MISE EN ŒUVRE DE L'IEC 61508

Dans la sécurité, ce qui compte avant tout, c'est la démarche…

Bureau Veritas est impliqué de longue date dans les applications de sécurité et a été un des premiers à soutenir la norme IEC 61508. La société insiste ici sur l'importance de la démarche et invite chacun à ne pas se laisser obnubiler par les SIL qui sont distribués parfois un peu trop à la légère. Elle déplore aussi que les Français soient aussi timorés dans l'application des nouvelles normes…

Mesures. Pouvez-vous résumer très brièvement l'activité du *Bureau Veritas*.

Michel Suzan. Pas simple, pour un groupe qui emploie aujourd'hui plus de 20000 personnes, est présent dans 140 pays et a plus de 200000 clients. Pour résumer, disons que le groupe assure des activités de certification de systèmes de management (qualité sécurité, santé, environnement), d'attestation de conformité, de formation et enfin de conseil et assistance technique.

Michel Suzan, Responsable "Equipements et Procédés industriels" à Bureau Veritas.

Ces différentes activités sont relativement cloisonnées. C'est ainsi qu'il y a une totale indépendance entre les prestations de vérification de conformité réglementaire d'une part, et de conseil et assistance technique d'autre part. Ces deux prestations sont assurées par des équipes différentes. Il est exclu que l'équipe spécialisée dans le conseil prolonge sa prestation par de la vérification de conformité.

Mesures. Cela semble pourtant s'inscrire dans une certaine logique. Vous montreriez à vos clients que les conseils que vous leur donnez ne sont pas "gratuits", et qu'en les mettant en pratique pour aboutir à une vérification de conformité, vous prendriez vos responsabilités…

Michel Suzan. Peut-être mais la question ne se pose pas : les autorités administratives, et notamment le *Cofrac*, qui nous ont mandatés pour délivrer des attestations de conformité imposent de ne pas mélanger les genres. C'est aussi une règle d'éthique et de bon sens. Notre indépendance, une de nos valeurs fondamentales, en dépend.

J'ajouterai que nos différentes prestations ne sont pas seulement assurées par des équipes différentes, elles peuvent être assurées par des sociétés différentes à l'intérieur du groupe. Par exemple, la certification des systèmes de management est assurée par BVQI, et non par *Bureau Veritas*. Par contre, c'est *Bureau Veritas* qui délivrera l'attestation de conformité d'une boucle de sécurité,

J'ajouterai que dans le groupe, nous avons aussi une activité de certification des produits électriques et électroniques : celle-ci est assurée par le LCIE. Ainsi, l'attestation de conformité et la certification de la sécurité fonctionnelle de produits sont désormais confiées au LCIE.

Mesures. Venons-en aux activités dans le domaine de la sécurité. Vous êtes depuis la première heure un ardent défenseur de l'IEC 61508 et de ses dérivées. On voit de plus en plus de conférences sur le sujet. Cette reconnaissance est plutôt bon signe, non?

Michel Suzan. C'est vrai que beaucoup nous ont emboîté le pas, ce qui montre bien que cette norme, malgré les critiques dont elle a été l'objet à un moment (on lui prêtait une certaine complexité), est en train de faire l'unanimité auprès des professionnels. Certains s'y sont ralliés un peu à la manière des "ouvriers de la 25ème heure". A *Bureau Veritas*, nous nous y sommes intéressés dès sa genèse. Soutenue au départ par *Bureau Veritas Consulting*, son utilisation a été étendue aujourd'hui à l'ensemble du groupe. Elle constitue pour nous un véritable référentiel pour traiter les problèmes de sécurité.

Et puis il y a eu des avancées importantes faites autour de l'IEC 61508, notamment au niveau de sa mise en pratique. Pour rendre les choses plus simples, l'IEC 61508 a été déclinée pour répondre à des besoins particuliers : la 61511 pour les systèmes instrumentés de sécurité, la 61512 pour les procédés batch, la 62061 pour la sécurité des machines, la 61513 pour le nucléaire, les EN 50128 et EN 50129 pour le ferroviaire. D'autres sont en préparation.

Un autre élément est venu renforcer sa crédibilité : c'est la loi du 30 juillet 2003 sur les risques technologiques et naturels majeurs, dite "loi Bachelot", qui introduit la notion de probabilités dans l'évaluation des risques, ce qui ne peut qu'apporter de l'eau au moulin de l'IEC 61508, qui est d'essence probabiliste. Ceux qui ne juraient que par l'approche déterministe pour traiter les problèmes de sécurité ont dû réviser leur jugement.

