Quelle Sécurité Machine en 2020 ?

2e volet

Interrogés par Jautomatise, 12 experts de la sécurité machine se sont prêtés au jeu des questions/réponses sur le devenir de la sécurité machine, face aux nouvelles technologies, à l'évolution des habitudes de conception et aux besoins de productivité toujours plus grands.
Suite et fin de l'enquête (le premier volet est paru dans Jautomatise n° 57) donnant la parole aux fabricants et intégrateurs, ainsi qu'à l'INRS.

AUJOURD'HUI

Plusieurs réseaux d'automatisme offrent la possibilité de gérer à la fois le contrôle-commande et la sécurité. Quelles sont, à terme, les limites d'intégration des composants de sécurité machine avec les composants d'automatisme ? Y a t-il une limite de la sécurité « répartie » ?

Volker Rohbeck, spécialiste sécurité machine et responsable de marché chez Leuze Electronic Allemagne avance des limites d'ordre technico-économiques : *« Il existe des limites techniques, conditionnées par le nombre de composants admissibles sur un bus, directement fonction de la plage d'adressage. Par exemple, AS-i Safety donne droit à 31 adresses et Profibus 126 adresses. Cette limite est aussi fonction de l'allongement du temps de réaction, qui prend toute son importance spécialement lors de la sécurisation de postes dangereux avec des barrières immatérielles. Mais surtout, le plus important sera le surcoût de ces composants connectables au bus de sécurité par rapport aux composants non connectables. Ainsi, aujourd'hui, l'intégration d'une connexion Profisafe dans un scrutateur laser ou dans une barrière de sécurité de haut de gamme est justifiée par son intérêt économique. En revanche, cela perd de son intérêt pour des composants plus simples et d'un coût moindre tels que les inter-verrouillages de sécurité, et ceci même dans un avenir prévisible, avec le développement de nouveaux bus de sécurité, qui sont souvent basés sur la technologie relativement coûteuse qu'est Ethernet Industriel. »*

« Sur les petites machines, explique **Mats Linger**, pdg de Jokab Safety AB et de Jokab Safety France, *le programme de commande est plus court et plus facile à maîtriser dans son ensemble. Il est alors possible de mélanger commande et sécurité. En revanche, pour des programmes plus longs et des systèmes plus complexes (part exemple plusieurs machines qui interagissent), il est préférable de séparer les systèmes de commande et de sécurité, aussi bien du point de vue de la sécurité que de la production. Si sécurité et commande sont regroupées dans le même programme, à chaque modification de programme, quel que soit le type de modification, la machine devra être soumise à une nouvelle procédure de certification durant laquelle le système de protection entier doit être testé.*

Du point de vue de la production, la séparation permet une plus grande flexibilité puisqu'il est possible de modifier le programme de commande (optimisation ou évolution) sans avoir à se soucier d'une nouvelle procédure de contrôle des fonctions de sécurité. De plus, si commande et sécurité sont mélangées, une modification de la commande peut avoir une influence sur les temps de réponse de la machine, essentiels à sa conception du point de vue de la sécurité.

La séparation permet d'utiliser des bus différents pour la commande et la sécurité et de réduire ainsi les temps de réponse pour les aspects de sécurité. Plus le temps de réponse est faible, plus la distance de sécurité est courte et il est alors possible d'utiliser des systèmes de protection sans contact au lieu de portes d'accès, d'où un impact, d'une part sur la productivité et d'autre part sur la convivialité du système de protection… et donc finalement sur la tendance à la fraude des protections. »

Coté intégrateur, selon **Thierry Vallenet**, directeur Actemium région Auvergne, en charge de l'animation du club Actemium « Biens d'équipements », *« il n'y a pas de limites. Les technologies permettent la convergence de la partie opérative et de la sécurité (matériel/technologique & état d'esprit). »*

Marc Guyon, responsable études automatisme, chez BBR Automation, rappelle : *« De nos jours il n'est pas recommandé de faire confiance aux automates programmables industriels standards pour gérer la sécurité. Il est préférable de gérer celle-ci par une logique câblée extérieure à la commande de l'API standard. Suivant le type d'application « machine de séries », « machines spéciales », l'intégration d'un API de sécurité peut-être utile. Alors que pour les « lignes automatisés », une logique câblée extérieure à la commande API reste une solution viable et maintenant connue. »*

