

# CONGRÈS

## COMPTE RENDU

### SIAS 2005

## 4<sup>ÈME</sup> CONFÉRENCE INTERNATIONALE «SÉCURITÉ DES SYSTÈMES INDUSTRIELS AUTOMATISÉS»

Suite aux trois précédentes éditions qui se sont tenues à Montréal en 1999, à Bonn en 2001 et à Nancy en 2003 [CR 02 - HST - CND 194 - 2004], la quatrième conférence internationale sur la sécurité des systèmes industriels automatisés s'est tenue à Chicago du 26 au 28 septembre 2005. Cette conférence a été organisée par l'ATC<sup>1</sup> en collaboration avec NIOSH<sup>2</sup>, NIST<sup>3</sup>, AMT<sup>4</sup>, RIA<sup>5</sup>, IRSST<sup>6</sup>, INRS, HSE<sup>7</sup>, BGIA<sup>8</sup>, CIOP<sup>9</sup>, et NECA<sup>10</sup>, avec le soutien de l'AISS<sup>11</sup>. Elle a fait l'objet de 40 communications réparties en 9 sessions thématiques ainsi qu'une session « posters ». Ces contributions présentent les derniers développements et recherches dans le domaine des risques professionnels liés aux systèmes industriels automatisés.

Le présent document synthétise les différentes communications exposées lors des sessions.

Dans son discours d'ouverture, Jeff FRYMAN (RIA) a exposé la problématique de la sécurité dans un contexte de marché concurrentiel international. Il a rappelé que, notamment aux USA, la sécurité a du mal à être acceptée car elle est trop souvent perçue comme un frein à la compétitivité. C'est pourquoi il s'est félicité d'organiser cette conférence qui montre notamment à travers les différentes communications des intervenants que la sécurité des systèmes est une préoccupation majeure qui, si elle est bien intégrée, peut au contraire être un atout sur un marché concurrentiel.

26 - 28 septembre 2005  
Chicago (USA)

- ▶ Jean-Christophe Blaise,  
Philippe Charpentier,  
INRS, Département Ingénierie des  
équipements de travail
- ▶ Jean-Louis Poyard,  
INRS, Département Expertise et conseil  
technique
- ▶ Elie Fadier,  
INRS, Département Homme au travail
- ▶ Anna-Maria Poli,  
INRS, Département Documentation

- <sup>1</sup> Automation Technologies Council (US)
- <sup>2</sup> National Institute for Occupational Safety and Health (US)
- <sup>3</sup> National Institute of Standards and Technology (US)
- <sup>4</sup> Automated Management Technologies (US)
- <sup>5</sup> Robotic Industries Association (US)
- <sup>6</sup> Institut de recherche Robert-Sauvé en santé et en sécurité du travail (CA)
- <sup>7</sup> Health and Safety Executive (GB)
- <sup>8</sup> Berufsgenossenschaftliche Institut für Arbeitsschutz (D)
- <sup>9</sup> Central Institute for Labour Protection (PL)
- <sup>10</sup> Nippon Electric Control Equipment Industries Association (J)
- <sup>11</sup> Association Internationale de la Sécurité Sociale

## SESSION 1 : ORIENTATIONS EN ROBOTIQUE

Animée par J. FRYMAN (RIA, USA) et S. SHAW (HSE, Royaume-Uni)

- **Systèmes de commande à sécurité intégrée pour machines/robots** par M. KRELL - BGIA - Allemagne,
- **Proposition d'un index de tolérance à la douleur pour la conception sûre de robots collaboratifs avec l'Homme** par H. IKEDA - NIIS - Japon,
- **PowerMate - Développement de la coopération Homme-robots dans les environnements industriels par la mise en œuvre de nouveaux capteurs et contrôleurs** par C. PARLITZ - Fraunhofer Institute for Manufacturing Engineering and Automation - Allemagne
- **Certification de la sécurité du robot de service « Wakamaru »** par T. KABE - NPO - Japon,
- **Automate dédié à la sécurité ESALAN** - Nouvelle référence pour la sécurité des robots. par F. ADAMS - LAN - Allemagne.

Lors du premier exposé, M. KRELL, après avoir fait le constat d'une augmentation de la flexibilité des installations robotisées, a évoqué les normes applicables à ce domaine notamment la future norme sur la sûreté des produits (CEI 61800-5-2) qui définira les principales fonctions de sécurité telles que : arrêt sûr sans couple, arrêt opérationnel sûr, limitation sûre de vitesse, limitation sûre de position, etc. Ces fonctions de sécurité peuvent être combinées pour garantir le comportement sûr d'un robot industriel.

Le deuxième exposé proposait un index de tolérance humaine à la douleur comme indicateur pour la sécurité dans la conception de robots collaboratifs. En effet, selon H. IKEDA, il n'existe pas d'indicateur définissant, par exemple, la force maximale que le robot sera autorisé à produire en cas de contact, lequel sera inévitable pour effectuer la tâche demandée. L'auteur a également souligné que les règles de sécurité classiques de distance à respecter et de dispositif d'arrêt, qui constituaient la référence en matière de sécurité des opérateurs travaillant avec des robots industriels conventionnels, ne sont plus applicables à ce nouveau type de robots. Enfin, le concept et la procédure de sécurité dans la conception de robots en fonction de cette tolérance ont été présentés.

Le troisième exposé présentait le démonstrateur appelé «PowerMate» développé dans le cadre du projet ASSISTOR.

