Quasi-machinement prêt ?

Depuis quelques années, tout le monde se contentait de la première Directive Machine, datant de 1989. Seulement, il fallait la faire évoluer ! Au final, le nouveau texte introduit quelques modifications de son champ d'application et des aménagements concernant les exigences essentielles de sécurité. En synthèse une évolution, pas une révolution.

Article 1 : Les Directives sont transposées à travers loi, décret, arrêté…, et doivent être appliquées.

Article 2 : La construction de machines est régie par la Directive Machines. L'objectif de cette dernière est de spécifier les exigences fondamentales en terme de sécurité pour la conception des machines. La conformité à cette Directive se visualisant notamment, par le marquage CE de la machine.

Voilà pour le décor. Depuis quelques années, tout le monde se contentait de la première Directive Machine, datant de 1989. Seulement, il fallait la faire évoluer ! La motivation première de la Commission Européenne était d'aboutir à une simplification de l'application de la directive et de faciliter son interprétation. Au final ce nouveau texte introduit quelques modifications de son champ d'application et des aménagements concernant les exigences essentielles de sécurité. En synthèse une évolution, pas une révolution. C'est ainsi qu'à la fin de cette année la directive 98/37/CE sera remplacée par la 2006/42/CE. Rentrant en application le 29 décembre 2009, elle aura un impact pour tous les industriels concepteurs et fabricants de machines et de composants de sécurité s'intégrant dans des machines.

LE 29 DÉCEMBRE 2009, C'EST DEMAIN

Avec cette nouvelle mouture c'est le champ d'application qui s'élargit, la Directive qui s'appliquait aux machines, aux équipements interchangeables et aux composants de sécurité traite également en plus par exemple des appareils portatifs de fixation à charge explosive, des ascenceurs de chantier. Mais surtout vient se rajouter la notion de quasi-machines…

Derrière le mot barbare de quasi-machine, on devine la notion de sous-ensembles. La définition est celle d'un ensemble qui constitue presque une machine, mais qui ne peut assurer à lui seul une application définie (un système d'entraînement par exemple). Une quasi-machine est uniquement destinée à être incorporée ou assemblée à d'autres machines ou à d'autres quasi-machines ou équipements en vue de constituer une machine à laquelle la directive s'applique. Difficile aujourd'hui de détailler les variantes de compréhension de cette définition. Beaucoup de points sont encore à régler.

Sur les principes de base, la directive reste inchangée. Son application repose toujours sur une évaluation du risque, tenant compte de la notion de *« mauvais usage raisonnablement prévisible »* et sur l'application des mesures appropriées visant à ces réduire. Les normes offrant une description du procédé d'appréciation du risque, et des solutions techniques assurant une présomption de conformité à la directive.

Il faut prendre en compte les exigences dans toutes les phases du cycle de vie de la machine, depuis la phase de transport et la fabrication, jusqu'à la mise au rebut. Certaines obligations ont été reformulées en ce sens, notamment pour la stabilité de la machine. Une exigence spécifique sur l'ergonomie a été ajoutée.

Parmi les changements qui vont perturber quelque peu les industriels, on trouve pour les protecteurs fixes, l'obligation d'avoir les moyens de fixations solidaires du protecteur ou de la machine. Impossible dorénavant de perdre les éléments de fixation des éléments de sécurité. Enfin notons que tout ce qui concerne la conception du circuit de commande a été aussi affiné.

LA SÉCURITÉ AU CŒUR DU SYSTÈME

Parallèlement, les référentiels normatifs sur les systèmes Instrumentés de sécurité ont également évolués. Ces systèmes prennent une place croissante dans tous les secteurs industriels, ils sont conçus et élaborés grâce à diverses technologies entraînant une multiplication des référentiels et des normes (CEI 61511 pour les industries du process ; EN 50126-50128-50129 pour le ferroviaire ; CEI 62061 et EN ISO 13849 pour le secteur de la machine...). C'est justement ces deux dernières qui participent au remplacement de la EN 954-1.

