de lois de défaillances de type exponentielles. Le taux de couverture de diagnostic est pris dans cet exemple égal à 60 % pour l'ensemble des dispositifs. Ce taux correspond à la valeur minimale préconisée par la norme de sécurité CEI 61508.

.

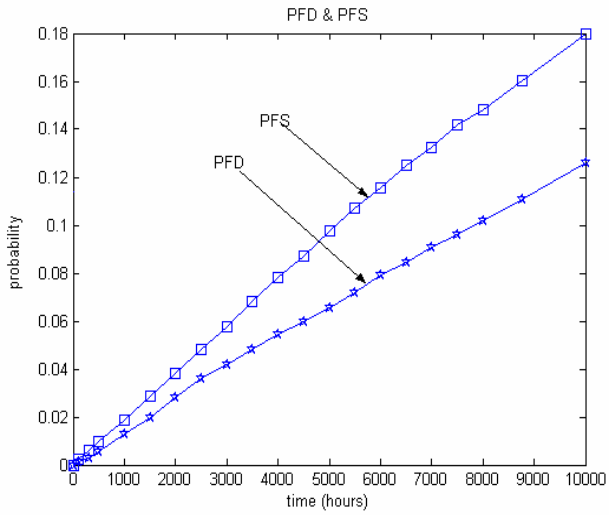

Figure 7 : Evolution de la PFD et de la PFS en fonction du temps

La norme préconise entre autres un taux de couverture moyen de 90 % et un taux de couverture élevé de 99 %. La période des autotests opérés par l'automate est choisie égale à une heure. C'est-à-dire, la durée de cycle de l'automate est de 3 heures (test du capteur, de l'automate lui-même et de l'actionneur). Notons aussi que cette durée affecte les valeurs de PFD et de PFS lorsqu'elle est changée.

5.2 Introduction du réseau de communication dans la structure du SIS

Les paramètres utilisés pour le système sans réseau sont repris avec les mêmes valeurs qu'auparavant. D'autres paramètres sont introduits, ils sont propres à l'utilisation du réseau de communication tels que le retard relatif à la transmission ainsi que les périodes d'échantillonnages des différents dispositifs (capteur, automate et actionneur). La simulation du modèle donne les résultats présentés dans le tableau suivant :

Temps (heures)	1000	5000	8760	10000
PFD	1.05^{E}-02	4.82^{E}-02	8.18^{E}-01	9.16^{E}-02
PFS	1.41^{E}-02	7.5^{E}-02	1.26^{E}-01	1.42^{E}-01

Tableau 1. Evolution de la PFD et de la PFS pour un système avec réseau

L'évolution des deux métriques relatives à la sécurité présentée dans la figure ci-dessus montre la contribution du réseau de communication et son influence sur les performances en sécurité. D'une façon générale, la probabilité des défaillances dangereuses a diminué ainsi

que la probabilité de défaillances sûres. Ceci est dû au fait que les informations qui concernent les défaillances ne sont envoyées que pendant des instants discrets et non pas en continu. Les performances sont en effet très sensibles aux périodes d'échantillonnages des différents dispositifs.

Ces résultats montrent bien l'utilité de l'emploi d'un réseau de communication dans une application sécuritaire. En effet, les performances en sécurité ont diminués. Ainsi les révélations des défaillances du système instrumenté de sécurité se font plus particulièrement par le moyen du réseau puisque les informations qui concernent la sécurité sont envoyées par voie de réseau de communication. De ce fait, les instants de révélations dépendent largement des périodes d'échantillonnages, ce qui provoque donc ce changement des valeurs de ces deux métriques.

