SÉCURITÉ

"La sécurité, d'accord. Mais où

Le Safety Users Group vient d'éditer un très intéressant coffret de deux DVD rassemblant les interviews d'une dizaine de personnalités spécialisées dans la sécurité, et plus particulièrement les systèmes instrumentés de sécurité. Nous avons extrait de ce volumineux travail quelques propos parmi d'autres, que nous avons associés par thèmes et que nous avons pris la liberté de présenter sous la forme d'un débat. On peut en tirer de nombreux enseignements…

Mesures. Depuis quelques années, la sécurité est devenue un enjeu majeur. Qu'est-ce qui a motivé cette évolution ?

Stefan Grassi (Inprotec). Si on remonte 20 ans en arrière, il est évident que l'industrie ne s'intéressait pas autant qu'aujourd'hui aux normes et aux bonnes pratiques en matière de sécurité, et elle ne cherchait pas à implémenter les dernières technologies, bien au contraire. Il y avait relativement peu de systèmes de sécurité pour protéger le fonctionnement des installations électroniques et ceux qui étaient en place étaient dans leur immense majorité à base de relais. Par ailleurs, la réglementation et les normes étaient beaucoup moins contraignantes, et souvent elles n'existaient même pas. La première directive Seveso, qui a bouleversé la donne, n'est apparue qu'en 1982 (une seconde directive Seveso a été publiée en 1996). Ces dix dernières années, le marché des systèmes de sécurité a fortement augmenté. J'y vois trois raisons. La première, c'est que dès le stade du projet, on pense à la protection des équipements et à la sécurité. Les industriels ont bien compris tout le bénéfice qu'ils pouvaient tirer à éviter les accidents. La deuxième raison, c'est que les utilisateurs sur site sont désormais familiarisés avec les solutions basées sur des systèmes instrumentés de sécurité et ils ont confiance en eux. La troisième raison, enfin, tient au fait que la technologie est devenue beaucoup plus accessible et qu'elle répond beaucoup mieux aux contraintes techniques des process et de leurs modes de fonctionnement.

Mesures. D'un pays à l'autre, la notion de risque n'est pas abordée de la même façon. Pouvez-vous nous donner quelques indications là-dessus ?

Bertrand Ricque (Isa/Club Automation). Avant de "pointer" les différences, il faut quand même rappeler qu'il y a des constances. Où que l'on se trouve, le point de départ d'une culture de sécurité, c'est d'accepter qu'un risque est toujours présent et qu'il est possible de fixer des limites "acceptable" et "non acceptable" de tout risque.

Franck Mairet (Bureau Veritas). Il y a de nombreuses différences d'un pays à l'autre. En France, les autorités parlent d'obligation de moyens alors qu'outre-Manche, on parle d'obligations de résultats. Dans le domaine des machines, la réglementation française définit précisément la périodicité des inspections. En Allemagne, les industriels fixent eux-mêmes cette périodicité, après avoir réalisé leur analyse du risque.

Autre différence, la notion de "risque résiduel". En France, on n'en parle pas et on ne reconnaît pas qu'il existe toujours un risque résiduel. Au Royaume-Uni, c'est totalement différent. Les autorités de la santé et de la sécurité en parlent et elles poussent les industriels à avoir une approche ALARP (As Low As Reasonably Practicable) du risque. Elles sont donc bien conscientes de cette notion de risque résiduel et elles savent qu'il n'est pas économiquement pertinent de chercher à le réduire car le coût serait plus élevé que le coût des dégâts que pourrait occasionner ce risque. Ces autorités parlent de "risque tolérable".

Cette notion de risque tolérable est à géométrie variable. Dans le domaine des machines, aux Etats-Unis, on se contente d'un panneau ou d'une étiquette avertissant de la présence d'un danger potentiel alors qu'en Europe, on mettra une barrière de protection. Cela dépend aussi du secteur d'activités. En France, on ne tolère pas un accident d'avion qui ferait 200 victimes alors que l'on s'accommode des 5 000 morts sur les routes.

Tino Vande Capelle (HIMA). Les différences se situent surtout dans la taille et l'activité des entreprises. Les grandes multinationales ont du personnel et des services spécialisés dans la sécurité. Ce n'est pas le cas des petites entreprises, qui ont souvent des contraintes de budget.

Bertrand Ricque (Isa/Club Automation). Il est clair que les choses varient beaucoup selon que l'on se trouve dans un pays émer-

commencer ? Où s'arrêter ?"

gent ou un pays industriel développé. Certaines sociétés font preuve d'un certain cynisme dans leur manière d'appliquer les normes de sécurité. C'est le cas par exemple lorsqu'elles appliquent le concept ALARP. Je n'ai pas de problème avec ce concept, je trouve qu'il est très utile pour évaluer l'impact financier de la sécurité. Mais j'ai du mal à accepter que lorsqu'il est appliqué dans un pays émergent, le niveau de risque acceptable soit plus élevé que lorsqu'il est appliqué dans un pays développé.