L'objectif de ce projet est de mettre en place des méthodes et des procédures permettant aux opérateurs et aux robots de travailler ensemble de façon plus productive et plus sûre, notamment pour les opérations de maintenance. «PowerMate» a été conçu pour illustrer les possibilités en matière de coopération Homme-robot selon les normes et directives en vigueur. Un laser scanner du commerce a été modifié sous forme de capteur multimodal permettant de créer une zone de surveillance en deux dimensions pour le contrôle de la vitesse du robot.

Le quatrième exposé concernait les robots de service. Avec le développement de la cyber-société, divers types de robots de service, coexistant avec les êtres humains et devant assumer de nouvelles fonctions sociales, font l'objet de recherche et développement. Néanmoins, il n'existe toujours pas de définition de ce type de robot de service. Avant l'entrée en vigueur d'une norme internationale servant de norme produit indépendante, le NPO (Japon) était chargé de la certification de la sécurité du robot de service «Wakamaru». Le conférencier a notamment expliqué que la norme ISO/CEI Guide 51 a servi de référence et les normes existantes relatives à la sécurité des machines ont également été prises en considération. L'état de l'art et le principe ALARP («principe du niveau de risque le plus bas que l'on peut raisonnablement réaliser») ont été considérés comme les facteurs de décision fondamentaux.

Enfin, le dernier exposé de cette session présentait le concept de l'automate dédié à la sécurité ESALAN ainsi que quelques unes de ses spécificités techniques. Ce système électronique programmable permet de surveiller la vitesse et la position de chaque axe d'un robot en fonction d'un mode de fonctionnement prévu. Ce système est certifié comme garantissant une catégorie 3 selon l'ISO 13849-1:1999. Les applications concernent notamment les risques de collisions entre robots collaboratifs mais aussi avec d'éventuels opérateurs.

*Globalement, cette session était orientée sur la sécurité de systèmes particuliers : les robots. Alors qu'ils étaient, a priori, cantonnés à des exploitations hors présence humaine, on assiste d'une part à un développement de l'interaction homme/robot, notamment par le biais de robots collaboratifs ou de service et d'autre part, à une prise de conscience que l'isolement des opérateurs et robots par des dispositifs de sécurité contraint l'exécution de tâches telles que la maintenance. Cette interaction nécessite de repenser les conditions sûres d'utilisation de ces robots.*

## SESSION 2 : APPLICATIONS PRATIQUES

Animée par P. CHARPENTIER (INRS, France) et T. FUJITA (NECA, Japon)

- **Sécurité des machines : retour d'expérience des accidents en automatisme à partir de la base de données EPICEA** par P. CHARPENTIER - INRS - France,
- **Modèle d'accidents dus au mauvais fonctionnement des systèmes de commande des machines** par M. DZWIAREK - CIOP Pologne,
- **Enquêtes d'accidents relatifs aux portes tambour automatiques** par M. SCHAEFER - BGIA - Allemagne,
- **Des exemples pour une conception efficace des systèmes de commande relatifs à la sécurité** par T. MALM - VTT - Finlande,
- **Analyse de défaillances opérationnelle des systèmes automatisés pour l'exploitation minière** par R. TIUSANEN - VTT - Finlande.

Pour le premier exposé de cette session, P. CHARPENTIER a présenté un retour d'expérience sur les accidents liés aux automatismes pour, d'une part, déterminer l'incidence que les automatismes peuvent avoir dans les accidents du travail et, d'autre part, tenter de faire émerger des points d'amélioration et observer les évolutions de la prévention en la matière. Il en est ressorti que les phases annexes de la production (mise en service, réglage, maintenance, etc.) représentaient une part importante du total des accidents. Le conférencier a également souligné que la prévention des accidents liés à l'automatisation passe nécessairement par une meilleure analyse des risques relatifs aux équipements dans tous leurs modes de fonctionnement, ainsi que par l'amélioration des protections et une information adéquate du personnel.

Pour le second exposé, M. DZWIAREK a présenté une étude recensant l'ensemble des événements résultant du mauvais fonctionnement des systèmes de commande de machines sur 700 accidents environ. Une checklist d'analyses des accidents a été élaborée pour faciliter le processus d'identification des causes d'accidents. Ce modèle montre le lien de cause à effet entre des causes indirectes spécifiques et des causes directes, ce qui permet l'identification de toutes les causes possibles d'accident et indique les mesures de prévention les plus appropriées. L'étude montre que les accidents dus au mauvais fonctionnement des systèmes de commande constituent 36 % des accidents et que les accidents graves sont beaucoup plus fréquents (41 %) que les autres types d'accidents (7 %).

En introduction du troisième exposé, M. SCHAEFER a relaté un accident ayant entraîné la mort d'un petit garçon de 18 mois, coincé dans une porte tambour automatique. Le BGIA a mené une enquête sur un échantillon de 14 portes tournantes. Les résultats ont montré que les enfants, les personnes handicapées et les personnes âgées étaient particulièrement exposées. Le conférencier a présenté une liste complète de mesures de protection avec trois niveaux de sécurité pour ce type de portes. Les mesures de protection doivent être choisies en fonction de l'évaluation des risques, conformément à la réglementation allemande et européenne. Par ailleurs, le BGIA travaille actuellement sur des principes de tests qui permettront de définir les principales exigences de sécurité relatives aux portes tambour automatiques.

Le quatrième exposé a mis l'accent sur la difficulté d'appréhension de l'architecture d'un système de commande relatif à la sécurité. T. MALM a constaté que les systèmes de commande relatifs à la sécurité assurent des fonctions de plus en plus diverses, avec une part accrue accordée aux logiciels impliquant une complexification de la conception de tels systèmes. Le système peut présenter des failles que le concepteur n'a pas remarquées. Pour concevoir correctement des systèmes, les concepteurs ont besoin de comprendre parfaitement le système et les principes de sécurité. Pour ce faire, les exemples visuels ont fait leurs preuves. Le conférencier a présenté un projet ayant produit 50 exemples de schémas (électriques, hydrauliques, pneumatiques, électroniques, etc.) permettant de visualiser le fonctionnement d'un système de commande relatif à la sécurité par le biais d'une animation.