Pour mieux comprendre l'évolution engagée, rappelons que le référentiel d'origine était la norme EN 954-1 version 1996. Elle reste applicable jusque fin décembre 2009 (en effet un report a été demandé auprès de la commission européenne et la décision de pouvoir continuer à utiliser ce référentiel au-delà du 29 décembre 2009 se fera courant-décembre à Bruxelles). Dans ce contexte, la prise en compte de logiques de sécurité programmées nécessitait de faire un petit détour via l'IEC 61508…

Un nouveau référentiel normatif a vu le jour en 2006, l'EN ISO 13849-1. Cette norme considère à présent l'électronique programmable, en intégrant les aspects liés aux logiciels et

la dimension probabiliste de la conception, en plus des catégories initiées par l'EN 954-1. Ces catégories restent d'ailleurs à la base de l'analyse qualitative.

SÉCURITÉ DES MACHINES, LE CAS DE L'ISO 13849

Avec l'ISO 13849, on peut schématiquement distinguer deux grandes étapes. L'analyse des risques et l'analyse technologique.

L'analyse des risques. Tout d'abord, le processus de conception du circuit de commande doit débuter par une analyse générale de risque. C'est durant cette étape que le concepteur décidera de faire appel au circuit de commande pour réduire ou éliminer certains risques. Ainsi, la norme donne deux exemples pour illustrer ce point. Il s'agit du traitement d'un risque d'écrasement sur un outillage de machine. Le concepteur peut décider d'avoir recours à un outil fermé (contribution du système de commande faible voire nulle) ou à un barrage immatériel (contribution importante). L'analyse de risques permet de lister les fonctions de sécurité à implanter sur la machine (verrouillage des protecteurs, vitesse lente,…) et de déterminer leurs spécifications en incluant le niveau de performance requis.

L'analyse technologique. Le concepteur doit ensuite procéder à une analyse technologique. Il doit étudier tous les éléments des schémas, et traquer de la façon la plus précise les possibilités d'apparition d'une défaillance. Un défaut lié au circuit de commande pouvant engendrer un risque, il faut le prendre en compte pour répondre à l'exigence essentielle de sécurité de la nouvelle directive « Machines » EES : 1.2.1 Sécurité et fiabilité des systèmes de commande. La partie 2 de la norme Iso 13849 donne une liste de défauts présents et énonce des principes techniques de sécurité sur lesquels le concepteur peut s'appuyer. Le concepteur peut gérer ces défauts en adoptant des mesures axées sur la fiabilité, par le choix et la bonne intégration des composants. Il peut aussi travailler sur l'amélioration de la structure de la fonction de sécurité et mettre en oeuvre des mesures visant à éviter, détecter ou tolérer les défauts. La solution à retenir dépendra de l'application, de la réduction de risque visée et des technologies employées.

L'ANALYSE DE RISQUE

L'application correcte de la directive repose sur une analyse de risque globale de l'équipement. Il faut en effet tenir compte de l'ensemble des dispositions prises pour éliminer ou réduire le risque, et ne pas analyser hors contexte les parties du système de commande relatives à la sécurité. Bien souvent, les conceptions les plus simples offrent les meilleurs gages de sécurité. Ceci permet aussi de dimensionner correctement la fonction de sécurité gérée dans le circuit de commande.

Sélectionner les fonctions de sécurité. A partir de cette analyse de risque, le concepteur détermine l'ensemble des fonctions de sécurité à implanter sur la machine. Il définit pour chacune les spécifications qu'elles doivent respecter (fréquence de sollicitation, temps de réponse…).