Mesures. Et pour la France ?
Bertrand Ricque (Isa/Club Automation). La France est dans une large mesure restée avec une approche déterministe du risque. C'est pour cela que, à l'exception des grosses sociétés multinationales, les normes IEC 61508/61511 (qui sont d'essence probabiliste) restent méconnues.
Autre caractéristique de la France, on s'appuie moins qu'ailleurs sur la responsabilité individuelle, on se défausse sur l'Etat et on compte sur lui pour faire le nécessaire en matière de sécurité. Du coup, le bon peuple est rassuré et lorsqu'il passe à côté d'une raffinerie, il estime que la zone dangereuse est confinée à l'intérieur et qu'il n'y a aucun danger à l'extérieur !
Du coup, une société française ayant peu d'expérience à l'international peut avoir du mal à acquérir la mentalité anglo-saxonne en matière de risque. L'inverse est vrai aussi. Lorsqu'un industriel étranger veut investir en France, il peut avoir du mal à trouver des partenaires sur place.
J'ajouterai qu'en France, pour déployer des systèmes instrumentés de sécurité, il y a deux sortes de sociétés. Il y a les intégrateurs, qui n'ont pas forcément une grande compétence dans les études de risques, et qui auront tendance à se reposer sur les solutions proposées par les constructeurs. Il y a ensuite des sociétés d'ingénierie qui ont une forte compétence dans le domaine de la sécurité, mais qui préfèrent travailler sur les marchés militaire ou du transport car les contraintes de temps et prix y sont moins fortes. Si elles veulent entrer sur le marché de la sécurité du process, il leur faut revoir leurs tarifs.

Mesures. La notion de couverture de risques s'est surtout développée sous la pression des réglementations, souvent durcies lorsque survient un nouvel accident grave…
Franck Mairet (Bureau Veritas). C'est vrai mais peut-être que l'on n'en serait pas là si les dispositions légales étaient considérées comme étant un minimum et non un maximum.

Mesures. Est-ce que la sécurité a "bonne presse" dans les entreprises ?
Bertrand Ricque (Isa/Club Automation). La sécurité est souvent vécue comme étant quelque chose qui coûte cher et impose des contraintes.
Michel J.M. Houtermans (Risknowlogy). D'une façon générale, je trouve que les gens se compliquent inutilement la vie. Ils ne pensent pas à la finalité de la sécurité et font des choses qui leur coûtent cher et la sécurité véhicule ensuite une mauvaise image.
Les industriels doivent comprendre que la sécurité leur permet d'économiser de l'ar-

gent. S'ils ont l'impression qu'elle leur en coûte, c'est qu'ils ne font pas les choses correctement. Quand on veut déployer une application de sécurité, il faut d'emblée se dire qu'elle sera rentable, et non la considérer comme un poids.

Fabrizio Gambetti (Snamprogetti). La procédure de management du risque est souvent considérée comme étant une perte de temps et se voit reprocher de ne pas apporter de valeur ajoutée à un projet. Je suis absolument convaincu que si les méthodologies disponibles sont utilisées correctement et au bon moment, elles peuvent apporter une quantité significative d'informations utiles dans le processus de conception de l'équipement à contrôler, et permettre de gagner du temps et de faire des économies…

Mesures. Venons-en aux normes IEC 61508 et IEC 61511 ? Pouvez-vous rappeler en quelques mots la différence entre les normes ?

Vous pouvez les commander…

Si vous vous intéressez à la sécurité des process industriels, vous ne pouvez pas ne pas connaître le site Internet www.safetyusersgroup.com. Ce site d'une grande sobriété rassemble une très abondante documentation sur la sécurité et fournit quantité d'informations pratiques.

La dernière initiative des animateurs de ce site nous apparaît plus particulièrement intéressante. Il s'agit de l'édition d'un double DVD rassemblant les entretiens menés avec 11 spécialistes européens de la sécurité (constructeurs, intégrateurs, utilisateurs, sociétés de conseil). Ces entretiens sont en anglais et ils montrent les nuances qui peuvent exister en matière de sécurité entre les différents pays. Ceux qui ont des difficultés avec l'oral de la langue de Churchill trouveront dans ce double DVD le script de tous les entretiens, sous la forme de fichiers .pdf.