Enfin, pour **Philippe Charpentier**, département Ingénierie des Équipements de Travail, responsable du laboratoire Sûreté des Systèmes Automatisés de l'INRS, *« la limite d'intégration des composants de sécurité machine avec les composants d'automatisme est liée à*

l'existence d'outils de développement adaptés, en particulier pour la validation des applications envisagées. Dans tous les cas, elle devra au-moins tenir compte de la capacité des concepteurs à concevoir et valider le niveau de sécurité de leurs installations.

En ce qui concerne la sécurité répartie, une limite spécifique résidera dans le respect des contraintes de temps des applications, primordiales dans l'industrie manufacturière. »

Le fait de mêler la sécurité machine aux fonctions d'automatisme n'est-il pas pénalisant, et même dangereux pour la sécurité, lorsque l'on doit modifier rapidement une partie de l'automatisme ? N'est pas un handicap pour la maintenance ?

Marc Guyon, BBR Automation, avance prudemment : *« Le fait de mêler sécurité et partie fonctionnelle apporte un risque de détérioration de la sécurité machine. Car les mémoires et entrées/sorties de l'API sont les mêmes pour les deux types de gestion. Quant à la maintenance, le but est de maintenir en fonctionnement les machines et de mettre en place des actions préventives. La majeure partie des nouvelles installations ou modifications des installations existantes est sous traitée. »*

Thierry Vallenet, Actemium, considère plutôt l'enjeu de la formation : *« Cela ne peut être un handicap, dans la mesure où la sécurité machine se doit d'être structurée au moment même du développement des automatismes. La seule contrainte, qui est par ailleurs une obligation permanente, consiste en la mise à niveau des équipes. »*

Chez Leuze Electronic, **Volker Rohbeck**, voit cette évolution de façon positive : *« Il reste possible de transmettre des données d'automatisme et des données de sécurité sur des bus séparés, même si un seul bus est capable de mêler ces deux types de données. Bien sûr, l'automate programmable en charge du programme de sécurité doit prendre en compte l'application. Tout comme l'automaticien qui effectue le câblage et la programmation. De plus, les programmes de sécurité sont normalement protégés par mot de passe, toute modification est enregistrée et peut être retracée très facilement grâce aux fonctions d'historique et d'archivage intégrées aux appareils. La plupart du temps, modifier un programme est plus simple à visualiser, à représenter et à documenter que modifier un câblage classique.*

Contrairement au câblage classique de composants de sécurité, la transmission des informations sur un bus de sécurité ne peut pas être manipulée avec des moyens simples, ce qui est une garantie pour la sécurité globale de l'installation. »

A l'INRS, **Philippe Charpentier** met en garde contre les effets d'interaction : *« L'intérêt de séparer fonctions de sécurité et fonctions de commande est de faciliter le développement et la validation des parties relatives à la sécurité. En revanche, une telle stratégie ne permet de développer que des applications relativement simples. Dans le cas où la séparation n'existe pas, le concepteur devra veiller à ce que les modifications ou les actions de maintenance faites au niveau de la partie fonctionnelle n'affectent pas les sécurités. En toute rigueur, le travail à réaliser sera donc beaucoup*

plus conséquent. Dans le cas de certains réseaux dédiés à la sécurité, il faudra notamment s'assurer que les modifications de la partie fonctionnelle n'influent pas sur les temps de réponse de l'application.

Les tâches de modification et de maintenance seront facilitées par la mise à disposition d'outils et ateliers de développement adéquats. Elles devront être encadrées avec la même rigueur que le développement initial de l'application. »

Finalement est-ce rentable pour le client, et ne va t-on pas vers des « usines à gaz » trop complexes, notamment lors de modifications de production de plus en plus courantes chez les industriels ?