Déterminer par fonction le niveau de performance requis (PLr). Pour chacune des fonctions de sécurité mises en évidence, le concepteur devra déterminer le niveau de performance qu'elle doit atteindre. Le niveau de performance représente l'aptitude d'une fonction à contribuer à la réduction du risque. Ce niveau de performance est classé en 5 niveaux (de a à e), allant d'une aptitude « faible » (a) à une aptitude « élevée » (e). plus la réduction du risque dépend de la fonction de sécurité, plus le niveau de performance requis sera élevé.

Ces niveaux de performance sont définis (en tant que grandeurs discrètes) en termes de probabilité de défaillance dangereuse par heure du système. En annexe A de la norme, un diagramme permet de sélectionner le niveau de performance.

VOUS AVEZ DIT QUASI ?

Une quasi-machine est un ensemble qui ne peut pas assurer à lui seul une application définie et est destinée à être incorporé ou assemblé à d'autres machines ou d'autres quasi-machines en vue de réaliser une machine (ex. : un moteur thermique ou un système d'entraînement). Elles ne suivent pas le même régime que les autres matériels.

Avant la mise sur le marché, un fabricant de quasi-machines ou son mandataire doit établir une documentation technique pertinente, une notice d'assemblage et une déclaration d'incorporation qu'il doit fournir à la livraison. ■

L'ANALYSE TECHNOLOGIQUE

Le concepteur doit choisir des composants aptes à *« résister aux contraintes normales de service et aux influences extérieures »* dans l'environnement d'utilisation prévu, et appliquer des moyens de protection si le composant doit rester dans des limites définies (exemple : fusible). Le circuit de commande doit être également conçu et construit de manière à éviter les situations dangereuses en cas d'erreur de logique dans les manœuvres.

De telles erreurs résultent de mauvaises manœuvres humaines, raisonnablement prévisibles, et dont le concepteur doit tenir compte (action simultanée sur deux commandes contradictoires, non-respect de l'ordre des séquences, choix d'un mauvais mode de fonctionnement).

Déterminer les parties constitutives de la fonction. Pour chacune des fonctions de sécurité, le concepteur doit déterminer les parties matérielles et logicielles qui la constituent. Dans ce travail, il peut être utile de recourir à une décomposition des fonctions suivant les modules d'entrée de traitement et de sortie. Suivant l'objectif assigné par l'analyse de risque et la technologie mis en œuvre, il peut choisir entre différentes architectures.

	Technologie mettant en oeuvre la(les) fonction(s) de commande relative(s) à la sécurité	ISO 13849-1	CEI 62061
A	Non électrique, par exemple hydraulique	X	Non couvert
B	Electromécanique, par exemple relais, et/ou électronique non complexe	Limité aux architectures désignées[a] et jusqu'à PL = e	Toutes architectures et jusqu'à SIL 3
C	Electronique complexe, par exemple programmable	Limité aux architectures désignées[a] et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
D	A combiné avec B	Limité aux architectures désignées[a] et jusqu'à PL = e	X[c]
E	C combiné avec B	Limité aux architectures désignées[a] et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
F	C combiné avec A, ou C combiné avec A et B	X[b]	X

X indique que ce cas est traité par la Norme internationale indiquée en tête de colonne.

[a] Les architectures désignées sont définies en 6.2 afin de fournir une approche simplifiée de la quantification du niveau de performance.
[b] Pour l'électronique complexe : utilisation des architectures désignées conformes à la présente partie de l'ISO 13849 jusqu'à PL = d ou toute architecture conforme à la CEI 62061.
[c] Pour la technologie non électrique, utilisation des parties en tant que sous-systèmes conformes à la présente partie de l'ISO 13849.

Utilisation recommandée de la CEI 62061 et de la présente partie de l'ISO 13849.

Schématiquement, les options suivantes sont envisageables :
- soit une stratégie de réduction des défauts, reposant sur la fiabilité,
- soit une stratégie de détection de défaut,
- soit une stratégie de redondance partielle ou complète
- soit une combinaison « détection de défaut - redondance ».