Cette session principalement basée sur des exemples ou un retour d'expérience sur les systèmes automatisés s'est terminée par l'exposé d'une méthodologie d'analyse du risque adaptée au problème émergent des systèmes automatisés pour l'exploitation minière. Cette méthodologie, basée sur l'analyse de défaillances opérationnelle « OHA - Operating Hazard Analysis », permet de compléter de façon substantielle l'analyse préliminaire des risques « APR » et les études de sous-systèmes « HAZOP » utilisées pour l'analyse des niveaux de sécurité des machines. Cette méthode prend en compte l'interaction entre les opérateurs, le système automatisé dans le cadre des tâches de travail individuelles quotidiennes d'ex-

ploitation et de maintenance. Une étude de cas ainsi que les nouveaux principes de protection et de fonctionnement ont également été présentés.

### SESSION 3 : CONSEILS PRATIQUES & FORMATION

*Animée par E. FADIER (INRS, France) et J. ETHELTON (NIOSH, USA)*

- **Guide pratique pour l'application des catégories de la norme ISO 13849** par R. BOURBONNIERE - IRSST - Canada,
- **prEN ISO 13849 : guide pratique pour l'évaluation des systèmes de commande relatifs à la sécurité** par M. HAUKE - BGIA - Allemagne,
- **Normalisation des guides utilisateurs pour les réseaux dédiés à la sécurité** par Y. MUNETA - OMRON CORPORATION Japon,
- **Développement de la formation aux risques dans les diplômes d'ingénieur de 1<sup>er</sup> cycle** par J. WILLIAMSON - Université de Liverpool - Grande-Bretagne,
- **La création du système d'accréditation de l'évaluateur de risques au Japon** par Y. ISHIDA - Japan Certification - Japon.

En introduction à cette journée, E. FADIER a proposé une communication intitulée « Sécurité proactive en conception : quelques recommandations génériques ». Dans cette conférence, l'auteur a montré, en s'appuyant sur la littérature existante, que la prévention et, plus particulièrement, la sécurité n'est citée explicitement dans l'expression de besoins (dans le cahier des charges) qu'à travers l'obligation réglementaire et, dans le meilleur des cas, à travers les normes techniques en vigueur. La prise en compte du couplage perception-action, l'accessibilité de la machine en fonction des opérations, l'intégration de scénarii de situations possibles (pas de situation unique), la facilitation de l'apprentissage et de la formation par l'outil, à travers une prise en compte des logiques utilisation/fonctionnement, sont des aspects à intégrer en conception.

Lors du premier exposé de cette session, R. BOURBONNIERE rappelait que les dispositifs et leur système de commande associé doivent être conçus conformément aux prescriptions normatives de l'ISO 13849-1:1999. Par contre, il a souligné que les concepts de cette norme sont malheureusement souvent difficiles à interpréter pour les chargés de sécurité des établissements au Québec. Les auteurs ont donc réalisé un guide qui pré-

sente, à partir d'exemples concrets, l'application des principes indiqués dans la norme. Les démarches préliminaires telles que l'appréciation du risque et la réduction du risque, nécessaires pour la sélection de la catégorie adéquate du circuit, sont d'abord présentées. Les concepts spécifiques relatifs à l'ISO 13849 et à ses catégories viennent ensuite compléter l'aspect théorique de ce guide. Enfin, le conférencier a souligné le manque de formation en sécurité fonctionnelle des ingénieurs.

Le second exposé concernait la révision de la norme objet du guide du premier exposé. En partant du constat que les normes CEI 61508 et CEI 62061 sont difficilement applicables aux « petits » systèmes de commande et ne sont pas adaptées aux systèmes de commande utilisant plusieurs technologies (électrique, électronique, hydraulique et pneumatique). M. HAUKE a alors présenté les éléments clefs de la révision de la norme EN ISO 13849, précédemment EN 954. Il a montré que cette révision tente de combiner les exigences déterministes et probabilistes de façon pragmatique.

Lors du troisième exposé, Y. MUNETA a présenté l'intérêt que suscitent les réseaux dédiés à la sécurité pour garantir à la fois la sécurité et la productivité sur le site de production. Suite à des entretiens avec des utilisateurs, des guides ont été créés sur le processus de développement de la sécurité, la validation de la sécurité, le contrôle des documents, la maintenance, la formation. Le conférencier a également souligné que ces guides avaient été proposés au titre de guides normatifs internationaux au sein du CEI/TC44.

Le quatrième exposé est revenu sur la problématique de la formation. Le conférencier a présenté un modèle permettant de définir la formation aux risques comme un ensemble d'objectifs pédagogiques dans l'enseignement supérieur au Royaume-Uni. En effet, les auteurs ont constaté que cette formation n'était pas en adéquation avec les risques que les étudiants pouvaient rencontrer dans leur vie professionnelle. Les résultats d'une évaluation des connaissances des étudiants en matière de risques ont également été présentés.

