Quelle Sécurité Machine en 2020 ?

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.
Articulée en deux volets, l'enquête donne la parole à 4 fabricants au travers de cette édition. Le n°58 de Jautomatise clôturera le tour de table avec les interventions d'autres fournisseurs, d'intégrateurs et de l'INRS.
Sans tomber dans la technologie-fiction, en partant du présent, voici de quoi sera fait demain… et après-demain…

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" ?

Olivier Kauffmann, directeur général, Pilz France Electronic rappelle les fondamentaux de la sécurité machine « *la sécurité machine doit être fiable, flexible et adaptée aux différents postes de travail. Fiable, car elle doit tenir compte des modifications de process et des normes. Adaptée aux postes de travail car elle ne doit pas être une contrainte pour l'opérateur et l'inciter à vouloir contourner cette contrainte pour être plus productif. Flexibilité et adaptation semblent de ce fait être des limites à l'intégration des composants de sécurité aux composants d'automatisme* ».

Pour **Haïthem Mansouri,** Regional Business Leader – Safety, Sensors & Connectivity Business, Europe, Middle East & Africa, de Rockwell Automation « *un produit de sécurité se différencie d'un produit d'automatisme standard par l'utilisation de principes de redondance, diversification et diagnostic. Généralement, une combinaison de 2 de ces 3 principes est utilisée pour chaque composant de sécurité. Théoriquement, n'importe quel produit d'automatisme peut être transformé en produit de sécurité si ces principes sont observés. Néanmoins, la réalité impose certaines limites pratiques telles que le coût, l'encombrement physique ou tout simplement l'intérêt du marché. En général, les fournisseurs de produits d'automatisme tels que Rockwell Automation se limitent à intégrer la sécurité dans les parties critiques des produits d'automatisme telles que la sortie physique d'un variateur de vitesse ou le processeur et les entrées/sorties d'un automate programmable* ».

Cette répartition de la sécurité a une limite comme l'indique **Frédéric Jeanparis,** Marketing Automatisation Siemens A&D France « *la limite de la sécurité répartie c'est le taux de charge du réseau et de l'unité centrale, la CPU de l'automate. Les unités centrales sont de plus en plus performantes et peuvent intégrées la sécurité qui relève souvent du traitement combinatoire. Ainsi, elle n'est pas excessivement gourmande en ressources CPU* ».

Même vision pour **Peter Seiler**, chef produits sécurité machines chez Schmersal France et **Friedrich Adams** Membre de l'équipe de direction du groupe Schmersal, expert sécurité des machines et responsable du centre de formation « *En théorie, il n'y a pas de limite d'intégration, si les temps de réponse relatifs à la sécurité ont été correctement déterminés en prenant en compte les conditions d'utilisations les plus défavorables (« Worst Case ») et les cas de défaillance. Sous le temps de réponse, on entend le temps entre la demande d'une fonction de sécurité, par exemple lors de l'ouverture d'un dispositif de sécurité, jusqu'à l'exécution par l'organe de commande et l'arrêt d'un mouvement dangereux. D'un point de vue sécurité, il peut y avoir une différence, si 10 ms ou quelques 100 ms sont nécessaires* ».

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-ce pas un handicap pour la maintenance ?

Sans complexe**, Haïthem Mansouri** de Rockwell Automation répond « *Bien au contraire. L'intégration de la sécurité au sein même du control machine est un facteur important contribuant à la hausse de productivité. Grâce à cette approche, les constructeurs de machines ainsi que les utilisateurs peuvent bénéficier d'une meilleure gestion de la machine. Ainsi, par exemple, l'automate pourra déterminer lui-même si une demande d'ouverture de porte peut être acceptée immédiatement, ou s'il convient de terminer un cycle, afin de minimiser les pertes de production.*

En ce qui concerne la modification des machines, les automates programmables comprennent des tâches séparées pour la sécurité et pour l'automation standard. Il est tout à fait envisageable d'apporter des modifications à la partie du contrôle standard sans devoir toucher à la partie de sécurité si celles-ci n'entraînent pas de nouveaux risques.

Pour des modifications importantes, il convient de refaire une étude des risques conformément à la directive machine. Dans ces cas, nous remarquons qu'une solution de sécurité intégrée réduit fortement le temps de développement ou de modification de la machine puisque les outils de développement et les langages de programmation sont identi-

ques à ceux utilisés pour la partie de contrôle standard. De même, la partie de sécurité aura accès à toutes les variables système facilitant ainsi la programmation.

