Déficience de la validation d'un capteur intelligent et incidence sur les performances d'une boucle de sécurité

Abdelhak Mkhida, Jean-Marc Thiriet, Jean-François Aubry

DEFICIENCE DE LA VALIDATION D'UN CAPTEUR INTELLIGENT ET INCIDENCE SUR LES PERFORMANCES D'UNE BOUCLE DE SECURITE

VALIDATION DEFICIENCY OF AN INTELLIGENT SENSOR AND INCIDENCE ON THE PERFORMANCE OF THE SAFETY LOOP

A. MKHIDA
MTICS, MAROC,
ENSAM Meknès, UMI,
50050, Meknès
abdelhak.mkhida@ensam-umi.ac.ma

J.M. THIRIET
GIPSA-Lab UMR 5216
Université J.F. Grenoble
38402 Saint Martin d'Hères,
jean-marc.thiriet@ujf-grenoble.fr

J.F.AUBRY
CRAN CNRS UMR 7039
INPL, ENSEM
54500 Vandoeuvre, France
jean-francois.aubry@isi.u-nancy.fr

Résumé

Le travail présenté dans cet article a pour objectif d'évaluer les performances en termes de sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) disposant d'instruments d'intelligents en conformité avec les normes de sécurité fonctionnelle. L'impact des défaillances possibles de la fonctionnalité validation relative au capteur intelligent appartenant à un système instrumenté de sécurité est évalué. L'influence de ce mode de défaillance additionnel relatif aux modules qui assurent la validation sur les performances en sécurité du système instrumenté de sécurité conformément à la norme internationale CEI61511 est élucidée. 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 SIS, CEI 61508 et CEI 61511. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres.

Summary

In this paper, the modeling and thus the performance evaluation relating to the dependability of safety instrumented systems (SIS) with intelligent instruments in accordance with the standards for functional safety. The impact of possible failures of the validation feature on the intelligent sensor belonging to a safety instrumented system is evaluated. The influence of this additional failure mode related to the modules that insure the validation on the performance of safety instrumented system safety in accordance with international standard CEI61511 is elucidated. Dynamic approach using Stochastic Petri Nets (SPN) is proposed and the metrics used for the evaluation of the dependability of the Safety Instrumented Systems (SIS) refer to two modes of failures mentioned by the safety standards: mode of dangerous failure and mode of safe failure.

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.

Le travail présenté dans cet article a pour objectif d'évaluer les performances en termes de sûreté de fonctionnement des systèmes instrumentés de sécurité disposant d'instruments d'intelligents en conformité avec les normes de sécurité fonctionnelle. La performance d'une fonction de sécurité peut être exprimée comme la probabilité de défaillance sur demande

PFD et la probabilité de défaillances sûres PFS. Nous allons introduire des défaillances possibles de la fonctionnalité validation relative au capteur intelligent appartenant à un système instrumenté de sécurité. Nous allons ensuite déterminer l'impact de ce mode de défaillance additionnel relatif aux modules qui assurent la validation sur les performances en sécurité du système instrumenté de sécurité conformément à la norme internationale CEI61511.

Concept d'instrument intelligent

Un instrument intelligent (qu'il soit capteur ou actionneur) est obtenu par l'association de la technologie issue de l'instrumentation, de l'électronique et de l'informatique. Il est capable d'intégrer des fonctions supplémentaires telles que la validation, l'autodiagnostic, la compensation, la communication, etc. Ces instruments sont capables d'adapter leur fonctionnement suivant des changements produits dans leurs environnements.
L'ensemble des fonctionnalités permet à l'instrument intelligent de crédibiliser sa fonction associée à sa coopération dans un système distribué. La capacité à valider la mesure pour le capteur et à rendre compte de la réalisation par l'actionneur reflète cette crédibilisation et la participation dans un système distribué se manifeste par la participation à la commande, à la sécurité (alarmes), à l'exploitation du système…
[NOB 04] définit un instrument intelligent par un instrument dont le but principal est la mesure ou la commande d'une variable d'un processus, c'est un instrument incluant de la flexibilité dans son utilisation avec des paramètres réglés par le fabricant ou l'opérateur. Le cycle de vie d'un instrument intelligent inclut la production de quelques progiciels générés par le fabricant et utilisés pour la configuration par l'opérateur.