Patrick Teixeira. Cette loi impose de faire la preuve de la diminution de la probabilité de risque, ce qui n'était pas le cas auparavant. La loi n'impose pas en tant que tel de quantifier cette probabilité mais de mettre

en place un indicateur d'évolution de la probabilité du risque.

Mesures. Comment se concrétise sur le terrain toute cette effervescence autour de l'IEC 61508?

Michel Suzan. Au niveau des acteurs de la sécurité, ainsi que je l'ai dit, l'IEC 61508 est devenue un standard. Depuis qu'elle a reçu l'onction officielle, cette norme sert d'argument marketing pour les constructeurs d'automates ou de capteurs destinés aux applications de sécurité. Voyez les catalogues des constructeurs, vous verrez que des capteurs ou des automates qui avaient déjà une longue carrière sont désormais attifés d'un niveau SIL (le paramètre de base de l'IEC 61508) et, dans certains cas, proposés à un prix plus élevé…

Patrick Teixeira. En matière de produits destinés aux applications de sécurité, il y a une certaine confusion. Certains produits sont dûment certifiés, d'autres ne le sont pas. De plus, il y a aussi une grande disparité entre les approches des organismes de certification des produits, chacun a son propre référentiel.

Mesures. Pour l'instant, vous ne délivrez pas de certification, vous n'êtes donc pas concerné…

Patrick Teixeira. En France, on ne s'improvise pas organisme de certification de produits. Avec le *LCIE*, *Bureau Veritas* dispose d'une bonne base. Mais pour l'instant, nous ne sommes pas entrés dans ce domaine.

Ce que nous faisons, c'est délivrer des attestations de conformité, c'est-à-dire que nous prenons la responsabilité d'affirmer qu'un produit a été conçu en étant conforme à un référentiel (l'IEC 61508, par exemple) et nous fournissons les éléments permettant de le justifier.

Mesures. Revenons à l'application de la norme IEC 61508, de plus en plus prisée par les constructeurs de matériels. Est-ce que sur les sites industriels, les choses avancent?

Michel Suzan. Vous avez parlé il y a un instant de l'effervescence autour de la norme. C'est vrai mais il faut tout de même voir qu'elle trahit une réalité peu glorieuse : elle donne à penser que tout est nouveau alors qu'en fait beaucoup de choses existent depuis des années. En fait, on a perdu beaucoup de temps et aujourd'hui encore, le marché n'a toujours pas réellement décollé, la 61508 et la 61511 sont encore peu appliquées en milieu industriel. Avec l'arrivée massive de matériels (capteurs, automates, vannes, etc.) conformes à l'IEC 61508, on peut penser que les choses vont s'accélérer…

Mais attention tout de même de ne pas traiter les problèmes de sécurité par le petit bout de la lorgnette. Réaliser une fonction de sécurité, ce n'est pas utiliser tel ou tel équipement conforme aux normes. C'est beaucoup plus que cela, c'est adopter une démarche. Il faut partir de la notion de sécurité fonctionnelle, évaluer le risque, choisir des moyens pour chercher à le réduire, vérifier que dans le temps le risque résiduel est maîtrisé. Et cette démarche que nous préconisons est loin d'être une pratique courante sur les sites industriels. De plus, les difficultés financières que connaissent bien des entreprises n'arrangent pas les choses.

Patrick Teixeira. Le plus difficile dans tout cela, c'est l'analyse du risque et elle est souvent mal faite.

Mesures. Pourtant, les Drire, qui sont chargées de donner l'autorisation d'exploiter les installations, doivent vérifier tout cela…

Patrick Teixeira. Oui mais leur rôle n'est pas facile. Les industriels qui exploitent des usines dangereuses ne sont pas fous, ils tiennent à ce qu'elles fonctionnent correctement. Et ceci d'autant qu'ils sont légalement responsables de tout accident qui pourrait arriver et de ses conséquences. Les industriels en question mettent en œuvre des stratégies de sécurité, avec leurs propres recettes, souvent rodées par des décennies de pratique. Et ils arrivent en général à de très bons résultats. Les Drire examinent le dossier et donnent leur feu vert d'exploitation.