Thierry Vallenet, Actemium, chiffre les gains : *« Les systèmes efficaces et bien structurés doivent pouvoir prendre en charge les changements de production et de campagne sans phénomène de type « usine à gaz ». Par ailleurs, avec le déploiement de solutions toujours plus souples on assiste à la migration d'une sécurité à logique câblée vers une sécurité à systèmes programmables. Pour preuve, en série, bien que le matériel représente un coût plus important, le passage vers des systèmes de sécurité sur automate permet des gains pouvant aller jusqu'à 30 % sur l'ensemble de la prestation d'électricité et automatismes. »*

« Bus et automates de sécurité sont intimement liés, souligne **Volker Rohbeck**, Leuze Electronic. *La modification par téléchargement du paramétrage des capteurs et des actionneurs sur un bus de sécurité est très simple et exempte d'erreurs, par comparaison avec celle réalisée sur site au moyen d'un ordinateur portable ou bien par modification du câblage.*

Si la structure même du système de sécurité doit être modifiée, il est bien plus facile, plus sûr et moins coûteux de modifier le programme que d'intervenir sur le câblage des composants. »

Marc Guyon, BBR Automation, revient sur la notion de coût : *« La répartition de la sécurité et du fonctionnement d'une machine sur deux automates permet d'effectuer les modifications au mieux, tout en réduisant les erreurs possibles. Cependant, au coût d'un API standards il faut ajouter un API de sécurité (dans certaines configurations), cela nécessite de la programmation supplémentaire. Il reste en plus à valider l'ensemble de la programmation et de l'installation électrique par un organisme de sécurité. »*

L'INRS ne peut pas se prononcer en terme de rentabilité d'un point de vu client. *« En revanche*, explique **Philippe Charpentier**, *pour faire face à la complexité croissante des applications automatisées, due notamment à l'utilisation de composants d'automatismes tels qu'automates ou réseaux dédiés à la sécurité, nous préconisons en particulier de :*
- S'assurer du niveau de formation des différents intervenants d'un projet basé sur ces technologies. La formation, proposée par exemple par les fabricants de composants, devra leur permettre d'une part d'avoir une parfaite compréhension de la mise en œuvre et de la configuration du matériel utilisé dans l'application à concevoir et d'autre part de posséder la maîtrise des outils et des langages de paramétrages et de programmation ;
- Respecter les consignes énoncées dans les différents guides et notices rédigés en support aux composants utilisés, ce qui impose notamment aux fournisseurs de mettre à disposition une documentation complète et lisible pour chacun des composants impliqués dans le traitement des sécurités. »

DEMAIN

Avec l'arrivée récente des liaisons sans fil dans certaines applications industrielles, d'autres interrogations se font jour. Les liaisons filaires de sécurité actuelles laisseront-elle la place à d'autres technologies comme la fibre optique ou la communication sans fil ? Et dans quel but ?

Mats Linger, Jokab Safety : *« La sécurité sans fil sera probablement utilisée sur les dispositifs mobiles qui excluront tout autre type de sécurité. Une sécurité sans fil signifie des temps de réponse plus longs par rapport à un système câblé. Car un système de sécurité doit contrôler en permanence le fait que la communication soit établie et en cas d'interruption (ce qui correspond à un câble coupé), les fonctions dangereuses doivent êtres stoppées. Pour que la production ne soit pas interrompue inutilement, il faut soit des temps de réponse longs pour contrôler que l'interruption n'est pas due à une perturbation, soit un environnement complètement dépourvu de perturbation. Un temps de réponse d'au moins 300 ms est courant pour un système sans fil seul. Il faut y ajouter le temps de réponse des dispositifs de protection et le temps de freinage de la machine. Avec une vitesse d'approche de 1,6 m/s pour une personne qui marche, ce temps de réponse donne une distance de sécurité de 1 m pour une barrière immatérielle multifaisceaux. Il faut y ajouter la longueur d'un bras, au moins 850 mm, ce qui fait finalement 2 m, une distance inacceptable. La solution pourrait être une cartérisation mais le temps nécessaire pour la contourner nuit à la productivité. Une solution par fibre optique pourrait diminuer les temps de réponse. »*