1. Evolution des instruments intelligents

L'instrument intelligent était basé sur l'utilisation d'un élément de mesure traditionnel, mais a inclut des possibilités de traitements micro programmés pour améliorer l'exécution de l'élément de mesure. La sortie était analogique en 4-20 mA et peut être aussi numérique en ajoutant le protocole HART par exemple. L'intelligence dans ces instruments intelligents est principalement assurée par des microprocesseurs. Typiquement la mesure du capteur après compensation était convertie en forme numérique et traitée, par exemple, en linéarisant la sortie dans le cas où elle excède sa plage de fonctionnement, et puis en l'adaptant dans un format approprié à la transmission sur un réseau analogique ou pseudo-numérique.
Vers la fin des années 90, les fabricants ont refait la conception des éléments de mesure de beaucoup d'instruments. Des techniques numériques ont été adoptées dans la conception de capteurs et d'actionneurs qui ont fait évoluer ces instruments avec l'emploi de ces nouvelles technologies. Le résultat était significatif dans trois secteurs de performances pour ces instruments

- ✓ Précision,
- ✓ Traitement des signaux à bord au plus près du procédé physique avec une délocalisation de certaines tâches de la décision.
- ✓ Diagnostic à bord ; une amélioration raisonnable du diagnostic est disponible. Par exemple, un émetteur de différence de pression a maintenant 64 sorties pour le diagnostic de signal disponible sur le réseau (Nobes, 2004).

2. Architecture fonctionnelle d'un instrument intelligent

Les capacités internes de calcul et de traitement assurées par un système à microprocesseur ainsi que sa faculté d'échange bidirectionnel d'informations avec le médium externe de communication ont permis à l'instrument intelligent d'intégrer les fonctions du système d'information, ainsi que de nouvelles fonctionnalités susceptibles d'améliorer la qualité de la mesure et de la commande.
Diverses fonctionnalités ont été proposées pour un instrument intelligent.
Robert (Robert et al., 19 93) a proposé les fonctionnalités de configuration, de communication, de mesure, de calcul et de validation. De même, Meijer (Meijer,19 94) inclut trois fonctionnalités; compensation, calcul et communication. Tandis que Tian (Tian et al., 2000) suggérait que ce qui s'appelle un capteur intelligent devrait avoir les fonctions de compensation, validation, fusion de données (data-fusion) et communication. Mekid (Mekid, 2006) propose les fonctionnalités de compensation, de traitement (processing), de communication, de validation, d'intégration, de fusion de données et de nouvelles fonctionnalités peuvent être ajoutées telles que l'auto-calibration.

La figure 1 illustre une proposition de fonctionnalités d'un instrument intelligent générique.