Le service de maintenance peut également profiter d'une solution de sécurité intégrée pour réduire les temps d'arrêt de la machine. En effet, si une machine se met à l'arrêt soudainement, toutes les informations relatives à la cause de cet arrêt seront directement disponibles. Le redémarrage de la machine sera ainsi fortement accéléré ».

Même remarque de la part de **Frédéric Jeanparis**, de Siemens, pour qui « *au contraire, c'est un avantage indéniable. La sécurité intégrée dans les automatismes programmables standards permet de garantir le niveau de sécurité pendant le cycle de vie complet d'une installation. Il existe des mécanismes dans les logiciels d'ingénierie qui permettent :*
- de contrôler les accès au programme dédié à la sécurité, il existe différents mots de passe et un historique avec un journal d'accès au programme. Pour la maintenance, le programme de sécurité reste bien évidemment lisible en mode hors-ligne comme en mode en-ligne sur l'installation ;
- d'assurer le suivi des modifications nécessaires ou malveillantes grâce aux signatures des blocs et du programme de sécurité, la traçabilité peut se faire depuis l'IHM/superviseur ».

Olivier Kauffmann, de Pilz France Electronic, a une approche bien différente de ce mélange de fonctions « *Nous avons toujours préconisé de séparer les fonctions de sécurité des fonctions de commandes de machines. Que ce soit pour le câblage avec les blocs logiques de sécurité ou par bus de sécurité. L'introduction et la reconnaissance de l'électronique programmée dans les circuits de sécurité à la fin des années 90 ont été une étape primordiale dans la conception des circuits de sécurité. Des armoires remplies de relais de sécurité avec un nombre important de lignes de câblage ont ainsi pu être remplacées économiquement par des automates de sécurité ou des blocs logiques configurables.*

Plus de flexibilité et une capacité de diagnostic plus étendue ont permis de limiter les temps d'arrêt et d'augmenter la productivité.

Il est vrai que ces nouvelles technologies nécessitent des connaissances et des outils plus performants en cas de maintenance, mais il en a été de même lors de la mise en place d'automates standards.

Contrairement aux automates de process, les interventions au niveau des automates de sécurité sur une machine sont très rares et généralement liées à des modifications mécaniques tel que l'ajout de capots protecteurs… De plus les capacités de diagnostic des systèmes électroniques permettent de remédier à plus de 95 % des défauts sans intervention sur l'automate lui-même, via l'afficheur ou l'HMI ».

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 ?

Bien au contraire, estime **Haïthem Mansouri**. Pour lui « *la modification de production demande de plus en plus de systèmes flexibles pouvant s'adapter rapidement et à moindre coût aux exigences de la production. Dans cette optique, les systèmes de sécurité intégrés représentent une solution idéale vu qu'ils offrent la possibilité de modifier la programmation à volonté et d'ajouter ou de retirer des entrées/sorties sans devoir redessiner et re-câbler tout un système de sécurité* ».

Et la rentabilité semble être au rendez-vous pour **Olivier Kauffmann** « *tout ce qui va dans le sens des réductions des interventions au niveau de la maintenance va dans le sens de la rentabilité. Tout ce qui va dans le sens du renforcement de la sécurité, malgré l'utilisation de techniques complexes, va dans le sens de la rentabilité puisqu'il réduit des risques d'accidents aux conséquences financières devenant exponentielles* ».

Mais **Friedrich Adams** et **Peter Seiler** mettent en garde contre une –liberté- trop importante « *Il convient de garder à l'esprit la capacité intellectuelle de maîtriser cette complexité croissante. Si l'on examine les accidents dans la construction mécanique, on peut affirmer qu'il existe certainement un risque objectif. À cet égard, les conséquences de ces changements jouent un rôle critique et il conviendrait de réduire les degrés de liberté actuels* ».

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-elles la place à d'autres technologies comme la fibre optique ou la communication sans fil ? Et dans quel but ?

« *Avec les protocoles de sécurité utilisant les bus de communication standards tels que Ethernet/IP ou DeviceNet, il est aujourd'hui parfaitement possible d'utiliser d'autres technologies de communication telles que des liaisons ponts sans fil… afin d'augmenter la flexibilité des machines. Néanmoins, nous ne verrons pas les liaisons filaires disparaître dans un avenir proche, elles restent encore aujourd'hui moins chères d'utilisation* », pour **Haïthem Mansouri**, de Rockwell Automation.

