NORMALISATION

L'Iso 13849-1, un sérieux atout pour développer un système de contrôle-commande de sécurité

Les systèmes de sécurité comportent souvent des automatismes de contrôle, qui doivent être eux-mêmes sécurisés. Plusieurs normes sont en lice pour aider le concepteur à développer le système qui assurera le niveau de sécurité désiré. Nous vous présentons ici l'Iso 13849-1 qui s'inscrit dans le prolongement de la célèbre EN954, bien connue des concepteurs de systèmes de sécurité machine.

La sécurité des machines passe souvent par la mise en œuvre de dispositifs (barrages immatériels, verrouillage de protecteurs, commande à action maintenue,...) qui font appel au circuit de commande. La directive demande qu'un dysfonctionnement du circuit de commande ne génère pas de situation dangereuse. L'objectif n'est donc pas de concevoir un équipement exempt de défaillances, mais de conduire une analyse de risque sur leurs conséquences.

Dans les systèmes de sécurité, la partie contrôle-commande joue évidemment un rôle important. Elle ne pouvait évidemment pas échapper au processus de normalisation. Les normes EN 61508 et EN 62061 ont fait couler beaucoup d'encre, ses promoteurs sont très actifs. Sont-elles pour autant bien adaptées à l'ensemble des problèmes posés et surtout aux habitudes des spécialistes de la sécurité? Sans doute pas. L'introduction de trop de concepts probabilistes, tels que ceux développés dans ces normes peut imposer de gros efforts d'appropriation par les bureaux d'études, sans pour autant garantir une plus-value en terme de prévention des accidents. Se profile également la menace d'une obligation, de fait, de recourir à des tierces parties pour des certifications "volontaires". Des efforts, des dossiers, des coûts… La sécurité serait dans ce cas la grande oubliée.

Une révision bien menée de l'EN 954/Iso 13849 peut donner aux industriels et aux préventeurs les outils qu'ils attendent depuis des années, pour statuer facilement et sans ambiguïté sur la conformité des fonctions de sécurité. Des passerelles sont établies entre le niveau de performance défini dans ces normes avec le concept SIL (Safety Integrity Level) développé dans les normes EN 61508/62061.

La norme Iso 13849-1 "Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : Principes généraux de conception" a été publiée en 1999. Elle reprend la norme européenne EN 954 : 1996, qui définit les catégories (B, 1, 2, 3, 4) auxquelles doivent répondre les fonctions de sécurité de machines. Elle a pour objectif de donner des prescriptions sur la conception des parties du système de commande relataive à la sécurité. Elle s'applique aux systèmes de commande de tous les types de machines, indépendamment de la technologie et du type d'énergie utilisés (par exemple : électrique, hydraulique, pneumatique, mécanique).

La norme Iso 13849-1 est actuellement en cours de révision, afin de prendre en compte les difficultés rencontrées lors de la mise en œuvre de la norme EN 954 initiale et de tenir compte de l'évolution de l'état de l'art avec l'arrivée de systèmes électroniques programmables.

La démarche décrite dans la révision de la norme Iso 13 849 s'inscrit dans le cadre défini par les normes Iso 12 -100 (principes généraux de sécurité des machines) et Iso 14121(analyse du risque).

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

De l'EN 954-1 à l'Iso 13849-1

Pendant très longtemps, et encore beaucoup aujourd'hui, les concepteurs, constructeurs et utilisateurs de machines ont utilisé l'EN 954-1 pour tout ce qui touchait à la sécurité. Cette norme fait l'unanimité pour son côté pratique. Mais elle avait aussi quelques limites qu'il était de plus en plus difficile de masquer face à la montée en puissance d'une norme concurrente, l'IEC61508 (et ses dérivées), qui s'est d'ores et déjà imposée dans les systèmes électroniques de sécurité dans les applications de contrôle de process (en chimie, par exemple). C'est dans ce contexte qu'a été élaboré le projet de norme Iso 13849-1, appelé à succéder à l'EN 954-1.

Plusieurs reproches sont faits à l'EN 954-1. Il y a parfois des mauvaises interprétations dans l'utilisation de la grille qui conduit à la définition de la catégorie à laquelle doit répondre le système de sécurité (cette catégorie dépend du niveau du risque à couvrir, de sa dangerosité et de sa fréquence). Plus important sans doute, cette norme est perçue comme étant plus qualitative que quantitative, et elle ne va pas en profondeur pour évaluer des données statistiques par essence, comme par exemple la définition du temps moyen avant une panne ou le niveau de couverture du diagnostic (rapport entre la probabilité de détecter une défaillance dangereuse et la probabilité du total des défaillances dangereuses). Enfin, l'EN954-1 n'avait pas été étudiée pour l'utilisation de systèmes électroniques programmables de sécurité.