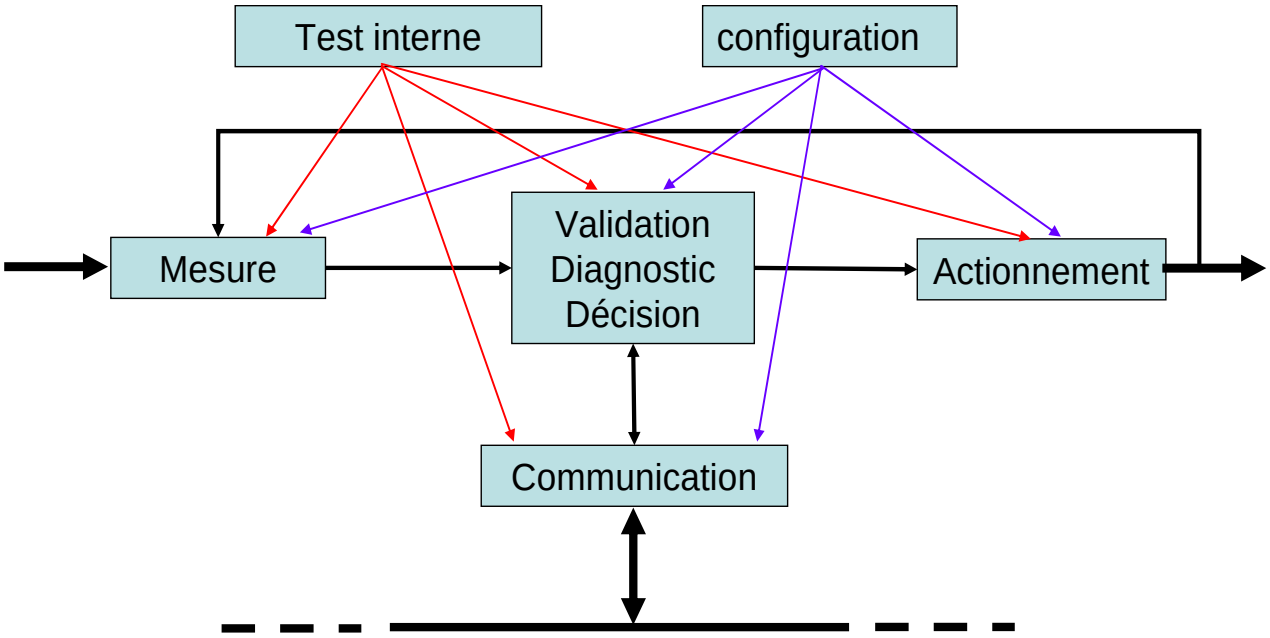

Figure 1 : Architecture fonctionnelle d'instruments intelligents (Mkhida et al., 2006)

La figure ci-dessus fait apparaître le schéma classique Mesure-Décision-Action dans la description de tout système automatisé. L'instrument intelligent est doté également d'un logiciel qui est implanté dans son nœud pour pouvoir intégrer toutes ces fonctionnalités.
L'instrument intelligent par l'implantation de ces fonctionnalités s'octroie des capacités de calcul et des moyens de communication. L'intelligence impliquera plus de renseignements dans le nœud instrument et une distribution accrue d'informations.
La fonctionnalité principale qui caractérise l'intelligence à notre sens est celle représentée par le trio validation, diagnostic, décision. Elle est le cœur de l'instrument intelligent et les autres fonctionnalités (autres la mesure et l'actionnement) concourent à son établissement et constituent des moyens au service de cette fonctionnalité. La capacité des capteurs de communiquer avec d'autres parties du système de contrôle permettra d'avoir plus de renseignements au nœud capteur (donc d'intelligence) et une distribution accrue du contrôle.
Cette fonctionnalité se rapporte donc à la correction des conditions environnementales et à leur validation, à la réalisation des fonctions de diagnostic et à la prise de décisions. C'est cette fonctionnalité qui sera à la base de l'amélioration de la sûreté de fonctionnement qui liée étroitement à l'amélioration de la crédibilité par la validation, la détection de défauts et la prise de décision adéquate

3. Validation dans les instruments intelligents

Un instrument intelligent doit fournir des informations réputées valides. La notion d'informations valides oblige la prise en compte de l'univers de la validation au sens le plus large. Il y a toujours une limite au delà de laquelle la validation devient impossible. Cette limite peut être soit : économique, technologique, ou liée à la méthode d'élaboration de la mesure …
La fonctionnalité validation d'un instrument intelligent se doit de couvrir : la totalité de la technologie alors mise en œuvre, l'ensemble de l'espace fonctionnel de l'instrument, et enfin le domaine opérationnel spécifique à l'exploitant propriétaire de l'instance matérielle de l'instrument.
La validation des données est une notion très importante dans la mesure que les systèmes sensibles aux défauts sont pris en compte. Lorsque des capteurs intelligents sont inclus dans de tels systèmes, des données sont fournies et elles vont qualifier l'estimation produite avec une certaine confiance associée.
La validation peut être représentée par l'intersection de trois cercles dans la figure 2 qui la montre comme résultat de combinaisons de technologies.