Cela dit, maintenant qu'il existe des référentiels, les choses devraient changer. Les industriels ont tout intérêt à les appliquer, ne serait-ce que pour pouvoir prouver, en cas d'accident, qu'ils avaient suivi une démarche rigoureuse. Les Drire, qui connaissent bien entendu ces référentiels, deviennent quant à elles beaucoup plus exigeantes.

Mesures. Quel est précisément votre rôle?

Michel Suzan. Notre principal rôle, c'est vraiment de sensibiliser les industriels à bien appréhender le risque. Cela fait, il est relativement simple de se fixer un objectif à atteindre et des solutions techniques à mettre en œuvre. *Bureau Veritas* apporte un réel savoir-faire dans tous ces domaines. Les industriels ont parfois tendance à sous-dimensionner le risque, car ils savent que plus le risque est élevé, plus les solutions à mettre en œuvre seront coûteuses et plus il y aura des contraintes au niveau de l'organisation et du comportement des personnes. Alors qu'il y a quelques années, ils faisaient un peu l'inverse, il leur arrivait de faire de la sur-sécurité. La crise que l'on connaît a fait évoluer les comportements…

Nous sommes neutres, nous les sensibilisons à l'importance de la démarche, les aidons à se poser les bonnes questions.

Mesures. Revenons à l'IEC 61508. Outre sa complexité, certains lui ont reproché de laisser trop de place aux interprétations…

Michel Suzan. Je ne comprends pas ce reproche. Pratiquement toutes les normes ont une marge pour l'interprétation. Et c'est le rôle des spécialistes d'apporter leur

Patrick Teixeira, responsable des activités "Sûreté de fonctionnement et mise en conformité CE des machines" à Bureau Veritas.

propre interprétation pour atteindre l'objectif de sécurité. *Bureau Veritas*, en proposant son interprétation, apporte une réelle valeur ajoutée.

Mesures. Parmi ces interprétations, certains disent que l'IEC 61508 s'applique aux constructeurs et l'IEC 61511 aux intégrateurs. Etes-vous d'accord?

Michel Suzan. Que l'IEC 61511 est destinée aux intégrateurs et aux utilisateurs, c'est une certitude. Pour l'IEC 61508, on ne peut avoir un avis aussi tranché parce qu'il s'agit d'une norme générique, applicable par tous. Mais, ainsi que vous l'avez souligné, elle est difficile à mettre en œuvre. Du coup, de fait, ce sont surtout les constructeurs de matériels qui l'appliquent…

Mesures. La notion de SIL (Safety Integrity Level, niveau d'intégrité de la sécurité) fait également débat. Normalement, elle s'applique à un système complet (capteur, contrôleur, vanne). Certains attribuent pourtant un Sil à chacun des éléments du système…

Patrick Teixeira. Le niveau Sil s'applique en effet à la boucle complète. Mais dans une installation, il y a par exemple des vannes manuelles qui contribuent à la réduction du risque, au même titre qu'un système instrumenté de sécurité. Il n'y a donc pas d'hérésie à lui attribuer un niveau SIL, en tant qu'objectif de fiabilité (car la norme et les SIL tels qu'ils y sont définis, ne s'applique qu'aux systèmes électriques, électroniques et électroniques programmables). L'IEC 61508 aborde d'ailleurs la notion d'éléments de sécurité, avec un niveau SIL pour chacun d'eux. Il peut être pertinent d'affecter un SIL à un sous-ensemble. Là-dessus, les fabricants de capteurs se sont engouffrés dans la brèche et attribuent des SIL à leurs produits, sans préciser dans quelles conditions ils sont obtenus ni ce qu'il faut faire pour les maintenir dans le temps. Là, il faut être très prudent…

Michel Suzan. Prenez l'exemple d'un capteur de vitesse. Selon qu'il est utilisé sur un compresseur, une turbine à vapeur ou une pompe, les conditions d'utilisation seront radicalement différentes, les constantes de temps seront différentes. Il est difficile dans ce cas-là de dire si le niveau SIL annoncé sera tenu dans les différentes situations. Nous ne sommes pas pour autant des intégristes de l'IEC 61508. Disposer d'un niveau SIL pour un capteur, c'est mieux que rien : il faudrait simplement que les constructeurs précisent les conditions dans lesquelles il a été obtenu et son champ précis d'applications. De ce côté-là, il reste du travail à faire. Mais il faut bien reconnaître que l'affectation de SIL aux différents éléments d'un système est pour beaucoup dans l'attrait du standard…

