
Nouvelle Approche d'Analyse de Fiabilité pour la Sécurité de Fonctionnement à base des Systèmes Multi Agents : Application aux Systèmes de Commande Industriels

H. BELEHDDAOUI[&] — H. MEDROMI[&] — J. SAADI[&] — O. MALASSE[§]

[&] Equipe Architecture des Systèmes ENSEM
BP : 8118 Oasis Casablanca-Maroc
belhicham@hotmail.com, hmedromi@menara.ma, janah1@menara.ma
[§]A3SI-ENSAM,
4 rue Augustin Fresnel, F-57078 METZ-France
Olaf.Malasse@metz.ensam.fr

RÉSUMÉ. Le but de ce travail est de proposer une nouvelle approche orientée diagramme de fiabilité pour les systèmes d'automatisation à de boucle de sécurité, notamment les systèmes comprenant un capteur, unité de traitement et actionneur pour en estimer les critères de la sûreté de fonctionnement pour le contrôle de qualité des systèmes.

La modularité de cette approche que nous proposons permet de créer des bibliothèques de composants et ensuite d'alléger la conception d'un système aussi bien en terme de temps d'analyse qu'en terme de coût. Cette approche a fait l'objet d'une réalisation expérimentale d'une plateforme logiciel d'aide à la conception des systèmes à boucle de sécurité pour la sûreté de fonctionnement des systèmes.

MOTS-CLÉS : Sûreté de Fonctionnement, Contrôle Qualité, Multi-Agents, Plateforme d'Evaluation, Supervision

1. Introduction

Actuellement le souci majeur de l'industriel est d'adopter des procédés sûrs et propres. De ce fait, la notion de sécurité de fonctionnement s'impose. D'autant plus que le respect de l'environnement (propre) et l'évaluation des risques professionnels liée à la sécurité des travailleurs.

Par conséquent la découverte tardive d'une erreur de conception peut induire un risque technique lourd de conséquences, et entraîner des surcoûts et des retards parfois importants pour le projet. L'apparition du risque peut aussi conduire à la mise en cause de la sécurité des personnes et des biens, à la dégradation de l'environnement, à la perte de fonctions ou tout simplement à la dégradation de l'image de marque. De ce fait, le présent article aborde selon deux axes, en premier lieu, la notion de sûreté de fonctionnement ainsi que les paramètres reliés à cette dernière. Tels que ; la fiabilité, disponibilité, maintenabilité et sécurité. L'approche qualitative des différentes méthodes relatives à la sûreté de fonctionnement et leurs limites d'utilisation. D'autant plus que les normes de sûreté tels que la norme 61508 et 62061 et leurs champs d'application. En deuxième lieu, la présentation de la plateforme logiciel de supervision, que nous avons développé, s'avère très importante dans le sens où cette application introduit la fiabilité dans le problème de transmission des données dans un réseau spécifique.

2. Notion de Sûreté de Fonctionnement

La sûreté de fonctionnement est une activité d'Ingénierie qualitative et quantitative. La part qualitative correspond à l'optimisation des études au Bureau d'Etudes; elle représente 70% environ de l'activité totale. Les 30% restants représentent la partie dite quantitative qui est consacrée à la maîtrise des risques avant fabrication à partir des architectures déjà élaborées. C'est donc la phase d'optimisation des architectures des systèmes et de leur mise en œuvre de façon à maximiser, à moindre coût, leur robustesse aux aléas. La sûreté de fonctionnement est donc une action de réduction de risques et, par voie de conséquences, du coût à l'achèvement. Elle s'exerce donc essentiellement pendant les premières phases des projets, jusqu'à la mise en production. Cette démarche est une partie de la démarche générale qui, depuis quelques années, est mise en œuvre pour contrôler la fabrication d'un produit ou d'un instrument donné, que l'on désigne sous le nom d'Assurance Produit.