Volker Rohbeck, Leuze Electronic est catégorique : *« Le support de transmission des données dans certains bus de sécurité n'a aucune influence sur la sécurité elle-même. Soit, on dynamise la structure des données standard, par exemple AS-i Safety at Work ; soit, on la sécurise par des moyens additionnels, tel PROFIsafe. En raison de la compatibilité avec les composants de bus existants, aucune modification n'a été faite au niveau du processus de transmission des bits d'informations. Si la transmission de données d'automatisme standard est possible, alors celle de données de sécurité l'est aussi. Dans ces bus, le support de la transmission n'a aucune importance, que ce soit de la fibre optique, du câble, de la transmission sans fil ou de la transmission optique de données. »*

Thierry Vallenet, Actemium, se dit prêt : *« Sans attendre demain, nous avons à notre actif l'intégration de réseaux d'automates dialoguant entre eux par fibre optique, chez Rockwool par exemple. Dès demain, on peut imaginer au-delà du dialogue fonctionnel celui des paramètres de sécurités. Les intérêts en la matière sont multiples : limiter les problèmes liés à la connectique et ainsi les probabilités de panne ; la nécessité d'optimiser les coûts considérant qu'aujourd'hui en intégra-*

tion électricité et automation, la main d'œuvre représente une part significative de ceux-ci.

En fait, il s'agit pour nous d'un changement de « métier ». De fait la sécurité passe du domaine de l'électrotechnicien à celui de l'automaticien ».

« Les liaisons en fibres optiques sont déjà sur le marché et permettent d'améliorer sensiblement les temps de communication, et par conséquent de baisser les temps de réponse des applications, rappelle **Philippe Charpentier** à l'INRS. *Les liaisons sans fil augmenteront la souplesse des installations, mais auront certainement pour conséquence un allongement des délais de réponse à des fins de sécurisation des transferts d'informations. D'un point de vue sécurité, le recours à ces nouveaux supports de communication ne devra se faire que si des organismes compétents ont validé le concept général (protocole, architecture matérielle…), puis chacun des composants pour lequel son constructeur revendique une compatibilité avec le profil de communication de sécurité en question. »*

Est-il probable de voir une sécurité des machines sans-fil ? Sinon, utiliser le même média que pour les automatismes sans-fil deviendra donc impossible ?

Et toujours la question du coût… *« Aujourd'hui il est techniquement possible de transmettre des données de sécurité par liaison sans fil*, précise **Volker Rohbeck**, Leuze Electronic. *Cela reste une question de coût, et de savoir combien et quels types de composants de sécurité doivent communiquer par liaison sans fil. Mais actuellement et à moyen terme, faire communiquer entre eux des composants de sécurité par liaison sans fil est dénué d'intérêt ! »*

Cependant, pour **Marc Guyon**, BBR Automation, *« Il semble difficile d'avoir le même niveau de sécurité entre des liaisons filaires pour gérer des actionneurs et une communication sans fil ! »*

Et **Philippe Charpentier** de l'INRS de conclure : *« A terme, il est envisageable de voir des fonctions de sécurité mettre en œuvre des technologies sans fil, à condition notamment que les critères en temps de réponse et de disponibilité soient respectés et que les concepts et composants aient été validés par un organisme compétent. »*

Il est facile de contrôler et de valider des équipements matériels de sécurité. Cela est beaucoup plus complexe lorsqu'il s'agit de composants logiciels. La sécurité machine deviendra-t-elle de plus en plus un jeu d'assemblage à base de blocs fonctionnels encapsulés et validés par le constructeur ?

Oui pour **Mats Linger**, Jokab Safety : *« Les blocs de fonction facilitent considérablement la programmation pour le concepteur car ils assurent une grande partie des fonctions de sécurité. On peut les comparer aux relais de sécurité qui ont facilité le travail du concepteur en prenant en charge la redondance et le contrôle des fonctions de sécurité. De plus, il est possible de commander des blocs spécifiques ou de développer ses propres blocs et de les faire contrôler par le fabricant ou un organisme agréé. La validation d'un système de sécurité programmé n'est pas différente de la validation d'un système à relais : toutes les modifications doivent être testées et chaque dispositif de sécurité activé pour vérifier que la machine se comporte comme prévu. Un logiciel permet de voir en ligne ce qui se passe quand un dispositif est activé et de contrôler que ce qui est observé sur l'écran correspond à ce qui se passe dans la réalité (la machine s'arrête à l'ouverture des contacteurs par exemple), ce que ne permet pas aussi facilement un système câblé. »*