Le dernier exposé de cette session a présenté le système d'accréditation de l'évaluateur de risques, établi en 2004 au Japon. L'objectif de ce système est de promouvoir les normes internationales

CEI/ISO dans l'industrie japonaise afin d'améliorer la sécurité des machines et des systèmes de production. Ces dernières années, les industries japonaises ont commencé à en reconnaître la nécessité et l'importance mais ont beaucoup de mal à comprendre ces normes. Cette communication a expliqué le programme détaillé du système développé dans ce projet, notamment l'historique, les objectifs, les programmes de formation et les fonctions des trois organismes (NECA, SOSTAP et JC) ainsi que la présélection des évaluateurs et sous-évaluateurs de risques. Ce projet a été promu en tant que projet standard de recherche et développement du ministère japonais de l'Economie, du Commerce et de l'Industrie.

*Cette session a permis de mettre en exergue la difficulté de maîtrise de la part des industriels des concepts relatifs à la sécurité des systèmes et, plus particulièrement, des systèmes de commande notamment à travers l'ISO 13849-1. Les voies préconisées lors de ces présentations sont donc par exemple la formation le plus en amont possible via les étudiants, potentiels futurs industriels, la réalisation de guides ou encore la mise en place d'organisation structurée (système d'accréditation au Japon).*

#### **SESSION 4 : MISE EN ŒUVRE DE LOGICIELS RELATIFS À LA SÉCURITÉ**

*Animée par W. DROTNING  
(Sandia National Laboratories, USA) et  
P. CHARPENTIER (INRS, France)*

- **Le logiciel prend la tête dans les applications relatives à la sécurité** par M. HUELKE - BGIA - Allemagne,
- **Développement d'un logiciel applicatif d'une machine à l'aide des méthodes formelles** par J.C. BLAISE - INRS - France.
- **Développement d'outils pour mesurer la qualité des logiciels** par N. JUNG - University of Applied Sciences Fachhochschule Bonn-Rhein-Sieg - Allemagne,
- **Système de commande intégrant un Automate Programmable Industriel dédié à la Sécurité : une méthode de validation par tierce partie** par J.C. BLAISE - INRS - France.

Lors du premier exposé, et en introduction à cette session, M. HUELKE a présenté un panorama de la problématique liée à l'utilisation de logiciels pour la commande des machines. Une analyse des statistiques d'accidents a révélé que plus de 60 % des accidents relatifs aux

machines fixes surviennent lors du fonctionnement d'une machine sans défaillance apparente. Le conférencier a poursuivi son exposé par tout une série de constats ou de questions relatives aux erreurs logicielles : Peuvent-elles également contribuer aux accidents si l'on considère le nombre important de cas non reportés ? Quelles sont donc les mesures de prévention et les activités applicables ? La plupart des erreurs sont introduites dès les phases de rédaction du cahier des charges et de conception des logiciels ; ce sont principalement des erreurs de raisonnement. Par contre, les erreurs de codage peuvent être revues ou détectées par le biais d'un test fonctionnel. Enfin, les fabricants de machines ayant rarement une bonne pratique du génie logiciel, la programmation d'applications aboutit souvent au prix d'une pression temporelle intense.

Dans la suite de cette problématique, J.C. BLAISE présentait une possibilité de réduire la sensibilité du système aux erreurs logicielles par l'application de méthodes formelles. Les méthodes formelles ayant rarement été utilisées dans le domaine des «machines», l'INRS a mené une étude de faisabilité visant à développer le logiciel applicatif d'une presse mécanique en utilisant deux types de méthodes formelles. Les concepts des deux méthodes formelles employées, la méthode B et une méthode de vérification formelle a posteriori basée sur le model-checking, ont été introduits, ainsi que l'intégration de ces méthodes dans le cycle de développement du logiciel. Une présentation des avantages et des inconvénients liés à l'utilisation de méthodes formelles, en particulier dans le secteur manufacturier, a conclu cet exposé.

Pour le troisième exposé, N. JUNG présentait, quant à lui, les résultats du développement d'outils pour évaluer la qualité des logiciels dans le cadre d'une collaboration de son université avec le BGIA. Cet exposé a présenté un nouvel outil incluant ces critères pour l'analyse des logiciels d'assemblage. L'outil permet d'identifier le langage machine pertinent à partir du texte source à analyser. Une interface utilisateur graphique aide à visualiser la gestion de l'ensemble du projet d'analyse. Cette interface comprend la gestion des données du projet, la configuration du module d'analyse et la visualisation des résultats d'analyse. Deux autres outils ont également été présentés : un module d'analyse pour langage C et un pour les étudiants s'exerçant au langage JAVA. Des résultats

de l'analyse de logiciels industriels ont enfin été présentés.

Enfin, dans le dernier exposé, J.C. BLAISE présentait plus généralement la problématique de la validation d'un système automatisé à base de logiciel. Au SIAS 2003, l'INRS avait présenté quelques approches prospectives pour le développement d'une méthode de validation de machines avec Automate Programmable Industriel dédié à la Sécurité et avait souligné l'importance de la validation de la partie programmable. Quelques outils d'aide à la validation, plus particulièrement dans le domaine des logiciels, avaient été également présentés. Lors de cette édition 2005, les principes généraux de la méthode, développée dans le cadre des activités de certification CE des presses travaillant les métaux à froid, ont été décrits. Le conférencier a montré comment la méthode doit s'appliquer à chaque étape d'un cycle de développement et que cette méthode s'appuie sur des documents, des informations et des résultats de tests fournis par le concepteur mais également sur une confiance justifiée entre le vérificateur et le concepteur.