3. Champs d'Application de la Sûreté de Fonctionnement

Afin d'assurer un produit de qualité et une bonne image de marque chez l'industriel il faut donc identifier le facteur de risque dans le cycle de fabrication d'un produit pour pouvoir le minimiser tout en respectant le facteur

environnemental et les normes de sécurité. Le processus itératif ci-dessous est le plus utilisé dans le but d'atteindre la sécurité :

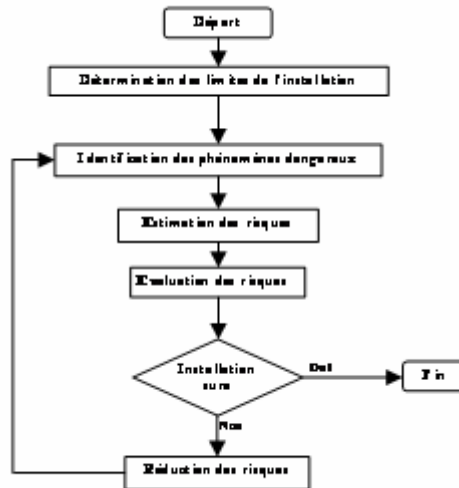


Figure 1 : Organigramme Représentant le Processus Itératif pour Atteindre la Sécurité

4. Outils d'Analyse de la Sûreté de fonctionnement

L'évaluation des critères de la sûreté de fonctionnement fait appel à de nombreux modèles et aux méthodes d'analyse qualitative et quantitative associées à ces modèles. L'analyse qualitative permet d'identifier les relations de causes à effets entre fautes, erreurs et défaillances (par exemple quelles fautes peuvent entraîner une défaillance (analyse de conséquence) alors que l'analyse quantitative évalue les paramètres probabilistes de la sûreté de fonctionnement.

Certaines méthodes conviennent aux deux objectifs. De très nombreuses approches ont été développées à l'initiative de secteurs industriels sensibles (domaine aéronautique, spatial ou nucléaire). Citons la simulation de monté Carlo, l'analyse des modes de défaillances, de leurs effets et de leur criticité (AMDEC), les méthodes d'arbres de causes ou de conséquence MAC : méthode de l'arbre de cause, MACQ : méthode de l'arbre des conséquences, les méthodes de diagrammes tel que (le diagramme de fiabilité, diagramme de succès..) ou encore les méthodes

basées sur des modèles d'état stochastiques (modèle MARKOVIEN, réseaux de PETRI stochastiques) ; etc....

Nous avons choisi d'introduire : la simulation de monté Carlo le diagramme de fiabilité (qui constitue l'un des premiers modèles analytique utilisés et l'analyse de modèle de type MARKOVIEN.

4.1. Simulation de Monté Carlo

Comme nous l'avons déjà signalé, la simulation constitue une approche quasi universelle et extrêmement utilisée. Il s'agit d'une démarche relativement facile à conduire dont nous donneront brièvement le principe.

Les événements qui font évoluer le système sont les mécanismes de destruction et de réparation, à chaque pas de simulation ces événements sont tirés au sort et injectés en tenant compte de leur loi de probabilité d'occurrence respective. Ce processus est répété un certain nombre de fois à partir du même état initial. Les lois de statistiques feront évoluer le système vers des états différents que l'on enregistre. Si le nombre de simulations effectuées est suffisamment important pour satisfaire la loi des grands nombres, on peut en déduire des informations quantitatives significatives sur les paramètres de sûreté de fonctionnement comme la fiabilité ou la disponibilité (par exemple, on calcul le cas « favorable » sur le nombre total pour estimer la survie la sécurité de produit simulé). Cette méthode exige un modèle de comportement du système et elle est souvent lourde en temps de calcul, elle est cependant très souple, acceptant des modèles statistiques complexes et l'introduction de mécanismes de files d'attente utilisée en informatique pou l'accès à certaines ressources.