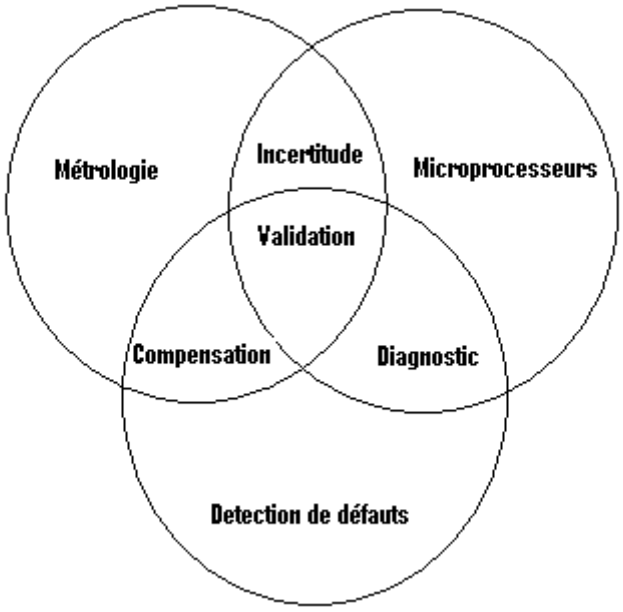

Figure 2 : La validation par combinaisons de technologies (Clarke, 2000)

Nous constatons que la validation est au cœur d'un processus combinant plusieurs technologies. L'utilisation de microprocesseurs offre plusieurs flexibilités garantissant l'implantation de différents algorithmes de détection de défauts assurant ainsi du diagnostic au sein des instruments dont les informations sont compensées. La détection de défauts basée sur l'utilisation de modèles (diagnostic) consiste en la génération d'incertitudes par la reconstruction de la sortie et sa comparaison avec la sortie mesurée et ensuite l'étape de la validation consiste en la prise de décision vis-à-vis de ce modèle pour formuler une approximation du comportement réel.

Performance en sécurité d'un système instrumenté de sécurité

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 3 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).

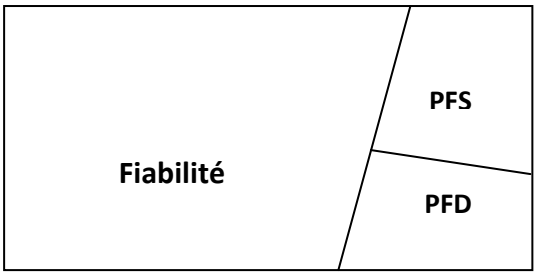

Figure 3: *Système avec modes de défaillances*

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.

Modélisation du comportement

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 cadre de nos travaux (mkhida et al, 2008), 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 . 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. Réseaux d'activités 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 et mathématique, 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).
Les portes d'entrée : les portes d'entrée sont représentées graphiquement par un triangle rouge dont le sommet est du côté des places d'entrée et la base est du côté de l'activité. Une porte d'entrée relie une ou plusieurs places à une seule activité. Une porte d'entrée possède un nom et deux fonctions : la fonction de validation qui définit les conditions d'activation d'une activité et une fonction de porte qui permet de modifier le marquage des places en entrée une fois l'activité franchie. Les portes de sortie : les portes de sortie sont représentées par un triangle noir dont la base est du côté de l'activité et le sommet est du côté des

places en sortie. Une porte de sortie possède un nom et une fonction de porte qui permet de modifier le marquage des places après le franchissement de l'activité.

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.

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 chaque composant, ainsi que de l'architecture du système. Cette étape définit les critères d'évaluation nécessaires pour notre étude.

5. 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.

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).