Dans notre article, nous avons rapporté quelques propos de la plupart des intervenants. Trois manquent à l'appel, et pas les moins intéressants ! Thomas Steiner d'Emerson Process Management et Josef Boercsoek d'Hima présentent les aspects théoriques des systèmes instrumentés de sécurité. Il s'agit de vraies fausses interviews, avec des formules, des courbes, des diagrammes. La troisième, de Christian Huglo du cabinet Huglo Lepage & Associés, aborde notamment les aspects juridiques de la sécurité. Et ce n'est pas simple, plus particulièrement en France.

Ce double DVD est proposé 115 $ (ou 90 €). Vous pouvez dès à présent le commander sur le site www.safetyusersgroup.com, rubrique Media/vidéothèque

Ron Bell (RBC). La relation entre ces deux normes est très simple. L'IEC 61508 est la publication de base, la publication de référence sur laquelle s'appuient tous les comités techniques chargés d'élaborer des normes dans le domaine de la sécurité fonctionnelle.
A partir de cette base, des normes plus sectorielles, plus pratiques à mettre en œuvre, ont été élaborées. C'est le cas de l'IEC 61511, qui porte sur les systèmes instrumentés de sécurité utilisés dans le domaine des process de fabrication. Cette norme aborde les logiciels, et plus particulièrement les langages de programmation utilisés dans le domaine du process. De plus des dispositions ont été prévues pour prendre en compte l'expérience du terrain, pour par exemple quantifier le niveau de fiabilité de certains équipements de process…

Mesures. Est-ce que l'avènement de ces normes vous a amenés à modifier vos façons de travailler?
Stefan Grassi (Inprotec). Oui, incontestablement. Nous avons mis en place de nouvelles procédures. Exemple parmi d'autres, chez nous, la personne qui teste la partie logique d'un système de sécurité est obligatoirement différente de celle qui l'a conçu. Ces normes constituent un moyen efficace et économique de minimiser les erreurs, notamment les fautes cachées et dormantes, qui étaient jusque-là les plus malicieuses à identifier.
Cela dit, on n'a pas encore beaucoup d'expérience dans l'utilisation de ces normes.

Mesures. Est-ce que leur mise en œuvre est simple?
Ron Bell (RBC). L'IEC 61508, et dans une moindre mesure l'IEC 61511, sont des normes complexes et pour les mettre en œuvre il faut donc un certain niveau de compétences, tant au niveau de l'organisation que des hommes.
Stefan Grassi (Inprotec). Je confirme. L'IEC 61508 est répartie sur 7 volumineux classeurs, ce qui représente un véritable parcours du combattant où on a des chances de se perdre.
Fabrizio Gambetti (Snamprogetti). Les choses sont un peu plus simples avec l'IEC61511, et c'est un peu normal puisqu'elle a été élaborée pour faciliter les choses. Pour autant, en pratique, elle n'est pas toujours facile à appliquer. La principale difficulté concerne les éléments simples tels que les vannes et les capteurs, par exemple, qui ne bénéficient pas des mêmes études fiabilistes que les contrôleurs.
Un autre handicap, c'est que les coûts initiaux (organisation, management, informations sur les éléments simples, documentation) sont relativement élevés. Mais ceux-ci se rattrapent par la suite car la conception et la gestion du système de sécurité, tout au long de son cycle de vie (et notamment lors de son exploita-

tion) sont largement facilitées.
De façon générale, la mise en œuvre de cette norme se fait souvent dans des conditions difficiles car il y a souvent un manque de coordination et d'harmonisation entre les différentes équipes concernées par le système, sans parler de la rétention d'information.

Mesures. Malgré tout, sur le principe, ces normes ont au moins le mérite de faire l'unanimité…

Stefan Grassi (Inprotec). Sur le principe, oui. Mais tout le monde ne les lit pas de la même façon. Les professionnels ne sont pas unanimes dans la façon de les mettre en œuvre, ce qui peut créer des conflits et des questions importantes n'ont toujours pas de réponse.
Cette norme entre dans une phase de révision et nous espérons qu'il sortira une version plus pratique. Nous sommes dans l'attente de normes plus synthétiques, accompagnées de guides simples.

Tino Vande Capelle (HIMA). Les normes IEC 61508 et 61511 sont désormais reconnues. Je pense cependant que de nombreuses personnes ont une fausse idée de ce qu'elles sont réellement. Il existe un réel besoin de formation en sécurité. De nombreuses personnes pensent qu'ils maîtrisent la sécurité, mais la réalité démontre que c'est tout le contraire.