4.2. Graphe de Markov

Il s'agit d'état à transitions non déterministes. On évolue d'état en état comme dans un graphe d'état classique, mais les transitions entre états sont étiquetées par des probabilités : le fait de franchir une transition ou une autre à partir d'un état est fonction de ces probabilités. En sûreté de fonctionnement, on exprime avec de tels graphes les différents états d'un produit soumis à des mécanismes de dégradation et à des mécanismes protecteurs. A condition que certaines hypothèses mathématiques soient satisfaites. On peut avoir recours à des outils assez simples d'analyse des matrices probabilistes associées à ces graphes. On évalue alors le comportement du produit de probabilité d'atteindre ou de ne pas atteindre un état ou un groupe d'états à partir d'un état initial connu (produit sans faute).

5. Evaluation FMDS d'un système

Le concept de sûreté de fonctionnement est d'autant plus large qu'il nécessite l'introduction de plusieurs paramètres qui sont mis en jeu dans l'élaboration de ce dernier. Parmi ces paramètres je citerai dans ce qui suit les notions de ; Maintenabilité, Disponibilité, Sécurité et Fiabilité (Bouras 1997).

5.1. *Fiabilité*

C'est une fonction du temps qui estime par des méthodes statistique l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données et pour un intervalle de temps donné (Barger 2003).

- Loi exponentielle : la fiabilité est décrite par des lois mathématiques décroissantes au cours du temps. Dans ce qui suit nous considérons uniquement la loi exponentielle qui est la plus simple et la plus utilisée en sûreté de fonctionnement des systèmes électriques.
- Les autres lois plus précises telles que la loi de WEIBULL sont plus complexes à comprendre et à manipuler. La loi exponentielle traduit la probabilité de survie par une fonction exponentielle décroissante du temps :

$$R(t) = \text{EXP}(-\lambda t)$$

Où λ est le taux de panne qui exprime une probabilité d'occurrence de pannes par heure (unités non MKSA), par exemple 10^{-6} pannes / heure

5.2. *Temps moyen de bon fonctionnement*

(Note MTBF pour Mean Time Between Failures), pour des produits réparables (le produit en panne est réparé et remis en service). Pour une loi exponentielle ce paramètre, valeur moyenne de la fonction vaut :

$$\text{MTBF (ou MTTF)} = 1 / \lambda$$

Il s'exprime avec une unité non MKSA en puissance de 10 heures : par exemple 10^6 .

5.3. *Courbe en baignoire*

En réalité, le taux de panne λ des systèmes physiques n'est pas constant au cours du temps. On admet qu'il est élevé au début de vie d'un système (sa jeunesse) puis qu'il s'abaisse en demeurant a peu près constant durant sa vie active, pour enfin croître a nouveau fortement lors de sa vieillesse. On a l'habitude de présenter cette évolution par une courbe $\lambda(t)$ dite <<en baignoire>> (Bath curve) comme celle de la figure suivante. C'est dans la partie <<vie active>> que se situe l'hypothèse de taux de pannes λ constant.

5.4. *Maintenabilité*

Elle consiste à arrêter la mission du produit pour lui faire subir, un certain nombre d'examens afin d'établir son état de santé (présence de fautes par détection) et éventuellement le remettre en bon état par la localisation de la faute pour ensuite la réparer. On dit que le produit est réparable dans le contexte de son application. La maintenance n'est pas envisageable pour de nombreuses applications où les systèmes sont isolés (la plupart des satellites ou balises polaires).

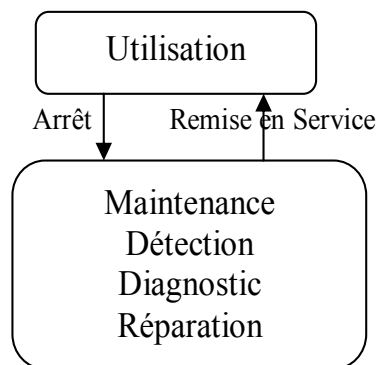


Figure 2 : *Maintenance*

La politique de maintenance est :

- Soit préventive, il s'agit alors d'une opération systématique pour détecter la présence d'une faute avant qu'elle ne conduise à une défaillance
- Soit curative, il s'agit alors de traiter un produit réputé défaillant.