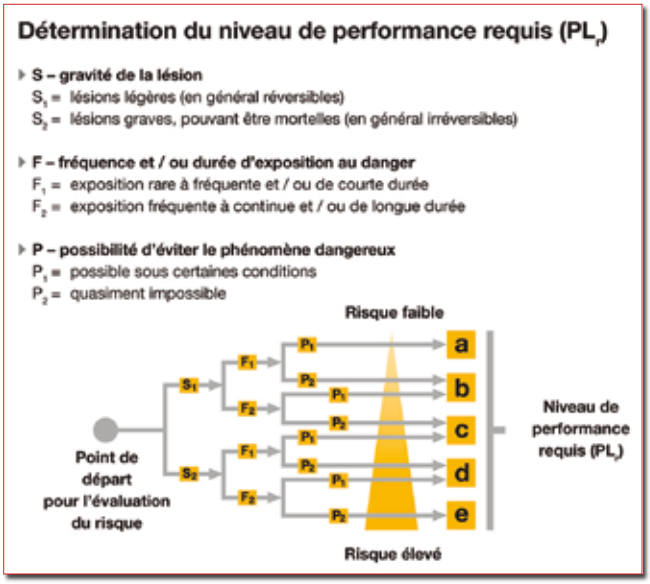
Estimer le niveau de performance atteint par la fonction. Il s'agit de vérifier maintenant, pour chaque fonction de sécurité, si le niveau de performance qu'elle atteint est suffisant au regard du niveau de performance (PL, Performance Level) requis par l'analyse de risque.

La probabilité de défaillance dangereuse du système dépend de plusieurs facteurs, tels que la structure du système, l'étendue de la détection des défauts (la couverture du diagnostic), la fiabilité des composants (le temps moyen avant défaillance dangereuse, la défaillance de cause commune), le processus de conception, la contrainte de fonctionnement, les conditions d'environnement et les méthodes de fonctionnement.

A cet égard, le concepteur doit schématiquement, pour chaque fonction, évaluer des notions telles que la fiabilité, la structure du système et les aspects qualitatifs non quantifiables.

Dans la norme, *l'estimation de la fiabilité* repose sur le calcul du MTTFd (temps moyen avant panne dangereuse). Effectuer ce calcul nécessite de pouvoir avoir, pour chacun des composants ou sous-ensemble de la fonction, les données de base. Pour les composants les plus usuels (relais, contacteurs…), la norme fournit des valeurs typiques qui pourront être appliquées sous réserve d'avoir choisi et intégré des composants en respectant les principes éprouvés. (Ces règles sont listées dans la partie 2 de la norme). La valeur du MTTFd est ensuite classée en trois niveaux (faible, moyen, élevé), pour faciliter la lecture dans le graphe final d'évaluation du niveau de performance atteint.

Pour évaluer le taux de détection de défauts de la fonction de sécurité, la norme donne en annexe des questionnaires qualitatifs qui permettent au concepteur d'être renseigné sur les mesures à mettre en œuvre pour détecter les défauts et le ratio de défauts détectés atteint. Ce taux de couverture atteint par la fonction (la couverture du diagnostic), sera classé, en fonction de sa valeur parmi trois classes (faible, moyen, élevé). Enfin, pour valider la fonction, si celle-ci prend en compte une architecture parti-



Détermination du niveau de performance requis (PL_r). (Doc. Pilz)

culière (à partir de la catégorie 2), le concepteur vérifiera que sa conception prend en considération, les défaillances de causes communes, en parcourant un tableau en annexe. La norme fournit également des « architectures désignées » qui sont des représentations logiques à respecter pour les différentes catégories.

Les aspects qualitatifs non quantifiables. Il s'agit par exemple de la défaillance systématique pour les parties logicielles. A partir de tous ces éléments, le constructeur peut alors estimer le niveau de performance atteint.