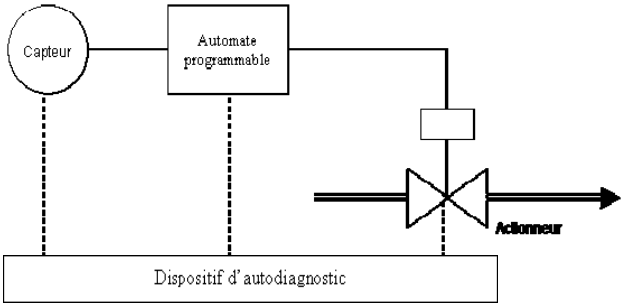

Figure 4 : Système instrumenté de sécurité

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

Le modèle du capteur est décrit par la figure suivante :

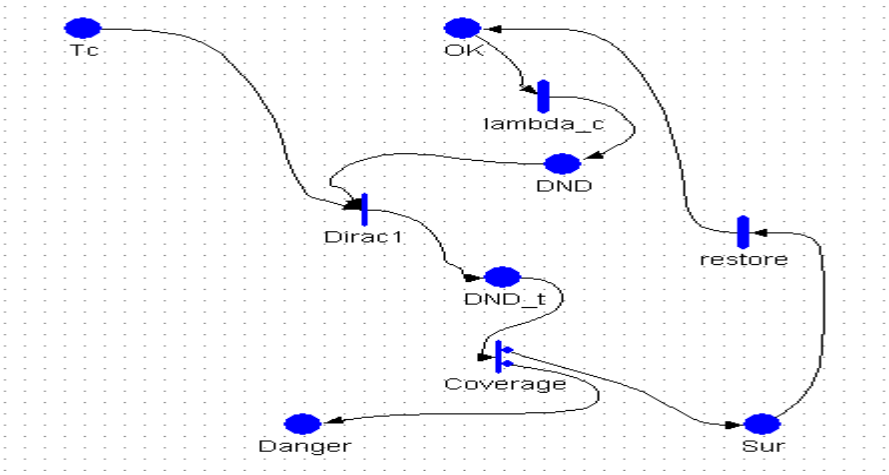

Figure 5 : Modèle du capteur

Dans le modèle du capteur de la figure 5, 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. 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.

Inclusion des défaillances de la fonctionnalité validation

Dans cette partie, nous allons introduire la défaillance possible du modèle qui reconstruit la sortie. En effet, une défaillance dans le circuit de diagnostic ne possède pas un impact immédiat sur le bon fonctionnement d'un capteur. Le capteur va continuer à fonctionner normalement. Toutefois, un défaut de diagnostic dans le circuit du capteur permet de créer une situation potentiellement dangereuse sur avènement d'une deuxième faute, la défaillance du diagnostic va être incluse dans l'analyse de la PFD moyenne.

6. Description des états du capteur intelligent

Les états 1, 2 et 4 représentent respectivement l'état de bon fonctionnement du capteur, l'état de défaillances sûres et l'état de défaillances dangereuses. Ces états sont communs au capteur décrit dans le modèle du système de sécurité utilisé pour le réservoir de pression. L'état nouveau est l'état 3 qui se comporte comme un état dégradé au niveau du capteur qualifiant la défaillance de l'élément qui assurait la redondance fonctionnelle.

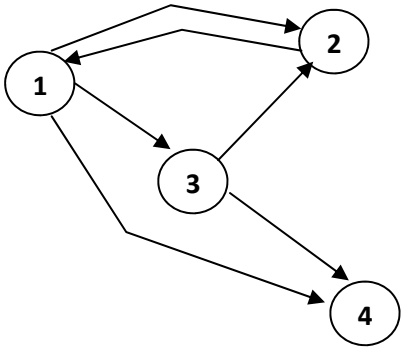

Figure 6 : Différents états du capteur intelligent

Le modèle SAN du capteur intelligent est le suivant :