La maintenance préventive d'un équipement informatique est conduite avec une périodicité fixe ou variable. La mesure de la période maintenance n'utilise pas toujours les mêmes paramètres, ils dépendent du domaine considéré.

On emploie le temps absolu, le nombre d'heures de fonctionnement ou encore le nombre de Kilomètres parcourus, ainsi on révisé un véhicule automobile tous les 10000 Km ou chaque années.

La maintenabilité curative est conduite après détection d'une anomalie, par exemple, on conduit un véhicule automobile chez le garagiste car son démarrage est difficile.

Par généralisation la maintenance concerne également des opérations de modification de certaines fonctions du produit déjà conçu et réalisé en vue d'améliorer ses performances ou de l'adapter à de nouveaux procédés ou à de nouvelles contraintes.

On pense aux versions successives des produits logiciels (1.0, 2.0, etc....) , on parle alors de maintenance évolutive.

La maintenabilité mesure donc l'aptitude déjà conçu et réalisé :

- A la réparation, c'est-à-dire à la remise en état de fonctionnement correct du produit affecté.
- Ou à l'évolution, c'est-à-dire à la modification par ajout de nouvelles fonctionnalités ou par amélioration des fonctionnalités déjà existantes.

On cherche d'abord à mesurer la facilité à conduire une opération de maintenance préventive : test de détection puis de localisation de la (ou des) faute(s) réparation et réinitialisation éventuelle. On s'intéresse ensuite à la facilité avec laquelle ce produit pourra subir des modifications pour s'adapter à un nouvel environnement fonctionnel ou pour accepter une nouvelle fonctionnalité.

5.5. Disponibilité

Pour des lois de fiabilité et de réparation de type exponentielles à Taux de panne λ et de réparation μ constants, on montre que la disponibilité vaut :

$$A(t) = \mu / (\mu + \lambda) + \lambda / (\mu + \lambda) \exp(-(\mu + \lambda)t)$$

5.6. Sécurité

La notion de sécurité (security en anglais) est directement liée à celle de criticité des défaillances décrite dans la première partie. Rappelons que les défaillances peuvent présenter plusieurs classes de conséquences externes sur l'application du produit : bénignes, sévères, critiques catastrophique. La sécurité et le critère privilégie des applications de haute critère pour lesquelles les conséquences de certains défaillances sont catastrophiques : systèmes embarqués du domaine avionique, spatial, etc. Ce critère mesure la confiance attribuable au produit de ne pas présenter de défaillance dont les conséquences externes sont catastrophiques.

La sécurité est la probabilité pour que le produit n'ait aucune défaillance catastrophique entre l'instant initial et l'instant t (Hamidi 2005).

Si on réfère a nouveau a un modèle statique a état, on mesure la probabilité de ne pas atteindre l'état 3, juge dangereux, sachant que l'on se trouvait a l'état 1 a l'instant initial et que l'on connaît les probabilités P_{12} et P_{13} sont directement dérivées de taux de panne par heure.

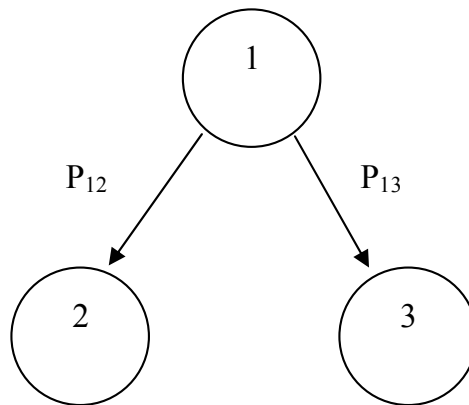


Figure 3 : État défaille dangereux

Un exemple simple est celui du régulateur de chauffe d'un ballon contenant un liquide dangereux : une défaillance du régulateur est dangereux si elle conduit a l'exploitation du ballon par surchauffe. On mesurera la sécurité de ce régulateur comme la probabilité pour qu'il n'atteigne pas un état conduisant à une explosion. La sécurité dépend bien sûr de la technologie utilisée et des paramètres d'environnement (comme la température), mais également des mécanismes de production qui tendent à éviter l'apparition de la défaillance cause de l'explosion ou à empêcher que la défaillance ne provoque l'explosion (protection externe au produit).