Les combinaisons. Les nouveaux concepts comme le niveau de performance et le taux de couverture permettent plus de souplesse dans l'application de la norme. On est loin des débats sur la détermination d'une hypothétique « catégorie globale » pour une fonction de sécurité réalisée à partir de sous-ensemble ayant des technologies et des structures différentes, et donc des catégories différentes.

Donnons un exemple pour illustrer la problématique (il ne s'agit pas ici d'exposer les règles à suivre pour pouvoir combiner des parties du système de commande de niveaux différents). L'exemple porte sur la fonction « verrouillage d'un protecteur », assurée par un interrupteur de position et une logique de commande agissant sur une électrovanne (pré-actionneur). On peut par exemple la réaliser en utilisant un interrupteur de position de catégorie 1 (PL = c), une électronique de commande de catégorie 3 (PL = d) et une électrovanne de catégorie 2 (PL = c).

Avec le seul concept de catégorie, il n'est pas possible de spécifier un niveau d'ensemble pour l'intégralité de la fonction. Maintenant cette fonction pourra être assignée avec un niveau de performance global PL = c. La norme donne les règles d'association.

Le logiciel. L'Iso 13849 prend en compte non seulement les défaillances aléatoires dues aux matériels et composants, mais également les défaillances systématiques (erreurs de spécification des prescriptions de sécurité ; erreurs de conception, fabrication, installation, exploitation du matériel ; erreurs de conception, modifications ultérieures, paramétrages, mise en œuvre, etc. du logiciel). La norme donne des prescriptions relatives à la réalisation du logiciel, en distinguant ce qui relève du logiciel embarqué de ce qui relève de l'application.

RESTENT DES QUESTIONS

Avec ces nouveaux référentiels normatifs qui vont entrer en applications il va falloir ajouter les données de chaque composant constitutif et donc connaître et posséder les informations correspondantes et comprendre les différentes formules.

Des outils logiciels spécifiques sont même proposés afin d'aider les industriels, c'est le cas de SIStema (logiciel distribué gratuitement par le BGIA – organisme de sécurité Allemand) qui peut s'avérer une aide à la fois à la validation des fonctions de sécurité selon la EN ISO 13849-1, et à la fois en apportant les données nécessaires, les fournisseurs de composants de sécurité alimentant régulièrement les bases de données du logiciel. ■

UN CHOIX CORNÉLIEN

Le constructeur de machines va devoir choisir entre une norme ISO et une norme IEC pour réaliser son projet.

S'il apparaît une certaine concurrence entre les groupes travail ISO et IEC, les deux normes ont été élaborées dans un climat relativement constructif. En témoigne un préambule commun aux deux normes ayant pour objectif d'expliquer leur utilisation. On notera toutefois une touche plutôt anglo-saxonne pour l'IEC 62061 et plutôt germanique pour l'ISO 13849-1.

Dans la pratique, un constructeur de machines va plutôt s'investir dans une norme plutôt qu'une autre. Mais il faut cependant comprendre que la connaissance des deux philosophies s'avère enrichissante ! Tout simplement parce que les fournisseurs de composants ou les donneurs d'ordre pouvant faire appel à l'un ou l'autre des référentiels, il sera donc impératif, pour le constructeur de machines, de connaître les deux.

La logique voudrait qu'à partir de ses deux normes, il n'en subsiste plus qu'une… à terme. Effectivement, pour une fois, la logique l'emporte ! D'ailleurs, une annexe commune aux deux textes devrait être éditée en 2009, de plus un groupe de travail commun sera chargé dans le cadre de la maintenance des normes, de produire une norme commune. Mais ne soyons pas trop pressés, car ce texte unique pourrait voir le jour à l'horizon 2015, 2016. Cet objectif est inscrit officiellement dans les résolutions prises en 2007 par le TC44 (groupe de l'IEC) et par le TC199 (groupe de l'ISO). ■

Guy Fages – Jautomatise

Philippe Lubineau – Responsable Recherche et Développement Mécatronique - Développement Durable