*Cette session a mis l'accent sur l'importance prise par le logiciel applicatif (plus communément appelé programme automate) dans les systèmes de commande relatifs à la sécurité. Le premier exposé a proposé une introduction générale à la problématique alors que les suivants ont montré que cette problématique pouvait être abordée à différents niveaux : en conception par l'utilisation de méthodes spécifiques de conception, en évaluation par l'utilisation d'outil de mesure de qualité et enfin d'un point de vue méthodologique par la mise en œuvre d'un cadre et d'une démarche pour la validation des systèmes.*

#### **SESSION 5 : SÉCURITÉ FONCTIONNELLE CONCEPT ET APPLICATION**

*Animée par M. SCHAEFER  
(BGIA, Allemagne) et J.J. PAQUES  
(IRSST, Canada)*

- **CEI 62061 : principes, méthodologie et application pour la sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité des machines** par S. FROST - HSE - UK,
- **Quelles normes pour la conception des systèmes de commande relatifs à la sécurité ?** par J.C. BLAISE - INRS - France,

- **Outils techniques pour l'estimation des risques et l'évaluation probabiliste des fonctions de sécurité dans l'automatisation** par B. MYSLIWIEC - Siemens AG - Allemagne,
- **Evaluation possibiliste de la sensibilité aux défaillances de mode commun d'architectures de commande de machines** par P. CHARPENTIER - INRS - France.

Dans ce premier exposé, S. FROST a présenté les principes fondamentaux et la méthodologie de conception contenus dans la norme qui traite de la sécurité fonctionnelle et qui correspond à la mise en œuvre dans le secteur machines de la CEI 61508 : la norme CEI 62061. Cette norme traite des systèmes de commande des machines à base de technologie électrique, électronique et électronique programmable.

Dans le deuxième exposé, J.C. BLAISE a présenté la position de l'INRS sur les possibilités d'utilisation des trois normes existant pour la conception des systèmes de commande relatifs à la sécurité. Cette position est synthétisée dans un diagramme d'aide au choix d'un référentiel normatif qui permet de sélectionner une norme de conception sans pour autant interdire l'utilisation des autres. Le choix de la norme est basé sur des décisions de conception tenant compte de critères tels que la technologie, le type et la complexité des composants utilisés pour assurer les fonctions de sécurité. Ces choix de conception dépendent également de la méthode de conception à savoir l'intégration ou le développement de sous-systèmes. Le conférencier a souligné que toutes ces normes mettaient en jeu de nombreux concepts et des préconisations complexes et que les concepteurs de machine devaient les maîtriser.

Dans la continuité des exposés précédents, B. MYSLIWIEC a souligné que l'évolution des normes (CEI 62061/ISO 13849-1 rev) confirmait la nécessité de nouvelles approches méthodologiques et donc le développement d'outils techniques mettant en œuvre ces approches notamment à travers des exigences accrues concernant le cycle de vie d'une machine, associées à des exigences accrues en matière de documentation. Globalement, ces approches consistent en la définition des fonctions mécaniques et l'analyse documentée des risques correspondants. Chaque danger se voit assigner un risque, ce qui permet de choisir les composants, des capteurs aux actionneurs, remplissant la fonction de sécurité. Après le câblage et la programmation, la fonction doit être

validée (test fonctionnel). Chaque étape doit être documentée au cours du cycle de vie de la machine. La validation qualitative de la fonction s'inspire de la liste des éléments et des schémas de câblage. Pour l'évaluation probabiliste de chaque composant et de la fonction, on peut utiliser des outils mathématiques pour obtenir les informations complètes. Deux exemples de réalisation basée sur cette approche ont été présentés.

Enfin, dans le cadre du dernier exposé, P. CHARPENTIER a souligné que les référentiels applicables à la sécurité des systèmes de commande de machines font maintenant intervenir une évaluation probabiliste pour appréhender l'effet des défaillances aléatoires du matériel sur la sécurité d'une machine. Il faut alors déterminer une probabilité de défaillance dangereuse et considérer notamment des taux de défaillances des composants utilisés, des taux de couverture des tests implantés, mais aussi, lorsque l'architecture est redondante, des défaillances de cause commune. Pour cette étude, une démarche de modélisation de l'imperfection des connaissances de l'analyste (imprécision et incertitude) et l'estimation de la valeur du facteur  $\beta$  ont été formalisées et nuancées en utilisant les concepts d'ensembles flous et de distributions de possibilité. Le conférencier a également montré l'impact des différentes réponses sur le niveau de sécurité et les décisions qui en découlent.

*Cette session a mis l'accent sur l'existence de plusieurs référentiels de conception des circuits de commande à base de technologie électrique, électronique et électronique programmable. Ces référentiels sont en fait complémentaires mais nécessitent une compétence plus grande de la part des concepteurs.*

## SESSION 6 SÉCURITÉ FONCTIONNELLE - TABLE RONDE

*Animée par S. SHAW (HSE, Royaume-Uni) et M. SCHAEFER (BGIA, Allemagne)*

Suite à la session sur la sécurité fonctionnelle une table ronde a été constituée afin de débattre du sujet et de répondre aux questions de l'assistance. Globalement, les principales questions concernaient l'existence de plusieurs référentiels - l'un CEI, l'autre ISO - traitant de sujet similaire mais avec des approches différentes. L'industrie a fait part de sa volonté d'avoir un référentiel unique sans pour autant dénigrer l'un ou l'autre. Cette volonté a été bien reçue par

les animateurs qui ont émis l'idée à terme de travailler dans cette voie. Des remarques ont été faites sur la prise en compte de la sécurité fonctionnelle liée aux modes de production, mais aussi sur le fait que d'autres opérations, telles que l'observation de process et la maintenance, sont rarement intégrées.