« *C'est déjà d'actualité avec des liaisons sans-fil sur Ethernet avec des applications concrètes, essentiellement dans les cas de figure de communication entre un élément mobile par rapport à un point fixe. Exemples : ponts roulants, système de navette ou téléphérique, funiculaire… avec comme avantages la réduction des coûts de câblage ou une maintenance réduite* » poursuit **Frédéric Jeanparis** de Siemens A&D France.

De toutes les façons, conclu **Olivier Kauffmann**, de Pilz France Electronic « *Les liaisons sans-fil semblent intéressantes pour leur facilité de mise en service. Elles ne s'imposeront que si leur coût de mise en œuvre est attractif et leur disponibilité (tenue aux CEM) optimisée* ».

Il est suivi dans cette réflexion par **Friedrich Adams** et **Peter Seiler**, de Schmersal « *La sécurité des machines sera à l'avenir sans fil, partout où le sans-fil, vu sous l'angle du «total costs of ownership» a un sens. Tout comme aujourd'hui, on transporte un signal de sécurité et d'automatisme sur les mêmes 2-fils, il est également possible de le réaliser sans fil* ».

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

C'est déjà le cas, insiste **Frédéric Jeanparis** « *C'est de plus en plus d'actualité avec déjà des applications industrielles concrètes* ».

Haïthem Mansouri est sur la même longueur d'onde « *Il est possible aujourd'hui d'utiliser des liaisons sans fil dans le domaine de la sécurité industrielle. Notre protocole de sécurité par exemple, transite sur les mêmes médias que la partie standard d'automatisme qu'elle soit câblée ou non. De plus, nous voyons lentement apparaître sur le marché quelques technologies de capteurs de sécurité sans fil. Bien que cette technologie soit encore à ses balbutiements en ce qui concerne la sécurité machine, elle est tout de même prometteuse d'un avenir où le câble pourrait lentement céder sa place à des liaisons sans fil pour certaines applications* ».

Bien entendu, il reste des contraintes analyse **Olivier Kauffmann** « *Nous avons déjà mis en service des installations avec des gestions de sécurité par ondes hertziennes notamment dans le domaine des téléphériques et des ponts roulants.*

Ce type de technologie ne pourra pas être installé partout, pour des raisons liées aux contraintes d'environnement ».

Même prudence pour **Friedrich Adams** et **Peter Seiler** « *La technologie haute fréquence est très sensible (aux perturbations) et pour des raisons de sécurité, ne dispose pas des mêmes possibilités que la technologie traditionnelle. De plus, chaque système, et ce conformément aux exigences de la sécurité des machines, se doit de disposer des mesures supplémentaires, garantissant notamment la disponibilité en cas de conditions critiques dans l'environnement de fabrication* ».

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 ? Explication…

Les mentalités doivent bouger pour **Friedrich Adams** et **Peter Seiler** « *L'utilisation de logiciels - au lieu de la logique câblée - exige certainement un changement de mentalité. Ceci concerne d'ores et déjà les nouvelles normes EN ISO 13849-1:2006 et EN 62061:2005 IEC sur la « sécurité des systèmes de contrôle relatives à la sécurité » où - comme pour l'utilisation des progiciels - le respect de certaines règles est nécessaire. La discussion sur les autres exigences relatives aux logiciels embarqués n'est certainement pas terminée. En revanche, il y aura beaucoup d'avantages qui rendront les machines du futur plus sûres, par exemple moins de manipulations par des fonctions machines plus intelligentes, une sécurité des machines plus discrète. Mais dans tous les cas, le thème de «la conception et de l'utilisation de logiciels» doit attirer plus l'attention, que ce soit par la formation, soit par la prise à la main des utilisateurs…* »

Car l'évolution est là, estime **Olivier Kauffmann** « *L'évolution des normes et des produits incite les fabricants (et les organismes de contrôle) à faire appel de plus en plus à des spécialistes et à utiliser des produits homologués et des blocs fonctions encapsulés* ».

Et les blocs de sécurité ne sont pas prêts de disparaître comme le précise **Frédéric Jeanparis** « *depuis de nombreuses années, il existe des bibliothèques de blocs de sécurité certifiés auprès des organismes compétents. Il y a des blocs de sécurité élémentaires (gestion d'AU, barrières immatérielles, …) et des blocs de sécurité métier (presse, brûleur)* ».