J-F P

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 l'anticiper.

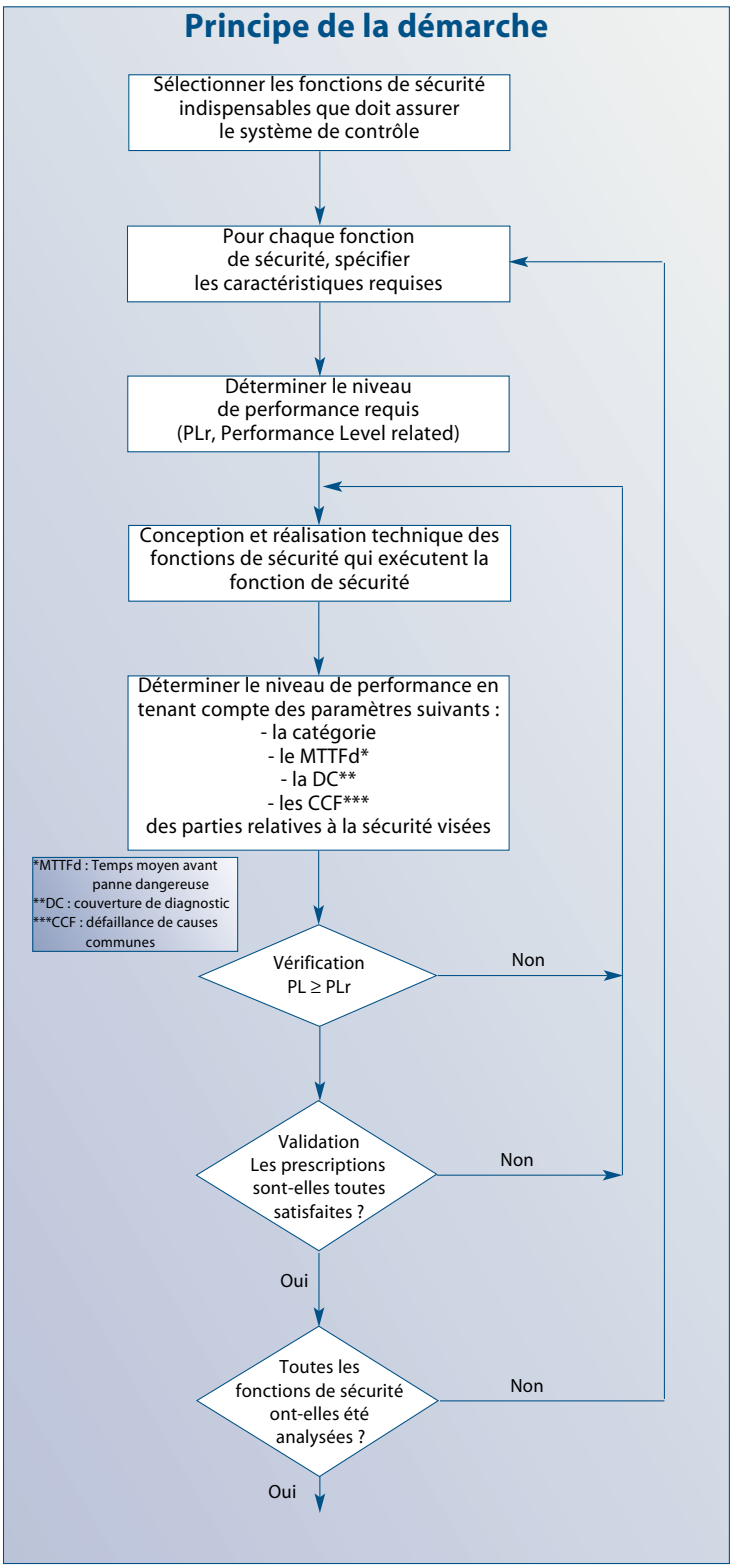
La partie 2 de la norme Iso 13849 donne une liste de défauts présents et énonce des principes techniques de sécurité sur lesquels le concepteur peut s'appuyer. Le concepteur peut gérer ces défauts en adoptant des mesures axées sur la fiabilité, par le choix et la bonne intégration des composants. Il peut aussi travailler sur l'amélioration de la structure de la fonction de sécurité et mettre en œuvre 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