Les méthodes permettant d'accroître la sécurité sont passablement coûteuses. Une première approche évidente concerne l'accroissement de la fiabilité des composants employés (réduction de la probabilité de faute, donc de défaillance). Cependant, lorsque cette approche s'avère insuffisante, on emploie des techniques spécifiques de redondance ; il peut y avoir antagonisme entre les deux paramètres, fiabilité et sécurité, si l'augmentation du nombre de composants destinée à accroître de la sécurité réduit la fiabilité (Luttenbacher 1997).

- Synthèse des principaux critères de sécurité de fonctionnement :

L'évolution du fonctionnement d'un produit est représentée sur la figure suivante par un modèle probabiliste simple à trois états : l'état 1 est l'état de fonctionnement correct, l'état 2 un état de défaillance n'entraînant pas la perte de la mission et pouvant être réparé selon l'arc (2-1) et l'état 3 un état de défaillance non récupérable (état « puit »). L'arc (1-2) entraîne la défaillance du produit et est étiqueté par la probabilité de défaillance P_{12} , et l'arc (1-3) entraînant la fin de la mission est étiqueté par la probabilité de défaillance P_{13} . Notons que les probabilités associées aux transitions s'expriment en général avec des taux de panne et de réparation de type λ et μ .

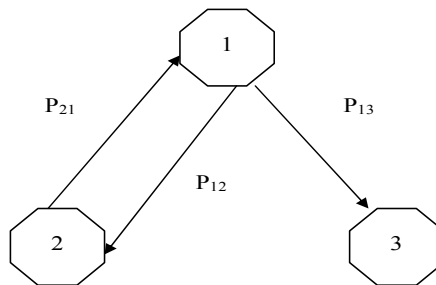


Figure 4 : *Modèle probabiliste d'évolution du fonctionnement.*

Avec ce modèle de base, les quatre principaux critères de la sûreté de fonctionnement sont exprimés, le graphe étant à l'état 1 (à l'origine des temps) (Jumel et al. 2003).

L'expression $q(t)$ désigne l'état (1, 2 ou 3) dans lequel se trouve le système à l'instant t . à l'instant initial ($t = 0$), le système est supposé être à l'état correct 1 :

- La fiabilité à l'instant t est la probabilité (noté P) pour que l'on soit resté à l'état 1 de 0 à l'instant t . Cela correspond bien à une mesure de la capacité du produit à rester sous défaillance.
- La sécurité à l'instant t exprime la probabilité pour que l'on ne se trouve pas à l'état 3 à l'instant t . cela implique que le produit ne se trouve jamais à cet état entre 0 et t .
- La disponibilité est la probabilité pour que l'on se trouve pas à l'état 1 à l'instant t quelles que soient les évolutions ayant eu lieu entre les états 1 et 2.

- La maintenabilité est la probabilité pour que le produit défaillant à l'instant t soit réparé avant une certaine durée Δ prédéfinie. Cette définition est une variante de la loi exponentielle à taux constant ; elle met l'accent sur le délai de réparation.

Les deux derniers critères s'appliquent à des produits réparables.

Fiabilité :	$R(t) = P(q(\tau) = 1, \tau \in (0,1))$.
Sécurité :	$S(t) = P(q(t) \neq 3)$.
Disponibilité :	$A(t) = P(q(t) = 1)$; système réparable.
Maintenabilité :	$M(t) = P(q(t+\Delta) = 1 / q(t) = 2)$; système réparable.