6. CONCLUSION

Notre travail était de construire un modèle de simulation de réseau de communication incorporé dans un système instrumenté de sécurité (SIS) dans le but d'évaluer les performances en sécurité. Le modèle construit à base de réseaux d'activités stochastiques permet de modéliser des architectures de SIS classiques auxquelles l'introduction du réseau de communication est facilitée par le pouvoir de composition hiérarchique de l'outil de modélisation. Le choix des réseaux d'activité stochastiques qui sont une extension des réseaux de Petri stochastiques s'est avéré être adéquat pour mener à bien l'élaboration du modèle. Ce modèle a ainsi pu être simulé grâce à l'outil Möbius. Les résultats de simulation ont bien montré l'impact de l'utilisation d'un réseau de communication dans une application sécuritaire sur les performances en sécurité. En effet, les valeurs des métriques (PFD et PFS) ont évolué avec l'introduction du réseau de communication (CAN dans notre exemple) illustrant ainsi la contribution et l'impact du réseau de communication : une diminution des deux métriques de base relatives à la sécurité reflétant ainsi une amélioration des défaillances détectées et une augmentation des défaillances non détectées.

REFERENCES

Beugin J., 2006. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. Thèse de doctorat de l'Université de Valenciennes et du Hainaut-Cambrésis.

Cauffriez L., J. Ciccotelli, B. Conrard, M. Bayart, the members of the working-group CIAME, 2004. Design of intelligent distributed control systems: a dependability point of view. Reliability Engineering and System Safety. Vol 84. pp, 19-32.

IEC, 2000. *Functional safety of electrical / electronic / programmable electronic safety-related systems*. International Electrotechnical Commission, Geneva, Switzerland.

IEC, 2003. *Functional safety – Safety instrumented systems for the process industry*. International Electrotechnical Commission, Geneva, Switzerland.

Deavours D., G. Clark, T. Courtney, D. Dalys, S. Derisavi, J. M. Doyle, W.H. Sanders, P. G. Webster. 2002. The Mobuis framework and its implementation. IEEE Trans. On Soft. Engineering, Vol. 28, N°10, pp 956-969,.

Dobbing A., D. Godfrey, M. J. Stevens and B. A. Wichmann 1998. Reliability of Smart Instrumentation. NPL, National Physical Laboratory. Middx, UK.

Garcia-Rivera M. & Barreiro A. 2007. Analysis of networked control systems with drops and variable delays. Automatica 43, pp 2054-2059.

Geffroy J.C. & Motet G. 2002. Design of dependable Computing systems. Kluwer Academic Publishers.

Juanole G.. 2002. Quality of service of communication networks and distributed automation, models and performances. Invited paper, 15th Triennial World Congress of the IFAC, Barcelona, Spain.

Marszal E. & W. Goble. 2001. High reliability computing for control and safety. Proceedings of the 2001 Particle Accelerator Conference, Chicago. IEEE. pp, 279-282.

Mekid S. 2006. Further Structural Intelligence for sensors Cluster Technology in Manufacturing. Sensors. Vol 6. pp, 557-577.

Mkhida A., J.M. Thiriet, J.F. Aubry, 2006. Effet de la variation des données de fiabilité sur le niveau de sécurité des systèmes d'automatisation distribués - 6ème Conférence Francophone de Modélisation et Simulation - Modélisation, Optimisation et Simulation des Systèmes , MOSIM'2006, Rabat (Maroc), , pages: 1120-1126, ISBN: 2-7430-0892-X.

Monclet G., S. Christensen, H. Demmou, M. Pauldetto & J. Porras. 1998. Dependability evaluation of a simple mechatronic system using coloured Petri nets In: Workshop on practical use of coloured Petri nets and Design. pp, 189-198.

Movaghar A., J.F. Meyer. 1984. Performability modelling with stochastic activity networks. Proceddings of the 1984 Real Time Systems, Symposium, Austin, TX. Pp 215-224.

Wolfgang V.P. & M.J.M. Houtermans, 2005. The effect of the diagnostic and periodic testing on the reliability of safety systems. TUV Industrie Service GmbH, Automation, Software, Information Teschnology (ASI).

Zhang W., M.S. Branicky, S.M. Phillips. 2001. Stability of Networked Control Systems. IEEE Control Systems Magazine. pp 84-89.