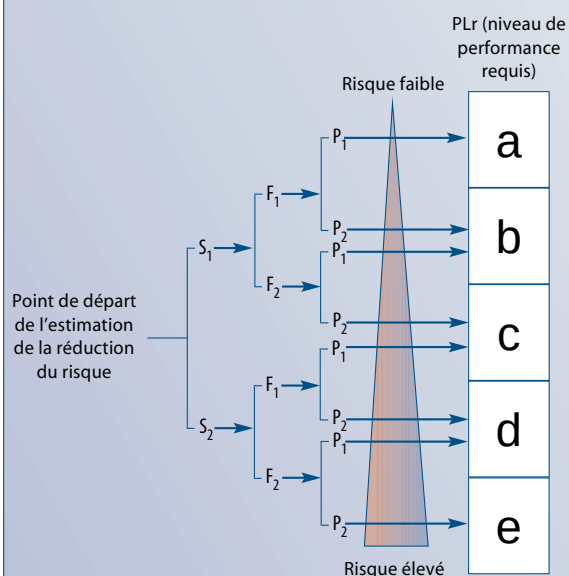
L'application correcte de la directive repose sur une analyse de risque globale de l'équipement. Il faut en effet tenir compte de l'ensemble des dispositions prises pour éliminer ou réduire le risque, et ne pas analyser hors contexte les parties du système de commande relatives à la sécurité. Bien souvent,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

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



Evaluation du niveau de performance requis



Paramètres de risques

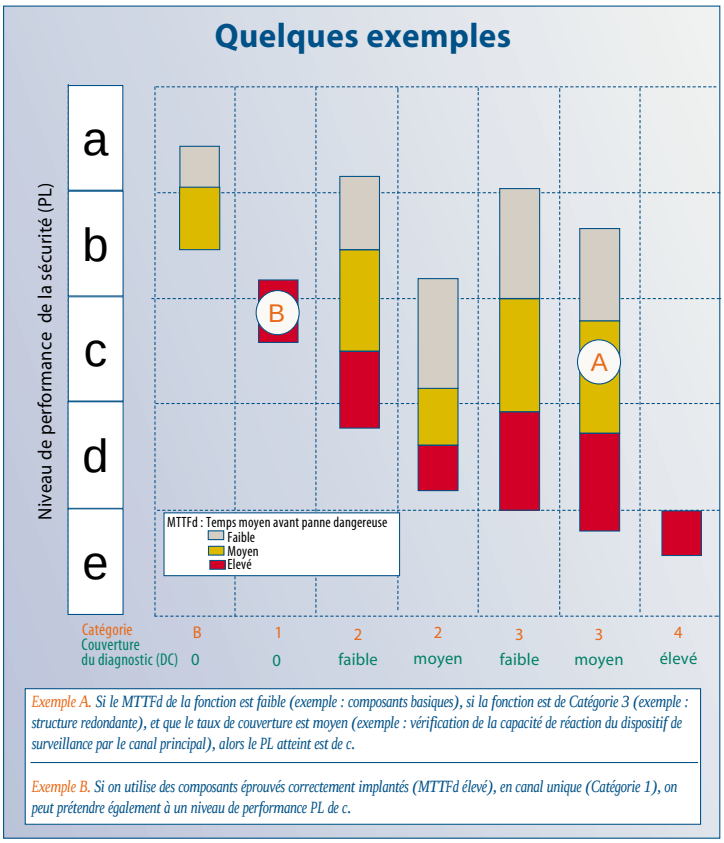
S	**Gravité de la blessure**
S1	Blessure légère (normalement réversible)
S2	Blessure grave (normalement irréversible, y compris le décès)
F	**Fréquence (et/ou durée d'exposition) du phénomène dangereux**
F1	Rare à assez fréquente (et/ou courte durée d'exposition)
F2	Fréquente à continue (et/ou longue durée d'exposition)
P	**Possibilité d'évier le phénomène dangereux ou de limiter le dommage**
P1	Possible sous certaines conditions
P2	Rarement possible

en 5 niveaux (de *a* à *e*), allant d'une aptitude de "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 du système. En annexe A de la norme, un diagramme permet de sélectionner le niveau de performance.

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. 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 le projet de 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 classée en trois niveaux (faible, moyen, élevé).
Pour l'évaluer *structure du système*, la norme donne en annexe des questionnaires qualitatifs qui permettent au concepteur de déterminer parmi trois classes (faible, moyen, élevé) le taux de couverture atteint par sa fonction (la couverture du diagnostic), ainsi que d'évaluer le taux de défaillance de causes communes. La norme fournit également des "architectures désignés" 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 construc-



Ce tableau donne une procédure simplifiée pour obtenir le PL (niveau de performances) atteint par une fonction de sécurité, en fonction du MTFFd, du taux de couverture (DC) et de la catégorie.

teur 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 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, 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.

Philippe Lubineau,
Responsable Produit Conception et Ecoconception,
Cetim