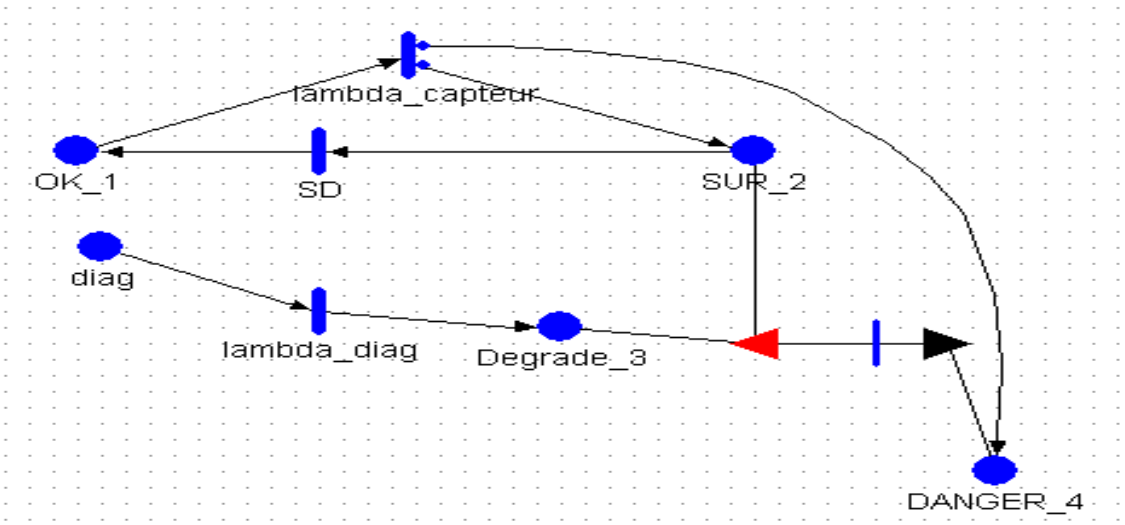

Figure 7 : Modèle SAN du capteur

Dans le modèle décrit par la figure 7, le capteur fonctionne avec succès dans les places ***OK_1*** et ***Degrade_3***. Ces places représentent les états de bon fonctionnement (1 et 3) décrits dans la figure 6. La défaillance du module relatif au diagnostic (tir de la transition ***lambda_diag***) entraîne l'exposition du capteur à un état de danger si celui-ci se trouvait dans un état de défaillances sûres puisque le module de diagnostic ne peut plus révéler les défaillances sûres.

La simulation de ce modèle qui tient compte des défaillances du module de diagnostic pour un temps de mission de 8760 heures nous a permis d'obtenir une probabilité de défaillances dangereuses d'une valeur de $1{,}29.10^{-2}$. Alors que la valeur de cette probabilité en ayant un module de diagnostic sans défaillances est de $1{,}25.10^{-2}$.
Cette donnée va avoir bien entendu un impact sur la PFD du système global. Il faut noter aussi que d'autres modes de défaillance sont nécessaires pour se procurer des informations sur les performances de sécurité et ceci a été mis en évidence par l'exemple d'application de ce capteur.

Conclusion

Notre travail était de construire un modèle de simulation d'un capteur intelligent 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 capteur intelligent 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 la défaillance de la fonctionnalité validation d'un capteur intelligent dans une application sécuritaire sur les performances en sécurité. En effet, la valeur de la métrique (PFD) a évolué avec l'introduction de la défaillance des modules relatifs à la validation dans le capteur illustrant ainsi les la contribution et l'impact d'un tel type de mode de défaillance sur les performances d'un système de sécurité.

7. Références

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.

Clarke D. W, 2000. Intelligent Instrumentation, Transactions of the Institute of Measurement and Control 22,1 pp. 3-27.

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.

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.

Meijer G. C. M., 1994. Concepts and focus point for intelligent sensor systems, Sensors and Actuators A, , vol. 41-42, pp. 183-191.

Mkhida A., J. M. Thiriet, J. F. Aubry ,2008.Toward an Intelligent Distributed Safety Instrumented Systems: Dependability Evaluation, World IFAC, Séoul,

Mkhida A., J.M. Thiriet & J.F. Aubry 2006. Evaluation de la fiabilité d'une vanne intelligente par une approche probabiliste - 15ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2006, Lille (France), 9-13 octobre 2006.

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

Nobes T. 2004. Smart instruments in protective measures, Is your product safe? –IEE Seminar.

Robert M., J. M. Riviere, J. L. Noizette, & F. Hermann,1993. Smart sensors in flexible manufacturing systems, Sensors and Actuators A, vol. 37-38, pp. 239-246.

Tian G. Y., Z. X. Zhao & R. W. Baines, 2000. A fieldbus-based intelligent sensor, Mechatronics, vol. 10, pp. 835-849.

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).