## SESSION 7 GESTION DES RISQUES LIÉS AUX SYSTÈMES AUTOMATISÉS

*Animée par J.J. PAQUES (IRSST, Canada) et J. ETHERTON (NIOSH, USA)*

- **Evaluation des risques dans le monde réel** par B. MAIN - design safety engineering inc - Etats-Unis,
- **Evaluation des risques : la méthode hybride** par J. PERSSON - Tetra Pak Carton Ambient AB - Suède,
- **Examen raisonné des outils d'évaluation des risques associés aux machines industrielles** par J.J. PAQUES - IRSST - Canada,
- **Réduction des risques relatifs à l'automatisation : leçons d'une évaluation du NIOSH concernant l'utilisation de l'ANSI B11 TR3 pour la réduction du risque machines au travail** par J. ETHERTON - NIOSH - Etats-Unis,
- **Résultats des tests exploratoires effectués sur des outils d'évaluation des risques associés aux machines industrielles** par J.J. PAQUES - IRSST - Canada.

Pour la première communication de cette session sur l'analyse du risque, B. MAIN a fait un bref exposé de la procédure d'estimation des risques et a présenté quelques unes de ses applications dans le «monde réel». Les exemples étaient : l'analyse d'un système automatisé nécessitant une activité minimale de la part de l'opérateur mais créant des activités de maintenance très contraignantes, l'utilisation de l'analyse des risques lors d'une inspection de l'OHSa suite à un accident, le développement de nouveaux produits, prototypes et machines chez différents constructeurs. Le conférencier a conclu en soulignant l'importance de l'analyse des risques qu'il a jugé comme l'étape incontournable d'une bonne prise en compte de la sécurité.

Lors de cette deuxième communication, J. PERSSON a présenté comment Tetra Pak® menait une évaluation des risques par le biais d'un formulaire associant des paramètres qualitatifs et quantitatifs. Au fil des ans, cette procédure d'évaluation des risques a permis d'assurer de façon appropriée la sécurité des machines.

Elle est annexée à la norme CEI 62061 afin de donner un exemple de méthode de détermination du SIL (Safety Integrity Level ou niveau d'intégrité de sécurité) nécessaire pour un système de commande électrique relatif à la sécurité. Elle se trouve également sous forme d'annexe dans l'ISO 14121 comme exemple de procédure d'évaluation des risques. Cette dernière englobe l'identification des risques, l'estimation et l'évaluation des risques et indique si la sécurité est assurée de façon appropriée ou si une réduction des risques supplémentaire est nécessaire.

Le troisième exposé concernait un projet commun entre l'IRSST, l'UQTR et l'INRS visant à analyser et classer plus de 250 documents décrivant les méthodes et les outils d'évaluation des risques associés aux machines industrielles. Ces documents ont été élaborés à partir de normes, de guides techniques et de procédures d'entreprises industrielles. Par le biais de paramètres précis, cette analyse a classé de façon théorique les outils ou les méthodes d'évaluation des risques enregistrés et identifié leurs points communs ou leurs spécificités. Les principales catégories de méthodes et d'outils proposés dans les documents analysés et les méthodes sélectionnées pour les essais ultérieurs ont été présentées.

Dans le quatrième exposé, J. ETHERTON a présenté les résultats d'une évaluation de l'efficacité de l'ANSI B11 TR3 chez les utilisateurs de systèmes de machines industrielles, dont certains étaient automatisés.

Résultats :

1) les équipes chargées de l'évaluation des risques peuvent fonctionner de manière efficace ;

2) la formation à l'évaluation des risques est directement liée au nombre d'actions de réduction des risques menées par l'équipe ;

3) moins une équipe a de connaissances préalables sur l'évaluation des risques, plus le nombre d'actions de réduction des risques est important.

Le conférencier a conclu que l'évaluation des risques selon la norme B11 TR3 et les méthodes de réduction des risques peuvent être appliquées dans de bonnes conditions par les utilisateurs de systèmes automatisés.

Cette session s'est terminée par l'exposé de J.J. PAQUES concernant les résultats des tests exploratoires effectués sur des outils d'évaluation des risques associés aux machines industrielles. Ces

tests ont permis de s'interroger sur la manière dont les sujets voient ou perçoivent les risques associés à certaines situations dangereuses dans l'environnement de production industrielle ; l'un des tests a permis de se focaliser sur la convergence des résultats afin d'estimer un indice de risque ; un autre a permis de comparer les performances théoriques et pratiques de 4 outils d'estimation et d'évaluation des risques associés aux machines industrielles. En général, ces tests donnent uniquement des résultats qualitatifs. Les populations impliquées dans ces tests étaient des industriels (experts ou fonctionnels de sécurité) ou des universitaires (étudiants de troisième cycle ou en formation continue).

*Cette session dédiée aux travaux sur l'analyse du risque a montré à quel point cette étape indispensable d'une démarche de prévention suscite encore de nombreuses questions. Que ce soit au Canada ou au Japon à travers les communications proposées, on s'aperçoit de la difficulté de maîtrise des concepts liés à l'analyse du risque et notamment de ces notions subjectives.*

## **SESSION 8 : EXPÉRIENCES PRATIQUES SUR LES DISPOSITIFS DE PROTECTION**

*Animée par E. FADIER (INRS, France) et M. DZWIAREK (CIOP, Pologne)*

- **Développement d'un nouvel interrupteur d'urgence permettant d'assurer la sécurité des opérateurs en cas de défaillance prévisible** par T. SAKAI - Idec Izumi Corporation - Japon,
- **Définition des arrêts - arrêts d'urgence et de protection** par G. DOMINGUEZ - Rimrock Automation Inc. - Etats-Unis,
- **Raisons de la manipulation (mise en échec) des dispositifs de protection** par M. SCHAEFER - BGIA - Allemagne,
- **De nouvelles solutions au problème d'entrée-sortie** par O. GORNEMANN - SICK AG - Allemagne.