Volker Rohbeck, Leuze Electronic, confirme : *« Oui cela deviendra plus facile, car la connexion de blocs fonctionnels est plus simple et plus économique qu'un câblage complexe dans des applications de moyenne et grande importance. De plus, elle est moins dangereuse que la programmation libre. Les blocs fonctionnels correspondent au relais de sécurité classique avec des fonctions déterminées et peu de paramétrage. Les connexions logicielles entre les blocs fonctionnels et les entrées-sorties du programme correspondent au câblage entre les relais et les capteurs/actionneurs. »*

C'est certain pour **Thierry Vallenet**, Actemium *« Dans la mesure où c'est son rôle, le constructeur s'affère à fournir plus de valeur ajoutée à son offre et à ses produits. »*

Oui dans le cadre des conceptions standard pour **Marc Guyon**, BBR Automation, *« Il sera toujours difficile d'imaginer pour des machines spécifiques, des blocs standards de sécurité. En revanche, pour l'industrie automobile où certains process sont répétables, il est envisageable de créer des blocs de sécurités. Les logiques câblées étant déjà standardisées au maximum pour réduire des coûts d'études. »*

L'INRS approuve, toutefois, **Philippe Charpentier** tient à préciser qu'il n'est pas facile de valider des équipements de sécurité mettant en œuvre du matériel et du logiciel. *« Force est de constater que les évolutions actuelles des automatismes s'orientent vers l'utilisation de blocs fonctionnels validés par des organismes de contrôle compétents. Il est alors essentiellement question pour les automaticiens de concevoir un programme à partir de ces modules. Les référentiels actuels en sécurité des machines (ISO 13849-1 et CEI 62061) ont été essentiellement rédigés pour développer les parties relatives à la sécurité dans cette optique. D'un point de vue sécurité, cette évolution a généralement pour intérêt de formaliser les différentes phases du développement, facilitant ainsi la phase de validation de la sécurité. »*

Comment l'automaticien va t-il s'y retrouver pour sécuriser son îlot de production ?

« Pour toutes les études d'automatisme, il existe une analyse de risque. Il est possible d'imaginer une fonction arrêt d'urgence, une fonction barrière immatérielle… », rappelle **Marc Guyon**, BBR Automation.

« Former les automaticiens à l'outil permettant de gérer la sécurité de la machine constituera demain plus encore qu'aujourd'hui une nécessité, un pré-requis indispensable », complète **Thierry Vallenet**, Actemium.

Vision technologique pour **Volker Rohbeck**, Leuze Electronic : *« Là où l'automaticien utilise*

aujourd'hui des relais de sécurité, il utilisera à l'avenir de plus en plus de blocs fonctionnels logiciels dans le programme de l'automate de sécurité. Là où il utilise du câblage entre les relais, il utilisera des connexions logicielles. »

Attention à la maîtrise de l'évolutivité ! *« Il faudra que les constructeurs mettent à disposition des automaticiens les outils nécessaires à développer leurs applications, de la phase d'expression du besoin à la phase de validation finale, mais aussi dans la maîtrise de l'évolutivité des îlots de production »*, ajoute **Philippe Carpentier** de l'INRS.

Le temps où le constructeur de machine câblait quelques relais de sécurité, barrières et arrêts d'urgence semble terminé. La sécurité machine a-t-elle tendance à devenir plus simple ou plus complexe ?

Plus simple pour Leuze : *« A l'avenir, il y aura de plus en plus de capteurs et d'actionneurs souvent paramétrables, dans des applications complexes. La complexité sera maîtrisée par l'automate de sécurité sur la base de blocs fonctionnels logiciels standardisés, qui assureront une bonne vue d'ensemble de l'application.*

Des applications de complexité équivalente deviendront alors plus faciles à réaliser et l'on pourra plus facilement réaliser et maîtriser des applications encore plus complexes », explique **Volker Rohbeck**.