Ces blocs de sécurité auraient même un avantage pour **Haïthem Mansouri** « *Le fait de pouvoir utiliser des blocs de fonction validés par le constructeur ainsi qu'un organisme de certification, facilite la programmation et la validation du programme de sécurité. Cette dernière peut se limiter dans ce cas à des tests d'intégration au niveau système selon le modèle V décrit dans la norme CEI 61508 puisque les « modules » (blocs de fonction) auront déjà été testés et validés par le constructeur.*

Côté programmation, il existe de plus en plus de blocs de fonction de sécurité orientés application. Le but étant d'encapsuler un maximum de fonctionnalités dans un bloc pour une application spécifique ».

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

Pour **Frédéric Jeanparis** « *C'est une évolution, l'automaticien doit prendre en charge la sécurité fonctionnelle. Avec comme avantages de simplifier son programme standard, et de mieux gérer les modes de fonctionnement de la machine en ayant 2 programmes dans la même CPU avec des échanges faciles entre les deux* ».

Assisté en cela par les offreurs, comme l'indique **Olivier Kauffmann** « *Les notions de service et de conseil des fabricants de composants de sécurité vont se généraliser pour proposer aux clients des solutions clés en main : matériel, programmation et validation CE de la machine* ».

« *Les normes de sécurité fonctionnelles tels que les normes CEI 62061 et EN ISO 13849-1 guident les utilisateurs vers une pratique méthodique et bien documentée de la sécurité machine. Nous offrons des formations, des conseils, des services, ainsi que des outils pour faciliter la mise en place et la gestion des systèmes de sécurité* » conclut **Haïthem Mansouri.**

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 ?

Evolution du métier confirmé par **Friedrich Adams** et **Peter Seiler**, de Schmersal, « *Le thème de la sécurité des machines devient plus complexe, car sa mise en œuvre requiert plus d'intelligence et de flexibilité. Que la machine soit en mode automatique, n'est plus une fin en soi. Il s'agit beaucoup plus de la conception des fonctions machines ergonomiques, par exemple dans les modes de réglage et d'observation des processus ou lors de la recherche de pannes...* ».

Position unique du constructeur pour **Haïthem Mansouri,** de Rockwell Automation, « *Le constructeur de machines est aujourd'hui dans une position unique qui lui permet d'incorporer une stratégie de sécurité aussi simple ou aussi complexe qu'il le désire dans ses machines. Ce choix existera toujours. Il n'est pas question d'abandonner les simples relais de sécurité au profit de systèmes plus complexes. Nous évoluons plutôt vers une ère de « sécurité fonctionnelle »*

où le rôle de la sécurité sera totalement remis en question.

Les questions à venir au niveau corporatif seront : comment utiliser la sécurité comme un réel avantage compétitif ? Comment réduire, voire éliminer les temps d'arrêt d'une machine ? Peut-on interdire l'accès à certaines zones de la machine au personnel non qualifié ?… ».

Mais l'utilisateur sort gagnant, précise **Olivier Kauffmann**, de Pilz France Electronic, « *La sécurité sera plus simple au niveau matériel (un seul bloc logique configurable au lieu de 15 relais par exemple). La programmation sera un peu plus complexe car elle gérera des fonctions de sécurité qui n'étaient pas possibles en logique câblée (contrôle de vitesse, signaux analogiques, …), mais au final l'utilisateur sera gagnant grâce à une plus grande fiabilité (moins de composant) et une meilleure flexibilité* ».

« *Plus simple et avec plus de sécurité pour l'exploitant grâce au diagnostic immédiatement disponible. Il en résulte aussi plus de maîtrise quant au niveau de sécurité, aux modes de marche…* » conclut **Frédéric Jeanparis**, de Siemens A&D France.

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 ?

Pour une fois, nos interlocuteurs ne sont pas forcément d'accord entre eux. Pour **Olivier Kauffmann**, elle revient au fabricant de la machine **«** *Comme aujourd'hui, les différents intervenants (constructeur de machine, intégrateur, fabricant d'équipement, B.E.) se partagent en quelque sorte les responsabilités, la responsabilité finale revenant à l'utilisateur, ayant lui-même une responsabilité vis-à-vis de ses opérateurs. La complexité des technologies ne devraient pas fondamentalement remettre en cause la chaîne de décisions et donc de responsabilités* ».