Lors du premier exposé de cette session T. SAKAI a rappelé l'importance, dans le domaine de la sécurité, du rôle joué par les interrupteurs de sécurité type arrêt d'urgence. L'analyse des modes de défaillance et de leurs effets a mis en évidence que la conception actuelle de ces éléments ne permettait pas d'interrompre le fonctionnement du système en cas de mauvaise installation ou de sollicitation avec une force excessive. L'origine de ce comportement est due au fait que le niveau d'énergie des interrupteurs d'arrêt d'urgence conventionnels est bas en

mode normal et élevé lors d'une sollicitation. Le conférencier a présenté les principes retenus pour la prochaine génération d'interrupteurs d'arrêt d'urgence. Elle sera conçue selon un principe innovant où le niveau d'énergie sera inversé.

La norme américaine RIA R15.06 relative à la sécurité robotique contient deux types d'arrêts : arrêt d'urgence et arrêt de protection. G. DOMINGUEZ a précisé que le terme «arrêt d'urgence» a été le seul utilisé par le personnel pour décrire l'arrêt d'une machine dans une situation de sécurité. Cependant, cette appellation est erronée et il est nécessaire de différencier ces deux types d'arrêt. Pour cela, le conférencier a présenté un tableau comparatif pour illustrer les différences entre ces types d'arrêts ainsi que les applications et circuits de sécurité associés.

Lors du troisième exposé, les études sur les accidents menées par les BG dans le secteur industriel indiquent que les dispositifs de sécurité des établissements sont volontairement contournés. Afin de posséder plus d'information sur ce sujet, une étude menée par le BGIA et le BGAG est actuellement en cours. Les premiers résultats confirment que le contournement est un phénomène fréquent dans les entreprises. M. SCHAEFER a présenté les axes d'amélioration possibles, notamment concernant la conception de l'interface homme/machine.

Lors du dernier exposé de cette session, O. GORNEMANN a mis l'accent sur l'accroissement simultanée des exigences de performance des machines modernes et des équipements industriels ainsi que sur les risques liés à l'interaction homme/machine. Pour assurer la protection des personnes, les technologies «éprouvées» atteignent leurs limites sans que les nouvelles technologies industrielles les remplacent ou les améliorent. Actuellement, la véritable innovation est l'utilisation conséquente des microprocesseurs et des bus de terrain dans les applications de sécurité. Après avoir présenté les nouvelles solutions pour pallier les problèmes relatifs aux entrées - sorties, le conférencier a esquissé le futur dans ce domaine en précisant que des dispositifs de sécurité basés sur la vision apparaîtront et remplaceront peut-être les dispositifs existants d'ici 3 à 5 ans.

*Cette session dédiée aux dispositifs de protection a mis l'accent, d'une part, sur l'évolution technologique de ces derniers mais*

aussi sur la nécessité de clarifier les concepts, plus particulièrement dans le domaine des arrêts. Enfin, la problématique relative au contournement des dispositifs de sécurité reste une préoccupation majeure des préventeurs.

## SESSION 9 : INNOVATION ET AVENIR

Animée par J.J. PAQUES (IRSST, Canada)  
et J. ETHELTON (NIOSH, USA)

- **Système neuronal avec reconnaissance avancée des situations de danger pour le contrôle de la sécurité** par R.A. KOSIŃSKI - CIOP — Pologne,.
- **Application de l'identification par radio-fréquence pour la sécurité** par T. IIDA - NECA - Japon,
- **Interface sans fil et d'identité pour le système LAMI (Local Area Machine Interaction)** par D. GENON - CATALOT - Institut National Polytechnique de Grenoble - France,
- **Protection des doigts et de la main sur les scies circulaires et à panneaux** par D. REINERT - BGIA - Allemagne,
- **Distance entre les lignes à haute tension et les arbres** par D. REINERT - BGIA - Allemagne,
- **Evolution de la norme de sécurité pour l'utilisation des robots mobiles en interaction avec l'Homme** par R. BOSTELMAN - NIST - Etats-Unis.

Le premier exposé a présenté un nouveau concept de protection des robots. Le conférencier est parti du constat que les postes de travail robotisés sont fréquents dans l'industrie et que les systèmes de sécurité classiques tels que les protecteurs fixes, les protecteurs interverrouillés, les barrières lumineuses, les appareils sensibles à la pression ou les détecteurs laser présentent différents inconvénients, notamment leur sensibilité à l'apparition aléatoire, dans l'environnement des robots, de petits objets ne provoquant pas de situation dangereuse. Le système présenté permet la reconnaissance avancée des situations de danger. Il peut réagir de façon intelligente à la situation qui survient dans l'environnement du robot et décide si la situation est dangereuse ou non. Ce système se subdivise en trois parties : une unité visuelle, des réseaux neuronaux et un système à base de règles. Un certain nombre de paramètres ajustables le rend adaptable à différents types de robots et de process. Par ailleurs, il est applicable à l'observation intelligente des pièces, des immeubles, etc.