Patrick Teixeira. Lorsque *Bureau Veritas* délivre une attestation de conformité pour un sous-ensemble, avec un SIL donné, les hypothèses faites pour arriver au résultat sont clairement explicitées. Les conditions à remplir pour que ce niveau SIL soit maintenu dans le temps (le type et la fréquence des autotests) sont également très clairement mentionnées. Ce faisant, l'intégrateur qui utilise un tel sous-ensemble a beaucoup moins de questions à se poser. Mais cette approche n'est malheureusement pas adoptée par tout le monde et nous voyons beaucoup de cas où des SIL sont attribués sans autre précision et il est nécessaire de faire des études complémentaires…

Cette réflexion est valable aussi bien pour les SIL obtenus grâce à une solide étude théorique (en utilisant des techniques de sûreté de fonctionnement, arbres de défaillances, les diagrammes de Markov et autres) que ceux attribués "par expérience" (pour attribuer un SIL, la norme, avec la notion de "proven in use", donne la possibilité d'exploiter les données obtenues en exploitation).

Mesures. Y-a-t-il un moyen de vérifier la validité du SIL obtenu?

Michel Suzan. Certains disent "Nous avons fait des millions de test sur ce produit, vous pouvez l'utiliser sans problème dans votre application de sécurité". Mais cela ne prouve pas tout! Ce qui importe, c'est l'approche retenue pour développer le constituant ou l'application de sécurité. Le référentiel IEC 61508 ne donne pas d'indications sur la manière avec laquelle doivent être effectués les tests. L'organisme qui délivre une certification de produits ou une attestation de conformité doit surtout s'attacher à valider le processus de développement qui a été mis en place pour arriver à la sécurité, à valider la pertinence des choix qui ont été retenus.

Mesures. Une autre question revient souvent dans les applications de sécurité : Faut-il séparer les systèmes traitant de la sécurité et ceux traitant du contrôle-commande?

Patrick Teixeira. La norme n'est pas si précise et comme vous le savez, il y a des bus de terrain où les signaux de contrôle-commande et de sécurité utilisent le même câble, il y a aussi des automates de contrôle-commande qui abritent l'application de sécurité.

Cela dit, quand on est évaluateur, on aime bien que tout soit séparé : il y a forcément beaucoup moins de modes communs, il est plus facile de démontrer que la sécurité est assurée…

Mesures. Un mot enfin sur le logiciel, qui fait l'objet de beaucoup moins de discussions que les matériels. Est-il bien traité dans la norme?

Patrick Teixeira. Encore une fois la norme met en valeur l'importance de la démarche. Dans un système programmable, l'aspect logiciel est aussi important que l'aspect matériel (voire plus, mais comme il est souvent moins bien maîtrisé ou qu'on y accorde trop de confiance, on s'y attarde moins). Quand nous faisons une évaluation de conformité, nous validons le système dans son ensemble.

Mesures. Donc avec le logiciel applicatif?

Patrick Teixeira. Bien entendu. Et pour cela, comme pour le reste, nous mettons l'accent sur la démarche suivie par le développeur. Nous nous assurons aussi qu'il applique un certain nombre de règles de codage, qu'il utilise des outils de vérification du code.

Mesures. Parmi ces outils de vérification, utilisez-vous la technique de la preuve formelle?

Patrick Teixeira. Le cas ne s'est pas présenté mais pourquoi pas? La méthode de la preuve formelle consiste à lister les propriétés qui découlent du cahier des charges et à apporter la preuve (mathématique) que, une par une, toutes ces propriétés sont respectées. La méthode de la preuve formelle est très efficace mais elle est lourde à mettre en œuvre et impose une application dès la conception du logiciel. Du coup, seules les applications complexes en aéronautique ou dans le transport par rail y ont recours car, dans ces cas-là, les pannes peuvent amener à des accidents catastrophiques sur le plan humain et il faut donc réduire leur probabilité à un niveau extrêmement faible.

Mesures. Peut-on envisager des certifications ou des attestations de conformité pour des logiciels applicatifs standard?

Patrick Teixeira. Bien sûr et cela se pratique déjà. C'est ainsi qu'il est possible de certifier des blocs de fonction proposés dans les ateliers logiciels des automates programmables.

Propos recueillis par Jean-François Peyrucat