Figure 5 : Expression des principaux critères

6. Introduction sur les normes de sécurité

Suite à l'automatisation, ainsi qu'à la demande d'une production plus élevée avec une réduction des efforts physiques des opérateurs, les systèmes de commande électriques relatifs à la sécurité (appelés SRECS) des machines jouent un rôle croissant dans la réalisation de la sécurité d'ensemble des machines. De ce fait, les SRECS utilisent de plus en plus souvent une technologie électronique complexe. Auparavant, en l'absence de normes, on a pu observer un manque d'utilisation des SRECS dans les fonctions relatives à la sécurité pour des phénomènes dangereux significatifs sur les machines, en raison de l'incertitude concernant le fonctionnement d'une telle technologie.

La norme internationale est destinée à être utilisée par les concepteurs de machines, les fabricants et les intégrateurs de systèmes de commande, et autres, impliqués dans la spécification, la conception et la validation d'un SRECS. Elle présente une approche et donne les exigences nécessaires à la réalisation du fonctionnement requis. La norme utilisée dans notre cas est spécifique au secteur des machines dans le cadre de la CEI 61508.

Elle est destinée à faciliter la spécification du fonctionnement des systèmes de commande électriques relatifs à la sécurité par rapport aux dangers significatifs des machines. Cette norme donne un cadre spécifique au secteur des machines pour la sécurité fonctionnelle d'un SRECS. Elle couvre uniquement les aspects du cycle de vie de sécurité relatifs à l'allocation des exigences de sécurité jusqu'à la validation de la sécurité.

7. Application

Avant d'introduire l'outil logiciel développé qui illustre la notion de sûreté de fonctionnement il s'avère important de citer le diagramme de fiabilité sur lequel est basée cette application.

7.1. Diagramme de fiabilité

Un produit étant constitué d'un assemblage élémentaire de fiabilité connue ; comment déterminer sa fiabilité globale ?

Le diagramme de fiabilité est issu des études sur les composants matériels, mais on le rencontre également, dans des études plus générales aux niveaux « système ».

7.2. Association « série »

Si le produit est constitué de n composants C1, C2,....., Cn de lois de fiabilité exponentielles R1 (t), ..., Rn (t), et si la défaillance de l'un d'entre eux pour entraîner la défaillance du produit (c'est le cas de la plupart des produits), on utilise les règles du calcul des probabilités pour déduire la fiabilité pour déduire la fiabilité de l'ensemble à partir de la fiabilité de chaque composant. On emploie le théorème classique des probabilités indépendantes. La fiabilité globale est le produit des probabilités des composants :

$$R = \prod R_i$$

Avec des composants ayant des lois exponentielles avec un taux constant, la loi globale est également exponentielle avec un taux λ qui est la somme des taux de panne λ_i des composants :

$$\lambda = \sum \lambda_i$$

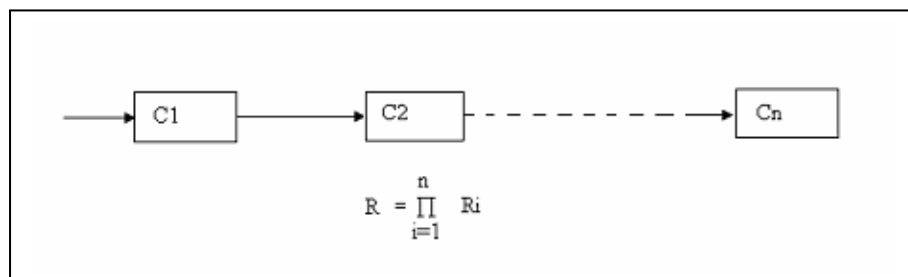


Figure 6 : *Composants en série***7.3. Association parallèle**

Toutes les structure électronique ne sont pas de type « série » (type précédent) (Bicking et al. 2002). En effet ; dans certains cas de redondance, la défaillance de l'ensemble ne se produit que lorsque tous les composants son défaillants. Un exemple simple est celui de la mise en parallèle de deux ampoules : tant qu'une ampoule fonctionne correctement, l'éclairage est assuré. On rencontre fréquemment de telles structures redondantes en sûreté de fonctionnement car elles ont une meilleur fiabilité (et une meilleur disponibilité dans le cas ses systèmes réparables). En effet, la probabilité pour que le produit soit défaillant est alors le produit des probabilités de défaillance de chacun des composants :