Le deuxième exposé avait pour thème la limite actuelle des dispositifs de sécurité

utilisés lorsque l'homme et la machine coexistent. Ces équipements permettent de détecter uniquement la présence d'une personne mais ne peuvent pas identifier chaque opérateur. Si l'utilisation de clefs prisonnières apportent un début de réponse, l'identification de chaque opérateur demeure cependant difficile. Afin de répondre aux exigences du référentiel OHSAS 18001 relatif au système de management de la santé et de la sécurité au travail, il est possible de mettre en œuvre des badges d'identification par radio fréquence. Trois exemples ont été présentés ; le premier concerne un contrôle d'accès, le second le démarrage d'une machine et le dernier une localisation d'opérateur en temps réel. En conclusion, le conférencier précise que la mise en œuvre de ces applications soulève plusieurs questions et que les principaux axes de recherche pour les techniques de base portent sur l'augmentation de la sûreté des technologies de la communication (autodiagnostic du badge ou autodiagnostic de l'environnement électromagnétique, par exemple). D'autres aspects importants concernent la standardisation des procédures de commande (accès interdit aux personnes ne portant pas de badge, par exemple) et la standardisation d'une méthode de détection des personnes ne portant pas de badge grâce à une méthode de détection différente, combinée à l'identification par radio-fréquence.

Le troisième exposé présentait un dispositif de sécurité, actuellement en cours de développement, reposant sur une liaison sans fil. L'interface assurera trois fonctions principales :

- 1 - interface de système sans fil pour machines d'opération de maintenance à distance donnant plus d'informations pour les opérations de maintenance, en particulier lorsque la personne chargée de la maintenance est à côté de la machine (informations plus détaillées) ;
- 2 - identification personnelle par détection permanente d'un dispositif d'identification par radio-fréquence passif attaché aux vêtements ou autre (montre, badge, etc.) ;
- 3 - dispositif de positionnement par radio-fréquence avec caractéristiques «itinérantes» dues à une interface asymétrique avec le système LAMI.

Le prototype sera testé sur le terrain cette année.

Lors du quatrième exposé, en partant du constat que les solutions actuelles de sécurité pour les scies ne fournissent pas encore de protection adéquate, D. REINERT a présenté de nouvelles approches pour assurer la sécurité des opérateurs sur ce

type de machine. Basé sur une détection sans contact des doigts, ces nouvelles approches sont destinées à assurer une protection totale et économique sur les scies circulaires. Ces principes fondamentaux peuvent également s'appliquer à d'autres types de machines à chargement et/ou déchargement manuel. L'une des solutions comprenant un capteur infrarouge passif associé à un capteur capacitif a permis de développer un dispositif de protection sûr et fiable assurant une diversité fonctionnelle. Le protecteur protège la main de l'opérateur dans un délai de 50 ms. Les forces du système de protection sont inférieures à la valeur de crête de 150 N. Une autre solution intégrant des images vidéo a été étudiée. Cette solution permet à son tour de détecter des doigts/pouces des individus.

Le cinquième exposé a présenté un dispositif permettant d'évaluer les distances entre les lignes haute tension et les arbres afin d'assurer la sécurité des élagueurs en leur fournissant une information fiable et facilement exploitable. Le principe de ce dispositif est le suivant : grâce à un détecteur laser, pivoté par un moteur pas-à-pas, une image 3D de l'environnement des lignes à haute tension est enregistrée. Le système peut mesurer précisément la distance entre les arbres et les lignes à haute tension. Il est prévu de calculer des paraboles en trois dimensions pour estimer aussi les lignes à haute tension masquées par la végétation.

Le dernier exposé était consacré à la protection des opérateurs travaillant à proximité des robots mobiles. R. BOSTELMAN a présenté les normes de sécurité US ASME B56.5 : 2004 et EN 1525 : 1998, une nouvelle caméra 3D, des expériences sur les capteurs sans contact, les algorithmes de détection et de segmentation d'obstacles et leurs résultats. Enfin, le conférencier a formulé des recommandations pour l'évolution des normes de sécurité visant à protéger les opérateurs travaillant à proximité des robots mobiles.

*Cette dernière session traitait principalement des nouveaux concepts de sécurité liés à l'interaction homme/machine. Si les protections actuelles reposent principalement sur des sécurités «physiques» (protecteur, barrière lumineuse...), les futures sécurités seront plus «intelligentes» et reposeront entre autres sur des analyses d'images, des communications sans fils... On peut noter, en particulier, le dispositif novateur pour améliorer la sécurité des élagueurs travaillant à proximité des lignes électriques haute tension.*

## CONCLUSION

Sans qu'il y ait eu de session dédiée aux facteurs humains, ce congrès a sans cesse évoqué le rôle et la place de l'homme dans les systèmes automatisés, et surtout les effets et les causes liés aux activités humaines et issus des coopérations entre l'homme et le système automatisé. De ce fait, on retrouve dans bon nombre de présentations des recommandations liées à la conception des systèmes automatisés en tenant compte de l'homme utilisateur de ces systèmes. On peut, évidemment, citer la communication d'E.

FADIER mais également celles de la première session concernant les problèmes de coopération entre l'homme et le robot, celle de M. SCHAEFER qui a exposé les raisons du contournement des dispositifs de sécurité par les opérateurs et proposé des solutions de prévention prenant en compte tous les facteurs concernés (homme, technologie et organisation). De même, l'ensemble des communications relatives au retour d'expérience des accidents survenus dans les systèmes automatisés a souligné la difficulté de la conception d'une sécurité sûre et intégrée d'un système industriel automatisé sans une

véritable connaissance de l'activité humaine mise en jeu lors de l'utilisation et de l'exploitation de ces systèmes.

Dans le même ordre d'idée, on peut souligner la récurrence de la problématique liée aux activités autres que la production «normale», par exemple la maintenance. Enfin, la persistance de la problématique liée à la sécurité fonctionnelle est également à retenir de ce congrès qui s'est clos sur la prise de rendez-vous pour la prochaine édition qui devrait avoir lieu au Japon en 2007.