Franck Mairet (Bureau Veritas). J'ajouterai que les normes IEC 61508/61511 étaient obsolètes dès leur publication. Ceci s'explique par la longueur de la procédure qui a conduit à l'arrivée de ces normes (plus de 5 ans…).
Par exemple, aucune restriction n'est imposée quand l'utilisation des langages de programmation tels que le C et C++. Dans le même ordre d'idée, on ne fait pas de distinguo entre le système d'exploitation et le logiciel applicatif.
Mais il faut quand même voir que malgré leurs insuffisances, ces normes sont d'un apport capital pour le déploiement des systèmes de sécurité. Elles fournissent un cadre général et des méthodes, elles prennent en compte tous les aspects d'un système de sécurité, l'aspect matériel, l'aspect logiciel et l'aspect système.

Mesures. Pour mettre en place un système de sécurité de process, il faut commencer par faire une analyse des risques. Pouvez-vous évoquer quelques-unes des méthodes utilisées?

Ron Bell (RBC). Avant d'évoquer ces méthodes, il faut rappeler que le risque est la combinaison de la probabilité d'un événement redouté et la gravité de cet événement. J'ai utilisé le mot "combinaison", mais celui-ci ne doit pas être compris au sens mathématique du terme.
Lorsque l'on se trouve dans des situations ou des événements dangereux peuvent avoir des conséquences significatives, on est amené à quantifier le risque. Mais dans la majorité des cas, les conséquences ne sont pas très sé-

rieuses et on utilise une approche qualitative…

Pasquale Fanelli (Invensys Process Systems). Les normes ne recommandent pas de méthodes particulières pour réaliser une analyse des risques. A partir de là, on est libre d'utiliser ce que l'on veut, aussi bien des méthodes qualitatives que des méthodes quantitatives ou semi-quantitatives.

Les méthodes qualitatives les plus utilisées sont le graphe de risques ou la matrice de risques, calibrés en termes de gravité des conséquences sur la santé, l'environnement et, si nécessaire, les équipements. Les méthodes qualitatives permettent d'aller vite en besogne mais, comme elles sont basées sur l'expérience et l'ingéniosité des personnes, elles sont très subjectives.

La méthode semi-quantitative la plus connue est la méthode LOPA (Layer Of Protection Analysis) et elle consiste à prévoir des multiples barrières de réduction du risque pour ramener le risque à un niveau acceptable. Dans les situations à risques critiques, on fera plutôt appel à des méthodes quantitatives, telles que l'analyse de l'arbre des fautes (Fault Tree Analysis).

Je citerai enfin la méthode ALARP (As Low As Reasonably Practicable) qui repose sur une classification des risques : "non acceptable", "tolérable" et "acceptable".

Mesures. Forts de votre expérience, pouvez-vous donner quelques conseils à ceux qui doivent mettre en place des systèmes intégrés de sécurité ?

Tino Vande Capelle (HIMA). La sécurité est et reste une affaire très sérieuse. Pour déployer une application de sécurité, l'industriel doit faire appel à des spécialistes, tant pour le conseil que pour la formation. Il doit confier la gestion de la sécurité fonctionnelle à une équipe. Celle-ci devra manager le cycle de vie complet du système de sécurité (conception, exploitation, maintenance), vérifier et valider les données de façon à garantir que le risque a été réduit à un niveau acceptable et qu'il reste à ce niveau.

On ne peut rien faire sans avoir un personnel compétent. Et surtout, il faut avoir un soutien actif de la direction de l'entreprise.

Franck Mairet (Bureau Veritas). De façon générale, le meilleur moyen d'améliorer le niveau de sécurité sur un site est de réaliser une analyse des risques dès les premières phases du projet. C'est devenu une pratique courante dans les industries du pétrole et gaz.

Stefan Grassi (Inprotec). Je pense qu'il est essentiel de considérer qu'un SIS (système instrumenté de sécurité) ne peut pas maintenir le niveau de sécurité pour lequel il a été conçu, s'il ne bénéficie pas d'une maintenance régulière. Pour cela, l'industriel doit faire appel à une équipe compétente et expérimentée pour pratiquer les tests de validations périodiques mais aussi pour maintenir à niveau les personnels chargés de l'exploitation de l'atelier ou de l'unité de production.

En tant qu'intégrateur de systèmes instrumentés de sécurité, nous ressentons une attente des industriels en termes de compétences, conseil, de faculté à s'adapter à leur besoin, de rapidité d'intervention… et de prix compétitifs. Nous pensons que cette tendance va se poursuivre. Nous pensons aussi que les industriels vont être de plus en plus demandeurs de fonctions de sécurité "prêtes à l'emploi", intégrées dans des produits et systèmes de sécurité.

Traduction et libre adaptation de Jean-François Peyrucat