Pour Friedrich Adams **et Peter Seiler**, « *Le conseil gagnera certainement encore en importance, mais la responsabilité finale incombe au fabricant de la machine. Finalement, seul lui connaît sa machine, et donc ce qui est nécessaire concernant la sécurité* ».

Ils sont deux à assumer cette responsabilité pour **Frédéric Jeanparis** « *C'est le constructeur de la machine ou l'installateur à qui incombe la responsabilité. Celui-ci peut assurer ce rôle avec ses propres ressources ou s'appuyer sur des experts reconnus chez le fournisseur de produits d'automatismes ou des organismes/ bureau spécialisés* ».

En conclusion, **Haïthem Mansouri**, penche pour une collaboration « *En évoluant de plus en plus vers la sécurité fonctionnelle, la conception de la sécurité machine sera faite en partenariat entre le constructeur de machines, l'utilisateur final et le fournisseur de produits de sécurité. Il ne sera plus seulement question de protéger les opérateurs, mais aussi de plus en plus la machine et la production. Une bonne coopération entre le constructeur de machine et l'utilisateur final lors de la conception de la machine est le meilleur moyen de garantir ces performances.*

Il sera également très important de bien choisir les produits et concepts de sécurité utilisés dans une machine afin de garantir les meilleures performances. Ici encore une bonne collaboration entre le constructeur de machine et le fournisseur de produits de sécurité est essentielle ».

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) ?

Tous nos interlocuteurs sont d'accords, à l'image de **Friedrich Adams** et **Peter Seiler** **«** *C'est exactement la tendance que nous observons et jugeons nécessaire. Sinon, le thème de la « fraude des dispositifs de sécurité » ne serait pas maîtrisé. Nous savons aujourd'hui, grâce à diverses enquêtes que les opérateurs qui manipulent les machines, ne le font pas par hasard. La plupart du temps, la manipulation vise à rendre le travail plus efficace et plus simple. La sécurité des machines d'aujourd'hui devrait tenir compte de ces exigences* ».

De nouveaux horizons s'ouvrent, comme l'indique **Olivier Kauffmann** **«** *L'interactivité homme-machine et homme-robot sera le chantier des années à venir. La vision en 3D pour la sécurité des opérateurs va permettre une relation directe entre l'homme et le robot sans contrainte mécanique* ».

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 ?

D'accord pour la collaboration, **Friedrich Adams** et **Peter Seiler** précisent « *Le temps d'une collaboration directe entre l'être humain et le robot va venir. Pour l'essentiel, il s'agit d'une question de capteurs plus intelligents, par exemple, des caméras plus sûres qui n'existent pas encore. En ce qui concerne les systèmes de contrôle-commande, les possibilités sont d'ores et déjà disponibles. Un exemple : le module de sécurité paramétrable qui permet de surveiller de manière sûre les coordonnées axiales et cartésiennes. Néanmoins, c'est là l'essentiel, mais aussi les nouveaux défis de la robotique. Le risque lié aux particules éjectées va aussi à l'avenir maintenir la distance entre l'homme et le robot* ».

Confirmation de **Haïthem Mansouri** **«** *Une chose est claire, nous ne sommes pas encore prêts à disposer des « cages ». Dans le cas de machines où il y a projection d'objets, par exemple, une protection physique est encore et toujours nécessaire. Néanmoins, les produits de sécurité se font de plus en plus discrets, en effet. De nos jours il est tout à fait concevable d'accéder à certaines zones dangereuses d'une machine sans que celle-ci soit forcément à l'arrêt. Nous passons d'une sécurité à deux états (marche, arrêt), à un monde de sécurité fonctionnelle où le but primordial est d'assurer le fonctionnement optimal de la machine tout en garantissant la sécurité des opérateurs* ».

Et même le sans-fil se fait sa place, **Frédéric Jeanparis, «***Oui, et la sécurité intégré va dans ce sens, c'est déjà le cas avec des IHM mobile dialoguant en liaison sans fil WifFi sur Ethernet / Profinet / Profisafe pour des opérations de réglages dans une enceinte robotisée* ».

« *L'utilisation du support Ethernet pour la gestion de la sécurité va également se généraliser.*

Les nouvelles normes de sécurité qui vont entrer en vigueur

en 2009 imposent des calculs de probabilité de défaillances du circuit de sécurité. Les composants les plus fiables seront privilégiés » conclut **Olivier Kauffmann**.