Même tendance pour **Mats Linger**, Jokab Safety : *« Le câblage d'une vingtaine de relais de sécurité est bien plus compliqué que la programmation de la même fonction dans un automate. Un bloc de fonction remplace un relais, le câblage est simplifié et la visualisation en ligne facilite considérablement la mise au point et la recherche de panne.*

La programmation offre davantage de possibilités que le câblage. Toutefois, la complexité dépend essentiellement de la facilité à discerner les différentes fonctions réalisées et donc la structure du programme. Si le logiciel de programmation permet de structurer le programme, la sécurité sera plus simple. Les performances des produits disponibles sur le marché varient considérablement à cet égard et la réponse à cette question dépend du matériel utilisé. »

Un nouveau métier pour Actemium : *« La fonction sécurité demeure telle qu'elle est, néanmoins c'est sa mise en œuvre qui évolue. Hier du simple câblage et demain plus encore qu'aujourd'hui elle consistera en de la programmation. Une fois encore, il s'agit pour nous d'un nouveau métier. Demain l'automaticien-intégrateur apportera avec lui quelques câbles pré-moulés et éléments de connectiques, le reste sera du ressort de la programmation »*, ajoute **Thierry Vallenet**.

Plus facile à terme pour BBR Automation : *« L'arrivée des automates de sécurité induit l'étude de nouvelles solutions, qui au départ restent difficiles à appréhender. A terme, cette solution devrait permettre de faciliter la prise en compte de la sécurité des machines, leur*

SÉCURITÉ DES MACHINES : UN GUIDE DU ZVEI EN FRANÇAIS !

La fédération professionnelle de l'industrie électronique et électrotechnique allemande a publié un guide d'une vingtaine de page sur l'interprétation et l'application des normes EN 62061 et EN ISO 13849-1. L'initiative vaut d'être mentionnée du fait qu'une version en langue française a été éditée ! Ce document orienté « sécurité fonctionnelle » s'adresse aux constructeurs de machines et intégrateurs.

Au travers des explications, ce guide n'hésite pas à reprendre l'explication des 2 normes, à la base : domaines d'application, résumé de chaque norme, lien avec la directive machine, les procédures de base en 6 étapes…

Un glossaire explique une trentaine de termes et expressions à la fois en anglais et en français (pratique !). Enfin, une rubrique FAQ vient mettre à mal quelques idées reçues… Démonstration :

- **Existe-t-il une spécification du SIL ou du PL (niveau de performance) pour les vannes ou contacteurs magnétiques ?** Non. Car un composant individuel n'a pas de niveau de performance PL ou de niveau d'intégrité de sécurité SIL.
- **Quelle est la différence entre SIL et SILCL ?** Le SIL se rapporte toujours à une fonction de sécurité complète lorsque le SILCL (Limite de revendication de SIL, valeur de SIL maximale) se rapporte au sous-système.
- **Est-il possible d'atteindre une tolérance aux défaillances du matériel de 1 avec une simple surveillance de porte ?** Non. Un défaut unique peut déjà entraîner la perte de la fonction de sécurité.
- **Que signifie l'indice « d » dans « MTBFd » ?** Ici, « d » est l'abréviation du mot anglais « dangerous », donc « dangereux ». LE MTBFd est le temps moyen avant la première défaillance dangereuse.

mise en œuvre et leur modification », précise **Marc Guyon**.

Mais plus complexe pour l'INRS : *« Les automaticiens tendent à demander des fonctionnalités de plus en plus complexes, entraînant de fait une complexification du traitement des sécurités, donc des composants utilisés et de leur mise en œuvre »*, défend **Philippe Charpentier**.

L'étude de la sécurité d'une machine sera-t-elle encore le rôle du constructeur de cette machine, et en a-t-il les moyens ? Demain, qui prendra la responsabilité de la conception « sécurité » et de l'intégration ? Le fournisseur d'équipements ? Le constructeur ? Un bureau d'étude spécialisé ?