$$1 - R = \prod (1 - Ri) \quad ; \quad R = 1 - \prod (1 - Ri)$$

Avec des composants ayant des lois exponentielles à taux constant, la loi globale est une fonction plus complexe que pour un montage « série ».

La redondance précédente est dite passive en ligne (ou à « chaud »), car les deux modules fonctionnent dans les mêmes conditions avec la même fiabilité. On rencontre parfois d'autres situations de redondance telle que la redondance passive hors ligne (ou à « froid ») où la mission est assurée par un module jusqu'à ce qu'une défaillance l'affecte ; alors on le remplace par second module en attente et non connecté dont la fiabilité est plus souvent supposée parfaite. Bien sûr, des situations encore plus complexes sont possibles et leurs étude exige d'autre outils comme la transformée de laplace.

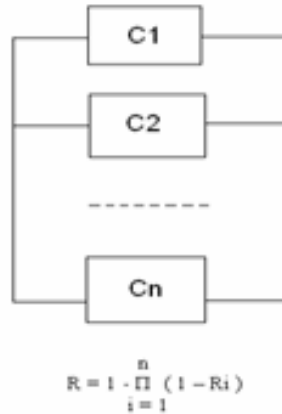


Figure 7. Composant en //.

La plateforme logiciel proposé dans le cadre de cet article pour l'évaluation de la sûreté de fonctionnement a été réalisé en VBA et utilise l'outil VISIO pour la représentation graphique des composants des fonctions de sécurité pour des systèmes automatisés.

Les figures représentées ci-dessous illustrent des interfaces graphiques de l'application qui calcule le taux de défaillance d'un actionneur ou d'un capteur ..., ainsi que le taux de défaillance dangereux et en sécurité. De plus la présentation de n'importe quel système sous VISIO ainsi que les librairie des composants qui le comportent.