APRÈS DEMAIN

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

Le futur se décline en déploiement total pour **Frédéric Jeanparis**, de Siemens A&D France « *L'approche "intelligence répartie comprenant la sécurité" sera totalement déployé, les systèmes de détection pour placer le personnel ou la machine dans un état sûre seront de plus en plus à base de caméra, de systèmes RFID et de localisation. Les outils logiciels d'ingénierie seront entièrement intégrés dès la phase d'analyse d'un projet de sécurité, il y aura donc traduction immédiate des boucles fonctionnelles de sécurité en paramètres/codes pour le système d'automatisation* ».

Pour **Haïthem Mansouri**, de Rockwell Automation**, «** *Dans le futur, nous pouvons imaginer une sécurité industrielle sans composant de sécurité à proprement dit. En effet, le choix des composants utilisés, en d'autres termes, leur niveau de fiabilité ainsi que la façon dont ils sont utilisés, détermineront le niveau de sécurité obtenu. Vu que les principes de sécurité (redondance, diversification et diagnostic) sont de plus en plus incorporés dans les produits d'automatisme classiques, nous parlerons peut-être dans le futur de produits à haute fiabilité pour désigner les produits que l'on nomme aujourd'hui de sécurité. De même, il pourrait être envisageable d'utiliser des produits standards, à moindre fiabilité, pour des applications où le niveau de sécurité est assez bas, ou même une combinaison des deux.*

Ainsi, il sera possible d'utiliser les produits dédiés à la gestion de la machine pour justement gérer la machine ainsi que sa sécurité sans « l'interférence » d'agents « externes » visant à mettre la machine à l'arrêt pour la moindre intrusion dans la zone dangereuse. Peut-être suffira-t-il tout simplement d'ajuster la vitesse de la machine en fonction de la distance et la vitesse d'approche de l'opérateur ? Ou peut-être dévier automatiquement la production vers une autre zone de la machine ? ».

De leur côté, **Friedrich Adams** et **Peter Seiler**, de Schmersal, pensent que l'on « *peut imaginer que des systèmes mono-canaux répondant aux exigences les plus élevées suffiront un jour. Le fait est que les dispositifs électroniques relatifs à la sécurité prennent de plus en plus de place en matière de contrôle-commande et ce, qu'il s'agisse de technologies bus, sans fil ou caméras. On peut penser qu'à l'avenir tout dispositif de commande sera muni ou pourra disposer de fonctions de sécurité, et ce qu'elle qu'en soit l'usage : en sécurité machine ou pas. Des systèmes de commandes spécifiques à certaines branches seront adaptés à une problématique spécifique. Des systèmes de commandes (dispositifs de sécurité) seront constitués de modules combinés entre eux et configurés sur place par le constructeur machine suivant la problématique requise. La sécurité des machines va être adaptée dans le monde entier en suivant le modèle de l'UE. On va pouvoir constater une scission entre les pays hautement industrialisés et les pays moins développés dans le futur. Comme par le passé, ces derniers auront besoin de systèmes de commande simples (hardware)* ».

Enfin, 2020, semble déjà du passé pour **Olivier Kauffmann**, de Pilz France Electronic « *2020 c'est déjà demain. Il est bien évident que les recherches menées hier concernent demain et celles menées aujourd'hui concernent après-demain ! Nos recherches actuelles visent à penser la sécurité dans un contexte plus général, l'utilisateur attendant une solution globale à ses problèmes. La sécurité sera alors associée à d'autres fonctions, ou d'autres fonctions auront aussi un rôle de sécurité.*

L'apport de technologies différentes de celles utilisées aujourd'hui, comme l'analyse d'images 3D, auront imposé une approche différente de la sécurité, mais l'objectif final reste identique, c'est-à-dire sécuriser les installations et protéger les opérateurs ».

NOS INTERLOCUTEURS :

Frédéric Jeanparis,
Marketing Automatisation
Siemens A&D France

Haïthem Mansouri,
Regional Business Leader – Safety, Sensors & Connectivity Business, Europe, Middle East & Africa, Rockwell Automation

Friedrich Adams
Membre de l'équipe de direction du groupe Schmersal en Allemagne, expert sécurité des machines et responsable du centre de formation Schmersal

Peter Seiler,
Chef produits sécurité machines chez Schmersal France

Olivier Kauffmann,
Directeur général Pilz France Electronic