« La sécurité d'une machine restera à la charge et de la responsabilité du constructeur, lance **Thierry Vallenet**, Actemium. *Néanmoins, comme c'est déjà le cas aujourd'hui, on peut imaginer qu'il s'appuiera plus encore sur les compétences spécifiques de bureaux d'études tels Norisko, Apave, … »*

Même tendance pour **Volker Rohbeck**, Leuze Electronic : *« C'est le constructeur qui connaît le mieux sa machine, zones dangereuses comprises. C'est donc lui qui, à l'avenir, définira les points et les zones dangereuses ainsi que les mesures de protection nécessaires. C'est lui qui en a la responsabilité. Pour la définition et la documentation des mesures de sécurité nécessaires, il existe des logiciels qui aident efficacement le constructeur dans l'élaboration de sa déclaration CE. »*

La difficulté reste au cœur de la conception pour **Mats Linder**, Jokab Safety : *« L'étude revient à celui qui est compétent. Cette décision ne dépend pas vraiment du type de commande choisi, relais ou automate, car hormis les systèmes très simples à un seul relais de sécurité, il est bien plus facile de concevoir un système de sécurité avec un automate de sécurité, qu'avec des relais de sécurité. L'expérience montre que la principale difficulté ne réside pas dans la réalisation de la fonction de sécurité mais dans la conception de la fonction de sécurité. En effet, le plus difficile est en général d'identifier tous les risques et d'adapter la sécurité à toutes les utilisations : l'opérateur, le technicien de maintenance, le personnel de nettoyage, tous doivent avoir une protection adaptée à leur tâche qui ne met pas en danger les autres. »*

Un jalon technologique de vérification pour l'intégrateur, aux yeux de **Marc Guyon**, BBR Automation : *« Les études d'automatisme sont dans la plupart des cas soumises au client final pour son approbation. Les études électriques sont alors transmises à un organisme de contrôle qui valide la bonne mise en œuvre des recommandations de sécurité. L'intégration des automates de sécurité dans le milieu industriel ne modifiera pas cette méthode de contrôle. Elle permettra en revanche de s'assurer plus facilement du niveau de sécurité atteint grâce à la standardisation de cette intégration. »*

Philippe Carpentier, INRS : *« Le constructeur d'une machine aura toujours un rôle à jouer, en particulier par la nécessité qu'il a de respecter les exigences essentielles de sécurité de la directive machine. En revanche, il n'est pas le seul intervenant impliqué dans la sécurité d'une installation. Lorsqu'il intervient, l'intégrateur a aussi sa part de responsabilité, sachant qu'au final, c'est l'employeur qui prend les mesures nécessaires afin que les équipements de travail mis à la disposition des travailleurs dans l'entreprise et/ou l'établissement soient appropriés au travail à réaliser ou convenablement adaptés à cet effet, permettant d'assurer la sécurité et la santé des travailleurs lors de l'utilisation de ces équipements de travail. »*

Ce futur ce sera quoi ? La sécurité machine du futur laissera-t-elle plus de marges de manœuvre en production (zones de sécurité adaptée, modes dégradés mieux adaptés) ?

Effectivement ce sera le cas pour **Volker Rohbeck**, Leuze Electronic : *« Aujourd'hui déjà il existe des capteurs plus flexibles tels que les scrutateurs laser et les barrières de sécurité intelligentes, qui délivrent plus d'informations qu'une simple commande d'arrêt. Cette tendance va s'accentuer, par exemple avec l'emploi de caméras de sécurité. Quant aux actionneurs, il existe, à côté du classique arrêt de sécurité, plusieurs fonctions nouvelles comme la « vitesse limite de sécurité », le « couple limite de sécurité » ou la « position de sécurité », fonctions qui rendront les équipements plus sûrs et en même temps plus souples d'emploi et plus économiques. »*

« Les avancées actuelles en terme de capteurs (laser, vision, RFID …) pourraient à l'avenir permettre de concevoir des

postes de travail évolutifs. Elles viseront à améliorer la détection de l'homme dans un environnement hostile afin de provoquer les réactions adaptées en terme de sécurité », ajoute **Philippe Charpentier**, INRS.

Le fait de ne plus vouloir confiner un robot, ou une machine, dans une cage, fait-il apparaître un mode de travail plus collaboratif entre la machine et l'opérateur ? Et tout en assurant sa sécurité ?