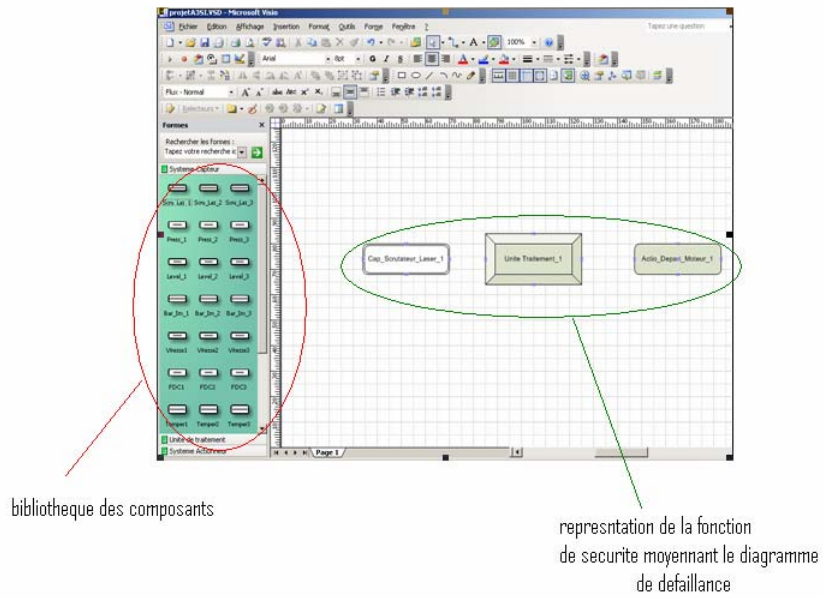


Figure 8 : Workspace principale de l'outil VISIO

The image shows a dialog box titled 'Actio_Contacteur1'. At the top, it says 'Les different Actionneur Contacteur' and has a dropdown menu. Below this is a large empty rectangular area. Further down, there are two input fields: 'Taux de defaillance d'actionneur:' and 'La valeur de SFF: 0,5'. Below these is a section titled 'Choix de DC et ProofTest' with a radio button selected for 'Activer nouveau calcul'. To the right of this section is a yellow button labeled 'Calculer Le Taux de Defaillance dangereux:'. Below this are four more input fields: 'Le Taux de Defaillance dangereux:', 'Le taux de defaillance en securite:', 'Taux de couverture de diagnostic: 0', and 'La Valeur De Proof Test en heure:'. At the bottom of the dialog are three buttons: 'Fermer sans Enregistrer', 'Valider', and 'Remise a zero'.

Figure 9. *Interface Utilisateur pou le Contrôle des Actionneurs*
Figure 10. *Interface utilisateur pou le contrôle des Capteurs*

8. Conclusion et Perspective

En arrivant au terme de cet article nous tenons a relever les points suivants qui representent les objectives de notre étude.

- Comprendre les exigences de sécurité conforme à la réglementation
- Connaître les technologies des systèmes instrumentés de sécurité
- Voir comment valider une solution a base de technologies de SIS connues

Les méthodes cités dans cet article ; objet de ce travail; ne representent qu'une partie de l'étude sur la sûreté de fonctionnement on retrouve d'autre méthodes qui font objectifs de recherche actuellement tels que les méthodes AMDEC, l'arbre de défaillance, réseau de pétri

Et comme perspectives nous tenons a introduire les autres méthodes cités ci-dessus et les implémenter dans la plateforme logiciel développé et ainsi pouvoir générer des résultats plus varies et très utiles pour le contrôle à distance des systèmes complexes.

9. Bibliographie

Barger P. Evaluation et Validation de La Fiabilité et de la disponibilité des Systèmes D'Automatisation à Intelligence Distribuée, en Phase Dynamique Thèse de Doctorat de l'UHP Nancy 1, France, 2003

Bouras A. Contribution à la Conception D'architectures Réparties : Modèles Génériques et Interopérabilité, d'Instruments Intelligents », Thèse De Doctorat, Université de Lille I, France, 1997

Charpentier P. "Architecture d'Automatisme en Sécurité des Machines : Etudes des Conditions de Conception liées aux Défaillances de Mode Commun, Thèse INPL/CRAN, France, 2002

Conrard B.; Thiriet J-M.; Robert M. Conception d'Architectures de Systèmes D'Automatisation par allocation des traitements sous des contraintes de sûreté de fonctionnement. Congrès QUALITA 2001, Annecy, France, 2001

Bicking F.; Conrard B.; Thiriet J-M. Integration of Dependability in a Task Allocation Problem. 19th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC2002), Anchorage (Alaska, United States), 2002

Hamidi. Contribution à un Modèle D'évaluation Quantitative des Performances Fiabilistes de Fonctions Electroniques et Programmables Dédiées à la Sécurité » Thèse de Doctorat INPL, CRAN, Nancy, France, 2005

Luttenbacher D. Modélisation du Concept Capteur Intelligent par une Approche Orientée Objet : Application à un Capteur Intelligent de Température, Thèse de Docteur de l'Université Henri Poincaré, Nancy, France, 1997

Staroswiecki M.; M. Bayart. Actionneurs Intelligents, Hermès, Paris, France, 1994

Jumel F; Thiriet J-M; Aubry J-F; Malasse O. Towards an Information Based Approach for the Dependability Evaluation of Distributed Control Systems" IEEE Instrumentation and Measurement Technology Conference IMTC 2003 Vail, Colorado USA, 2003, pp. 270 – 275.