C'est possible pour **Thierry Vallenet**, Actemium : *« Aujourd'hui même, des radars sont utilisés autour de certaines machines. On peut donc tout à fait imaginer demain que bracelets électroniques ou patchs permettront de détecter l'approche à proximité de la machine. Par comparaison du niveau de dangerosité de la zone et de l'habilitation du collaborateur, la carte vocale de l'automate diffusera le message adapté ou la machine recevra l'ordre de passer en mode dégradé de sécurité, voire de tout stopper. »*

Oui à long terme pour **Volker Rohbeck**, Leuze Electronic : *« Toutefois en condition préalable, les capteurs de sécurité n'arrêteront pas simplement un mouvement dangereux lors de la détection d'un objet, mais détecteront avec fiabilité et sécurité la position de personnes et les parties du corps et transmettront ces informations à un automate de sécurité en temps réel. Pour arriver à cela, il y a encore un long chemin à parcourir, bordé de solutions très onéreuses. C'est pour cela que les capteurs de sécurité classiques garderont encore longtemps leur légitimité. »*

Il faudra toutefois patienter pour **Philippe Charpentier** de l'INRS : *« Des études et expérimentations sont en cours pour ne plus confiner le robot dans une cage, mais cette pratique devrait encore être une réalité pour bon nombre d'année. »*

APRÈS DEMAIN

Vision prospective : comment imagez-vous la sécurité machine en 2020 ?

Une évolution certaine mais pas si rapide selon **Mats Linder**, Jokab Safety : *« A l'avenir opérateurs et machines dangereuses se côtoieront. Mais pour pouvoir travailler à proximité d'un robot, il faut un système fiable afin de limiter le volume de travail du robot, de bons freins de robot et des capteurs de distance entre le robot et la personne qui ne gênent pas le travail. Les possibilités techniques existent et je pense que ce sera économiquement envisageable à l'avenir.*

Il y a 20 ans, on pensait qu'il n'y aurait bientôt plus que des systèmes de sécurité programmables. Pourtant, ils se développent tout juste ! Pendant ces 20 dernières années, ce sont les ventes de relais de sécurité qui ont le plus augmenté. Ces relais constituent la solution la plus utilisée pour la commande des fonctions de sécurité de la plupart des machines. Aussi, il semble plausible qu'il faille attendre 2020 pour que l'homme et la machine travaillent réellement côte à côte ! »

Pour **Volker Rohbeck**, Leuze Electronic, le futur est à Ethernet industriel et aux bus de capteurs et actionneurs : *« J'imagine l'utilisation à grande échelle de transmission de données de sécurité sur réseau Ethernet Industriel (LAN/WAN), complétée par des bus capteurs/actionneurs de type AS-i en environnement industriel. Il sera possible d'accéder facilement à distance aux capteurs et actionneurs de sécurité. Par ailleurs, les capteurs fourniront des informations de sécurité complémentaires telles que des données de mesure ou de qualité. Enfin, seront utilisés des systèmes coopératifs homme / machine. »*

Vision pragmatique : *« Si les 12 années à venir vont au rythme des 12 dernières, la sécurité machine sera totalement intégrée et encore plus interactive avec les opérateurs*, explique **Thierry Vallenet**, Actemium. *Si on va jusqu'au bout du raisonnement sur les bracelets ou patchs précédemment évoqués, on peut tout à fait imaginer que ceux-ci viendront compléter le package des équipements de protection individuelle actuels ! »*

Et **Philippe Charpentier** de conclure cette enquête : *« L'INRS fera ce qui est en son pouvoir pour que le niveau de sécurité des machines ne se dégrade pas du fait des évolutions techniques et que ce niveau soit toujours adapté aux risques encourus. »*

NOS INTERLOCUTEURS :

Volker Rohbeck, Spécialiste sécurité machine et responsable de marché, Leuze Electronic Allemagne.

Mats Linger, PDG de Jokab Safety AB (maison mère en Suède) et de Jokab Safety France.

Thierry Vallenet, directeur Actemium région Auvergne, en charge de l'animation du club Actemium « Biens d'équipements ».

Marc Guyon, responsable études automatisme, BBR Automation.

Philippe Charpentier, département Ingénierie des Équipements de Travail, responsable du laboratoire Sûreté des Systèmes Automatisés de l'INRS.